LA ACTUACIÓN POLICIAL EN LA PRE VISUALIZACIÓN DE CELULARES SECUESTRADOS EN EL MARCO DE UNA INVESTIGACIÓN PENAL: HERRAMIENTAS Y DESAFÍOS

Trabajo Final de Especialización en Cibercrimen

Alumno: Tomás Valdés, DNI N°33894303

Código: C-10

Formulación Del Problema

¿En qué medida el secuestro y la pre visualización de celulares secuestrados en investigaciones penales en la Ciudad de Córdoba se beneficiaría de la existencia de un marco normativo que los regule?

Justificación Del Problema

En la práctica actual del Ministerio Público Fiscal de Córdoba, el personal que lleva a cabo el secuestro de objetos de prueba, en el caso bajo estudio, dispositivos de telefonía celular, son miembros de la Policía Administrativa, que actúan bajo la dirección de funcionarios del Ministerio Público Fiscal. Ya sean Fiscales o Ayudantes Fiscales (Código procesal penal de la provincia de Córdoba. ley 8.123. 1991). Luego de su secuestro, el celular es alojado en un depósito de la comisaría más cercana al lugar del secuestro y finalmente es remitido al Gabinete especializado de la Policía Judicial para el relevamiento técnico de su contenido (Ley orgánica del Ministerio Público Fiscal ley 7.826. 1989). Desde su secuestro hasta su llegada al gabinete de Policía Científica, el celular es manipulado por diversos miembros de la Policía Administrativa. Dada la alta complejidad de los dispositivos de telefonía celular en la actualidad, los mismos deben ser manipulados con un especial cuidado y adoptando los recaudos necesarios para garantizar la incolumidad y preservación de la información contenida en el dispositivo, la cual servirá para la investigación penal que se esté llevando a cabo (Di Iorio, 2017). Ahora bien, previo al arribo del celular secuestrado al gabinete especializado que estará encargado del relevamiento de la información contenida en él, y con base en un criterio de celeridad, el Fiscal a cargo de la investigación, previa autorización de un Juez de Control y Faltas, puede encomendar a la Policía Administrativa que haga un relevamiento previo de la información contenida en un dispositivo móvil secuestrado. Ésta actividad, denominada pre visualización consiste en que un funcionario policial accede al contenido del celular secuestrado y navega por el mismo a los fines de recabar información relevante para la causa que se encuentra investigando. Luego realiza un Acta consignando la información relevada y declara su contenido. La pre visualización actualmente se encuentra avalada por el Tribunal Superior de Justicia de la Provincia de Córdoba (TSJ, Sala Penal "Aguilar", S. n°251, 03/10/2007). Ésta práctica, que como su nombre lo indica, debería ser de carácter preliminar y excepcional, pareciera haberse tornado en la regla a la hora de relevar información de un celular secuestrado e incorporar la misma al proceso. La complejidad de los dispositivos electrónicos y en concreto de los teléfonos celulares, hace necesario un marco normativo que regule ésta actividad a los fines de evitar alterar o perder la información contenida en el dispositivo electrónico. Actualmente y desde el año 2012, existe la norma ISO/IEC 27037, la cual establece un conjunto de pautas y protocolos para la identificación, adquisición y conservación de evidencia digital. Su implementación contribuiría a mejorar el trabajo realizado por la Policía Administrativa y minimizar los riesgos inherentes a un mal manejo de evidencia digital, en pos de una investigación más eficaz y transparente.

Objetivo Principal

Elaborar un ensayo que provea de herramientas al personal policial de Córdoba capital para la realización de una pre visualización de celulares secuestrados en el marco de una investigación penal del Ministerio Público Fiscal de la Provincia de Córdoba.

Objetivos Específicos

1. Realizar un estudio pormenorizado de la bibliografía, normativas y protocolos vigentes respecto de la manipulación de celulares secuestrados.
2. Establecer si la realización de la pre visualización es utilizada en forma excepcional o habitual.
3. Identificar actividades y prácticas realizadas por la policía ante el secuestro de celulares, haciendo foco en la pre visualización.
4. Relevar los recursos actuales con los que cuenta la Policía de la Provincia de Córdoba para la realización de una pre visualización de celulares secuestrados.

Marco Metodológico

Hipótesis

Los escasos recursos, formación y protocolos de actuaciones para el secuestro y pre visualización de celulares secuestrados -en el marco de una investigación penal- se constituyen en factores de riesgo para la conservación probatoria.

Finalidad Del Proyecto

La finalidad del presente proyecto es co-construir un ensayo de protocolo donde se especifique el accionar frente a la pre visualización de celulares secuestrados en el marco de una causa penal. El ensayo estará dirigido a la policía de Córdoba -agentes encargados de la pre visualización de teléfonos- y se nutrirá de experiencias previas -normativas internacionales ISO/IEC 27037- y protocolos vigentes en otras provincias argentinas.

Clase De Proyecto

El presente proyecto constituye una investigación de acción participativa, puesto que realizará un trabajo de campo -para la recopilación de experiencias- así como también un análisis exhaustivo del material bibliográfico existente en la temática. Se propone esta modalidad, ya que la finalidad del proyecto es la co-construcción de un protocolo de actuación frente al secuestro y la pre visualización de celulares secuestrados.

Enfoque Del Proyecto

El enfoque del proyecto es de tipo mixto, es decir cuantitativo y cualitativo. Se estructuró en dos etapas bien definidas. La primera orientada a una búsqueda de antecedentes -nacionales e internacionales- en la temática investigada y en una segunda etapa se relevó -mediante entrevistas semi-estructuradas y encuestas- el estado actual de la pre visualización de celulares en Córdoba.

Se realizó un estudio y análisis profundo de la norma ISO/IEC 27037, de la bibliografía existente al respecto y de los protocolos o buenas prácticas respecto del manejo de celulares, existentes tanto a nivel nacional como internacional. Durante la construcción del "estado del arte" se dio especial relevancia a los informes y trabajos realizados por organismos internacionales especializados en Informática Forense, tales como el Scientific Working Group on Digital Evidence (SWGDE) y el National Institute of Standard And Technology, (NIST), ambos dependientes del Departamento de Comercio de los Estados Unidos. A nivel nacional se realizó un estudio de los principales trabajos que refieren la materia, como la Guía Integral De Empleo De La Informática Forense En El Proceso Penal (Di Iorio, 2016) y los distintos protocolos existentes a nivel nacional y Provincial.-el Protocolo del Ministerio de Seguridad de la Nación y el Protocolo de la Provincia de Neuquén- Este análisis tuvo como objetivo dar cuenta de la existencia -o no- de marcos claros y bien definidos acerca de las buenas prácticas en el manejo de celulares secuestrados.

En la segunda etapa se realizaron encuestas virtuales a través de un formulario de Google Docs a miembros integrantes de Unidades Judiciales y Fiscalías de Instrucción de Córdoba capital. Ello con la finalidad de establecer cómo es llevada a cabo la actividad de pre visualización de teléfonos secuestrados en la ciudad de Córdoba. Seguidamente se realizaron entrevistas a distintos miembros de las Brigadas de Investigaciones de Unidades Judiciales y Fiscalías de Instrucción de la Provincia de Córdoba a los fines de establecer cuál es el modo en que se realizan las pre visualizaciones de celulares. Las entrevistas fueron llevadas a cabo con una modalidad semi-estructurada, y estuvieron orientadas a recabar datos sobre la manera en que se pre visualiza un celular, en qué espacio físico, con qué recaudos (en modo avión, conectado, cargando) si se realizan copias de la información, quienes intervienen en la manipulación del celular, si se realiza en un solo acto o en varios, entre otras y la existencia o no de un documento de cadena de custodia del celular secuestrado. A los fines de realizar las entrevistas se utilizó un celular con sistema operativo Android, con una aplicación de grabadora instalada, con el objeto de registrar los resultados.

Posteriormente se realizó una matriz de análisis, teniendo en cuenta las principales preocupaciones de las personas entrevistas en la que se construyeron categorías de análisis, que a la postre fueron constatados con los datos cuantitativos obtenidos en las encuestas realizadas. Del diálogo cuali-cuantitativo se obtuvo un acercamiento a la situación actual de la pre visualización de celulares en Córdoba.

Por último, -y no por eso menos relevante- se llevó a cabo durante todo el proceso una evaluación desde el comienzo del mismo, establecida cada 21 días y donde se realizó una reflexión constante acerca de los objetivos propuestos. Esta evaluación le imprimió al trabajo un carácter dinámico, en virtud del cual fue siendo revisado en función del

contexto, posibilidades reales de llevar a cabo el trabajo presentado y la disponibilidad de recursos.

Cronograma

Actividades:

1. Introducción.
2. Planteamiento y justificación del problema.
3. Planteamiento del Marco Teórico.
4. Planteamiento del Marco Metodológico.
5. Planteamiento de los objetivos (General y específicos).
6. Análisis de la bibliografía.
7. Realización de encuestas.
8. Realización de entrevistas.
9. Conclusiones.
10. Entrega.

	MESES	ENERO	FEBRERO	MARZO	ABRIL
ACTIVIDAD					
INTRODUCCIÓN					
PLANTEAMIENTO DEL PROBLEMA					
PLANTEAMIENTO DE OBJETIVOS					
MARCO TEÓRICO					
MARCO METODOLÓGICO					
ANALISIS DE BIBLIOGRAFÍA					
ENCUESTAS					
ENTREVISTAS					
CONCLUSIONES					
ENTREGA					

Fecha de Inicio: 30 de enero de 2024

Fecha de Finalización: 30 de abril de 2024

Marco Teórico

Durante el curso de una investigación penal, la policía administrativa o judicial puede proceder a la incautación de un dispositivo electrónico, dado que éste puede contener información importante para la investigación que se esté llevando a cabo (Código procesal penal de la provincia de Córdoba. ley 8.123. Córdoba, 5 de diciembre de 1991). La incautación, en el marco de un proceso penal se denomina "Secuestro", que se define como la aprehensión de una cosa por la autoridad judicial con el objeto de asegurar su función específica: la investigación de la verdad y la actuación de la ley penal. Se trata de un acto coercitivo, pues importa una restricción de los derechos patrimoniales o de terceros, que se ven privados temporalmente de la disponibilidad de una cosa. (Cafferata Nores, 2003).

Tanto la actividad del secuestro de dispositivos de telefonía celular, como las actividades subsiguientes, tendientes a extraer información de los mismos son parte de una disciplina llamada Informática Forense. La informática forense es "un método probatorio consistente en una colección de evidencias digitales para fines de investigación o legales" (Darahuge y Arellano, 2005, p. 9). En el marco de una investigación penal, la cual tiene como fin último la búsqueda de la verdad real, suele ser de vital importancia la información que pueda estar contenida en diversos dispositivos electrónicos, los cuales en la actualidad son utilizados para almacenar gran cantidad de información de todo tipo. Éstos dispositivos electrónicos (computadoras, tablets, notebooks y especialmente teléfonos celulares) funcionan como contenedores de lo que Di Iorio llama evidencia digital, la cual se define como "cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.)" (Di Iorio, 2016).

Dada la complejidad de los dispositivos informáticos se ha tornado necesario establecer pautas claras y protocolos para la correcta manipulación de dichos dispositivos. Procedimientos incorrectos o una manipulación inadecuada de celulares secuestrados, puede causar la pérdida de datos contenidos en él (Ayers, R., Brothers, S. and Wayne, J., 2014). Con el fin de minimizar dichos riesgos y con el objeto de dotar de legalidad a las pericias informáticas, diversos autores han arribado a un conjunto de principios básicos de la Informática Forense, recogidos por la norma ISO/IEC 27037, los cuales serán pilar fundamental del trabajo final, brindando un dialogo entre perspectivas que permita aportar teórica-metodológicamente al objetivo general presentado:

Principio de Confiabilidad

Una prueba es confiable si los métodos de preservación aplicados en las distintas etapas hacen que la prueba conserve su inalterabilidad a lo largo de todo el proceso. La informática forense otorga métodos y herramientas para garantizar la confiabilidad de una prueba indiciaria que ha sido recolectada. (Darahuge, M. E. y Arellano, L. E., 2005).

Principio de Relevancia

Que una prueba indiciaria sea relevante significa que tiene un alto grado de importancia para que sea categorizada como evidencia. (Darahuge, M. E. y Arellano, L. E., 2005).

Principio de Suficiencia

Una prueba indiciaria es suficiente si alcanza para exponer el o los hechos indiciarios que tienen que demostrarse en el proceso pericial. (Darahuge, M. E. y Arellano, L. E., 2005).

Principio de Trazabilidad

En todo momento de un proceso pericial, la prueba tiene que ser trazable a lo largo del tiempo. Esto significa que debemos saber quiénes fueron los responsables de la posesión y tenencia de las pruebas o evidencias, en cualquiera de sus formas, en cualquier etapa del proceso. (Darahuge, M. E. y Arellano, L. E., 2005).

Con el objeto de materializar éstos principios la International Organization for Standarization (ISO), creó la norma ISO/IEC 27037, denominada "DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL" con el objetivo de estandarizar las actividades realizadas por las fuerzas del orden sobre dispositivos electrónicos. Con base en esta norma, diversas organizaciones internacionales, han trabajado en protocolos e informes estableciendo buenas prácticas para el manejo de dispositivos electrónicos secuestrados. El trabajo presentado recuperó aportes teóricos de investigaciones previas; "Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition" (SWGDE, 2020) y "Best Practices for Mobile Device Forensic Analysis" (SWGDE,2020) del Scientific Working Group on Digital Evidence (SWGDE).

El tema ha sido tratado a nivel nacional por diversos autores, entre ellos Ana Haydee Di Iorio que en su trabajo "guía integral de empleo de la informática forense en el proceso penal", a tono con la norma ISO 27037 y demás trabajos internacionales, establece un conjunto de lineamientos y métodos para la manipulación de dispositivos informáticos secuestrados. Se observa que, entre dichos lineamientos, cobra especial relevancia el concepto de "Cadena de Custodia", el cual puede ser definido como "el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de los objetos o muestras que pueden ser fuente de prueba de hechos criminales (preservación total de su eficacia procesal). La documentación de dicha actividad a partir de la planilla correspondiente, permite detallar las particularidades de los elementos materia de prueba, los custodios, el lugar, el sitio exacto, fecha y hora de los traspasos y traslados de los mismos" (Protocolo de Cadena de Custodia N°889/15 de la Provincia de Buenos Aires, 2015).

Equipos Móviles Smartphone. Consideraciones generales

A continuación, se analizarán una serie de conceptos básicos relativos a los teléfonos celulares Smartphone que servirán para comprender mejor el análisis de la información que pueden llegar a contener y la forma de extraerla. Se puede definir a un Smartphone como el segmento de teléfonos móviles que, por sus características y capacidades, emulan las funciones propias de un ordenador o computadora. Ésta característica, dota a los teléfonos Smartphone o inteligentes de una alta funcionalidad y por consiguiente, capacidad para almacenar gran cantidad de datos.
Actualmente y con la industria de la telefonía en constante evolución, los teléfonos inteligentes abarcan un sin número de funciones, que van desde las que brinda un teléfono común, una calculadora, computadora personal, cámara de fotos, grabadora o reproductor multimedia.
Como rasgos comunes y generales a todos los Smartphone, podemos nombrar que cuenta con un microprocesador, una menor ROM, una memora RAM, micrófono, altavoz y actualmente la mayoría de ellos cuenta con una pantalla táctil LCD. Cuentan con slot empotrado o bandeja para colocar la memoria extraíble SD y la tarjeta SIM; Distintos medios de conectividad inalámbrica, tales como WiFi, Bluetooth o infrarrojo. (SWGDE, 2020)

Tarjeta SIM

Bajo el nombre de tecnología GSM (Global System for Mobile Communications) se engloban dos elementos. El equipo móvil, que ya fue brevemente descripto *supra* y el UICC (Integrated Circuit Card), el cual es un componente removible del dispositivo móvil que almacena datos sobre la identidad e información del abonado al servicio de telefonía.
La tarjeta SIM (Susbscriber Identity Module) es una tarjeta desmontable que se utiliza en los teléfonos celulares o algunos módems para identificar al suscriptor del servicio al momento en que quiera acceder a la red de telefonía. La tarjeta SIM almacena toda la información necesaria del suscriptor al servicio, de modo tal que puede utilizarse el mismo en cualquier dispositivo, sólo intercambiando la tarjeta SIM. Asimismo, estas tarjetas pueden almacenar datos tales como contactos telefónicos o de envío y recepción de mensajes. Es por ello que, al momento del análisis forense de un dispositivo móvil, es necesario también tener en cuenta la tarjeta SIM colocada en él.
Actualmente los dispositivos móviles que utilizan tecnología GSM no pueden operar como teléfonos sin una tarjeta SIM. (SWGDE, 2020).

Tipos de Tarjeta SIM

Actualmente existen tres tipos de tarjetas SIM.

1. Tarjeta Mini Sim: fueron las primeras en ser utilizadas para la tecnología GSM y cuentan con una capacidad de almacenamiento de 2k a 32k.
2. Tarjeta Micro Sim: Cumple exactamente la misma función que la anterior. La evolución tecnológica ha logrado reducir el tamaño de la tarjeta sin sacrificar funcionalidad. De hecho, las tarjetas Micro Sim cuenta con una capacidad de almacenamiento mayor que su antepasado, siendo la misma de 32k a 128k.
3. Tarjeta Nano Sim: ésta última categoría cumple las mismas funciones que las anteriores, pero logrando reducir aún más su tamaño. Respecto de la Micro Sim, la Nano es un 30% más pequeña. También cuenta con una capacidad de almacenamiento de 128k.

Como se vio, tanto el equipo móvil en sí mismo, como su memoria extraíble SD y la Tarjeta SIM pueden contener numerosa información que pueden contribuir al esclarecimiento de un determinado o aportar datos relevantes para una investigación. A modo de resumen y en forma enumerativa no taxativa, se indicarán los tipos de datos o archivos que pueden ser contenidos por un SmartPhone:

- Contactos
- Registros de llamadas entrantes y salientes
- Mensajes de texto enviados y recibidos
- Mensajería instantánea
- Coordenadas de GPS
- Mensajes de correo electrónico
- Historial de navegación web
- Fotografías
- Videos
- Archivos de audio
- Información financiera en general
- Historia de Búsqueda en motores de búsqueda web
- Agenda personal
- Información sobre e-commerce
- Datos de tarjetas de crédito o similares
- Datos de cuentas bancarias
- Archivos de cualquier clase almacenados en el dispositivo
- Redes sociales y la actividad en las mismas
- Claves y contraseñas

Etapas del proceso de relevamiento de datos de un teléfono celular

Siguiendo a Rick Ayers, Sam Brothers y Wayne Jansen, en su trabajo "Guidelines on Mobile Device Forensics", se analizaron las diversas actividades que se realizan para poder extraer datos contenidos en un teléfono celular. Dichas actividades se encuentran a su vez volcadas en la norma ISO/IEC 27037 bajo examen.

Preservación

Podemos decir que la primera actividad a realizar respecto de dispositivos que contienen evidencia digital es la preservación. A los fines de poder utilizar correctamente la evidencia digital recolectada, es importante que la misma sea preservada, para que no sufra alteraciones que puedan poner en riesgo una investigación mediante posibles pérdidas de información. El concepto de "preservación", engloba diversas tareas tales como la búsqueda, reconocimiento, documentación y recolección de evidencia digital. Seguidamente se analizarán las tareas propias que componen el concepto más amplio de preservación. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Asegurar y Evaluar la escena

Llevar a cabo procedimientos incorrectos o un mal maneja de dispositivos que contengan evidencia digital, puede traer aparejada una pérdida de la información contenida por el dispositivo. Sumado a ello, si el dispositivo no es manipulado con los recaudos necesarios, actividades propias de la criminalística tradicional, tales como relevamientos de huellas digitales o ADN podrían verse frustradas.
Se debe tener en cuenta que también pueden resultar de utilidad los accesorios del celular a secuestrar, tales como memorias extraíbles, por lo que el personal que concurra al lugar del secuestro debe realizar un relevamiento minucioso del lugar para evitar perder evidencia digital, teniendo en cuenta el pequeño tamaño que suelen tener los dispositivos extraíbles de almacenamiento, que facilitan su ocultamiento.
Si el propietario o tenedor del dispositivo secuestrado se encuentra en el lugar, puede ser de utilidad consultarle por las claves o patrones de desbloqueo del dispositivo en cuestión.
Puede ocurrir que el dispositivo que se pretende secuestrar se encuentre dañado o en una situación que dificulte su secuestro, como por ejemplo inmerso en algún líquido. En éstos casos, el personal que realiza el secuestro debe recuperar el dispositivo en el mismo estado en que se encuentra, aún inmerso en un líquido y remitirlo en forma urgente al laboratorio forense. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Documentación de la escena

Todos los dispositivos contenedores de evidencia digital deben ser identificados y fotografiados. La toma de fotografías debe ser realizada sin alterar la escena, es decir con el dispositivo en el estado en que se encontraba al momento de ingresar al lugar. Con todos sus accesorios conectados si los hubiera. En caso de que el dispositivo esté encendido, debe fotografiarse la pantalla de inicio en la cual puede consignarse información como la fecha, hora, nivel de batería, estado de servicio y demás consideraciones que puede ser útiles a la postre para establecer el entorno en el cual fue secuestrado el dispositivo. (Ayers, R., Brothers, S. and Wayne, J, 2014)

Identificación del dispositivo

Una vez en el lugar del secuestro de un celular y habiendo dado con el mismo, es importante identificar de qué tipo de dispositivo se trata, es decir la marca del fabricante, el modelo del dispositivo, la compañía de telefonía con la cual opera. En caso de ser posible, ubicar el número de IMEI del dispositivo.

Puesto que, en ocasiones, los previos tenedores de los celulares secuestrados pueden alterarlos mediante remoción de etiquetas o colocación de otras, resulta útil tomar fotografías del frente, dorso y laterales del mismo, así como también del estado actual del dispositivo, las cuales servirán para una ulterior identificación. Si el dispositivo se encuentra encendido, en la denominada pantalla de desbloqueo, pueden observarse datos útiles para la identificación del dispositivo, tales como la empresa prestadora de servicios, la marca o modelo del dispositivo. Existen otras estrategias que pueden aplicarse en el lugar de secuestro para identificar un celular. Si la batería del mismo es extraíble, debajo de ésta suele estar inscriptos la marca, modelo y número de IMEI del dispositivo. Éste último número también suele encontrarse grabado en la bandeja en la cual se coloca la tarjeta SIM.

Por último, otras herramientas para identificar las características de un celular secuestrado pueden ser las características exteriores generales del mismo. Diversas marcas tienen diseños únicos que distinguen sus productos y les confieren características únicas que los diferencian de otros fabricantes.

Es útil también analizar los conectores del dispositivo, ya que algunos fabricantes utilizan un tipo de conector que no es utilizado por los otros. Estas características además de aportar pistas para identificar la marca del dispositivo, también nos aporta datos respecto de la antigüedad o lapso en que el mismo puede haber sido fabricado.

La identificación del celular secuestrado cobra relevancia puesto que, conociendo la marca y modelo del mismo, puede accederse al manual de uso, el cual suele estar publicado en las páginas web del fabricante, y determinar cuál es la mejor forma de proceder para la extracción de la evidencia digital contenida en el dispositivo. (SWGDE, 2020).

Acceso al dispositivo

Frecuentemente, un equipo de telefonía celular se encuentra bloqueado. Éste bloqueo puede estar basado en una contraseña, un patrón de desbloqueo, en una ubicación por GPS o algún sistema de medición biométrica como una huella digital o el escaneo del rostro del usuario. Dependiendo del dispositivo de que se trate, las restricciones de uso varían cuando el celular está bloqueado. (SWGDE, 2020).
Además de éstos métodos tradicionales de bloqueo de celulares, éstos permiten agregar otros mecanismos de bloqueo o desbloqueo que no vienen incluidos en el dispositivo:

- **Detección Corporal:** Algunos dispositivos permiten instalar éste tipo de bloqueo. El dispositivo se programa para mantenerse desbloqueado mientras detecte que se encuentra en posesión del usuario. Por su parte se bloquea automáticamente si detecta que ya no se encuentra cerca del cuerpo de propietario. Este tipo de bloqueo y desbloqueo utiliza en giroscopio incorporado a los celulares y detecta determinados patrones de movimiento. Por ejemplo, apoyar el celular en una superficie plana como una mesa. Por otro lado, si el celular reconoce que está dentro de un automóvil u otro medio de transporte, puede llegar a permanecer desbloqueado aún si no se encuentra en manos de su propietario. Ésta característica debe ser tenida en cuenta al momento de realizar el secuestro de un celular. (SWGDE, 2020).

- **Lugares de confianza:** Esta función está diseñada para desbloquear el celular cuando abandona un lugar determinado por el usuario como “de confianza” y bloquearlo cuando lo abandona. Esto se determina más comúnmente mediante servicios de localización y redes inalámbricas de internet. Un usuario, por ejemplo, puede configurar su hogar como un "lugar de confianza" que permite que su dispositivo permanezca desbloqueado mientras se encuentre dentro de su domicilio. Cuando el teléfono detecte que abandona la ubicación determinada, se bloqueará. Esto debe tenerse en cuenta al confiscar o recuperar un teléfono antes abandonando la escena, ya que puede procederse a extraer los datos en el lugar de confianza. (SWGDE, 2020).

- **Dispositivos confiables**: Esta función está diseñada para bloquear y desbloquear un dispositivo, cuando éste está conectado a otro dispositivo previamente consignado por el usuario como “confiable”. Por ejemplo, un usuario puede configurar su reloj una “Smart Band” como confiable. Entonces, cuando un teléfono se vincula con un dispositivo confiable, se puede configurar para permanecer desbloqueado y cuando esta conexión se corta, el dispositivo se bloquea nuevamente. La conexión a la que se hace mención será generalmente a través de Bluetooth, pero no se descartan otras formas de

conexión por cable o inalámbricas. Éste modo de bloqueo debe ser tenido en cuenta y considerarse secuestrar el dispositivo confiable juntamente con el teléfono celular al cual esté vinculado. (SWGDE, 2020).

Dispositivos encendidos y bloqueados

En caso de que el dispositivo a secuestrar se encuentre encendido y bloqueado debe evitarse intentar adivinar la clave o solicitársela al usuario del teléfono. Ello puesto que los celulares pueden ser configurados para eliminar la información que contienen, en caso de que se ingrese una clave errónea. (SWGDE, 2020).

Dispositivos encendidos y desbloqueados

En caso de que se quiera secuestrar un dispositivo con sistema de bloqueo, que se encuentra encendido y casualmente desbloqueado, se debe mantener el teléfono encendido y "despierto" a los fines de evitar su bloqueo automático con el tiempo. Ello debe hacerse utilizando el método menos invasivo posible, con el objeto de no dañar o alterar la información contenida en el dispositivo. El método más simple, pero efectivo, será interactuar manualmente con la pantalla o el teclado. También pueden modificarse los parámetros de bloqueo automático, pero éste suele solicitar el ingreso de la clave. (SWGDE, 2020).

Aislamiento

Muchos dispositivos móviles cuentan con la capacidad de realizar un bloqueo o barrido de información remoto, con un simple mensaje o envió de código. Ello hace importante que el personal que realice el secuestro de un dispositivo electrónico, inmediatamente proceda a aislarlo de redes tales como Wifi, 3G, GSM etc. Además de evitar bloqueos o barrido remotos de información, se evita que ingresen nuevos datos al dispositivo, alterándolo de su esencia al momento de ser secuestrado. A grandes rasgos, existen tres métodos para aislar un dispositivo celular:

1. Configurar el dispositivo en "modo avión". Ésta opción aísla el dispositivo de las redes de telefonía, Wifi, Bluetooth, etc. No así de impactos magnéticos o radio eléctricos, dejándolo vulnerable a éste tipo de ataques. Asimismo, configurar el celular en modo avión requiere una interacción con el mismo por parte de la persona que realiza el secuestro, lo cual puede traer inconvenientes.
2. Apagar el dispositivo. Al igual que la opción anterior, apagar el dispositivo lo aísla de los diversos modos de conectividad mencionados. Apagar el dispositivo puede

activar requerimientos de claves de acceso o códigos de autenticación que pueden a la postre dificultar la extracción de la información.

3. Utilizar contenedores aislantes. Diversos fabricantes han desarrollado bolsas o contenedores que, por su material de fabricación, aíslan las comunicaciones radio eléctricas y magnéticas del dispositivo que contienen. Los más difundidos son los contenedores Faraday. Se creía que éste último método era el más eficaz para aislar un dispositivo. Pero la Universidad Perdue realizó un estudio acerca de la eficacia de los contenedores Faraday. En la mayoría de los casos bajo estudio, el contenedor Faraday permitió el ingreso de mensajes SMS y llamadas MMS al dispositivo que contenían. Casi en ningún caso, la protección aislante fue del 100%. El estudio concluyó que las causas de las filtraciones de debían a que el material utilizado no era lo suficientemente aislante, un deficiente sellado del contenedor y que el mismo contenedor funcionaba como antena receptora.

Además de los inconvenientes mencionados, los contenedores Faraday tienen un alto costo económico, por lo que su adquisición no se encuentra al alcance de todas las fuerzas de seguridad. (Ayers, R., Brothers, S. and Wayne, J, 2014)

Embalaje, trasporte y almacenamiento

Una vez secuestrado un dispositivo electrónico, es conveniente resguardarlo dentro de un contenedor sellado, al cual deberá incorporársele una etiqueta que identifique el elemento que contiene. Dada la fragilidad de los dispositivos electrónicos, es recomendable que sean remitido rápidamente al laboratorio forense. En caso de no contarse con uno, a un depósito apto para almacenar dichos dispositivos. Como requerimientos mínimos el depósito debería ser un lugar seco
y libre de humedad. Idealmente el depósito debería encontrarse aislado de impulsos electro magnéticos. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Cadena de Custodia

En este punto se abordará el concepto de cadena de custodia, el cual es transversal a todos los procedimientos con elementos secuestrados. A tales fines se siguieron los lineamientos del Manual de Procedimientos del sistema de cadena de custodia del Ministerio Público Fiscal de la Nación. Se puede definir la cadena de custodia como "el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal. Debe garantizar que el elemento de prueba o evidencia que se presenta en juicio, con el objeto de probar una determinada afirmación, sea el que ha sido reclutado y que no haya sufrido adulteraciones o modificaciones de parte de quienes lo introducen o terceras personas. Se debe tener especial cuidado en evitar cuestionamientos respecto del levantamiento y la custodia de los elementos o rastros que se presentan en el plenario, aventado cualquier sospecha sobre su procedencia y

dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen. Para llevar adelante esa actividad es preciso acreditar tanto el método utilizado, cuanto el personal que lo practicó. En definitiva, si las pruebas no se bastan a sí mismas –si es preciso identificar los objetos o huellas del delito, el sitio en que fueron encontrados, o la persona que tuvo a su cargo esa tarea-, resulta central prestarle atención al levantamiento y la conservación de ese material. Porque, si el método es incorrecto, el almacenamiento inadecuado o la persona incapaz de cumplir su cometido, el trabajo será inútil y la evidencia inservible (Rubén A. Chaia, 2010).

A modo ejemplificativo se adjuntan algunos modelos de Documento de Cadena de Custodia utilizados en nuestro País:

Documento de Cadena de Custodia utilizado en la Provincia de Buenos Aires

PROVINCIA DE BUENOS AIRES
PODER JUDICIAL
MINISTERIO PÚBLICO

Cadena Nro. :

DOCUMENTO DE CADENA DE CUSTODIA

UFI: **DEPTO. JUDICIAL:**

I.P.P./CAUSA:

DEP. POLICIAL INTERVINIENTE:

CARATULA:

VÍCTIMA:

IMPUTADO:

DATOS DE LA MUESTRA

Descripción de la muestra:	
Modo de conservación: (tachar lo que **NO corresponda**)	0°C a -4°C / frezzer / lugar frío o seco / Otro:
Lugar de toma /Identidad de la muestra:	
Perito que intervino: (**PRIMER ESLABÓN** de la cadena de custodia)	Datos personales Firma
Fecha / Hora:	
OBSERVACIONES:	

Documento de Cadena de Custodia utilizado a nivel Federal

Argentina unida — Ministerio de Seguridad Argentina

FORMULARIO DE CADENA DE CUSTODIA N°

FECHA		HORA	
CARÁTULA (preventiva)			
SUMARIO	N°		
JUZGADO/FISCALIA	N°		
SECRETARÍA	N°		
LUGAR DE RECOLECCIÓN			
Otra información de utilidad			
Identificación del Material			
Breve descripción del Material:*			

*La descripción completa se encuentra en el acta que corresponda (secuestro, allanamiento, levantamiento, entre otras) o en la pericia perteneciente a este material.

Modo de conservación	Medio ambiente		Conservadora refrigerada		Otros				
Tipo de embalaje / elemento contenedor	Sobres de papel		Bolsas Plásticas		Cajas		Frascos		Otros

RESPONSABLE DEL LEVANTAMIENTO (FIRMA)	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
1.				
Observaciones:				
	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA		HORA
2.				

Adquisición

La tarea de adquisición hace referencia a la copia u obtención de la evidencia digital contenida en un dispositivo electrónico, que luego podrá ser usada como prueba en un proceso judicial. Existen diversos modos de extracción de información, de los cuales sólo abordaremos algunos. (SWGDE, 2020).

Consideraciones generales de dispositivos con sistema operativo IOS

Desde el lanzamiento de los dispositivos móviles I Phone 3G en el año 2009, Apple ha incorporado a sus teléfonos un chip criptográfico dedicado, lo que hace posible un cifrado acelerado por el mismo hardware del equipo. La compañía incorpora esta criptografía acelerada al sistema operativo de sus teléfonos, como una característica que denominan “Data Protection”. Ésta característica es la combinación del cifrado

acelerado por hardware y un esquema criptográfico de autenticación, haciendo posible que cada pieza de información sea cifrada o descifrada con una clave diferente.
Los datos protegidos con éste esquema de "Data Protection" son encriptados con una clave aleatoria, la cual a su vez se encuentra protegida por una clave de nivel superior y almacenada en una carpeta del dispositivo. Las contraseñas y otros datos sensibles que pueden encontrarse almacenados en el dispositivo, se encuentran cifrados utilizando un enfoque parecido y se almacenan en lo que Apple denomina el "IOS Keychain" (llavero en inglés), que funciona como un mecanismo de depósito de claves que se encuentra dentro del mismo sistema operativo del teléfono.
Los archivos y elementos almacenados en la "keyChain" de un dispositivo I Phone se encuentran protegidos por uno de muchos números de acceso de control de claves, los que a su vez se encuentran encriptados de manera tal que el cifrado incluya la clave de desbloqueo del usuario o PIN.
De tal manera, la clave de usuario es necesaria para poder des encriptar las claves de acceso que protegen los archivos sensibles y los elementos almacenados en la KeyChain.
Este sistema de "Data Protection" ha sido criticado cuando salió al mercado, por considerarse que una clave de usuario de cuatro dígitos como el PIN o claves numéricas cortas similares, serían blanco fácil para un ataque de fuerza bruta. De hecho, se comprobó que una clave numérica de cuatro dígitos podría ser descifrada mediante un ataque de fuerza bruta en no más de veinte minutos.
Pese a ello, el esquema de cifrado utilizado por Apple presenta varios desafíos para su relevamiento y análisis forense. El analista forense debe estar al tanto de éste modo de cifrado y de los problemas que el mismo puede traer aparejado. El mayor de ellos es que numerosos dispositivos Apple, tanto I phone, como I Pods y I Pads, cuentan con una con opción de borrado remoto. Al llevarse a cabo éste borrado remoto, el UID (Users ID o clave de usuario) se elimina del teléfono, dejando así un grave problema de encriptación para el analista forense. Ya que como se dijo supra, la clave de usuario es parte del cifrado de los archivos de un dispositivo I Phone.
Es por esto, que es de suma importancia aislar un dispositivo I Phone secuestrado, de señales de radio o impulsos electromagnéticos. Tanto durante el traslado del equipo como durante su relevamiento y análisis de datos.
Cuando el "Data Protection" se encuentra activo, al eliminarse un archivo, también se elimina la clave de cifrado del mismo. Dejando así, archivos encriptados (y generalmente irrecuperables) en espacios no asignados. Lo que a su vez, torna inútiles las técnicas de "file carving", tradicionalmente utilizadas para recuperar archivos eliminados. (SWGDE, 2020).

Consideraciones generales de dispositivos con sistema operativo Android

"Android" es un sistema operativo diseñado por compañía Google principalmente para dispositivos móviles, es decir teléfonos celulares y Tablets, aunque recientemente ha sido incorporado a televisores inteligentes. El sistema Android es de código abierto y la misma compañía Google lanza actualizaciones prácticamente en forma anual.

Todas y cada una de éstas actualizaciones lanzadas por Google requiere modificaciones y características propias para poder ser aplicadas a cada familia de dispositivos, lo que en la práctica lleva a que existan incontables variantes de un mismo sistema operativo, cada una con características propias.
El sistema operativo Android cuenta con un repositorio o almacén principal de aplicaciones, llamado "Google Play Store". Pese a ello, el sistema de verificación de solvencia de una aplicación utilizado por "Google Play Store", llamado "Play Protect", no es del todo eficiente, lo que ha llevado a que los analistas encuentren innumerables aplicaciones dañinas dentro de dispositivos que utilizan el sistema operativo Android.
Android utiliza el sistema SQLite como sistema de almacenamiento. La mayoría de los datos referidos a los usuarios o aplicaciones, se encuentran almacenados en tablas de SQLite, ubicadas dentro de carpetas separadas para cada aplicación instalada en el dispositivo.
Dado que el sistema operativo Android fue diseñado principalmente para ser usado en dispositivos con pantalla táctil, el esquema de protección del dispositivo consiste en un patrón de desbloqueo Que básicamente es un gesto que se realiza con el dedo del usuario, el cual es dibujado en una cuadrícula de 3x3 puntos, los cuales deben ser unidos entre sí, formando el patrón. Una vez se inserta correctamente dicho patrón, el dispositivo se desbloquea.
La mayoría de los relevamientos de datos y análisis forense de dispositivos que usan el sistema operativo Android, se basan en la utilización del modo de depuración del mismo equipo. Existen herramientas de análisis forense que permiten habilitar el modo de depuración en celulares con sistema operativo Android. Pero con el constante lanzamiento de equipos nuevos al mercado y las diferencias entre el mismo sistema operativo Android, que existen entre las distintas familias de celulares, las herramientas de análisis deben recibir soporte y actualización constante.
Por otro lado, es importante mencionar que muchos dispositivos que utilizan Android, por su menor capacidad de almacenamiento propia, en contraste con los celulares I Phone, suelen contar con una tarjeta de memoria removible MicroSD. El analista forense debe prestar especial atención a éstas tarjetas, ya que las mismas suelen contener numerosos archivos que rara vez se encuentra encriptados o protegidos. Como mejor práctica, la Tarjeta de memoria debe ser bloqueada para escritura y realizar una imagen forense de la misma, utilizando las herramientas tradicionales de análisis forense. (SWGDE, 2020).

Consideraciones generales sobre las UICC

De manera similar al relevamiento de datos de un dispositivo móvil, para obtener datos de una UICC, es necesario establecer una conexión entre la estación de trabajo del analista forense y la UICC a través de la utilización de un lector PC/SC (Smart Card). Como siempre, la herramienta utilizada, debe ser documentada previo a la realización del análisis. Una vez establecida la conexión, la herramienta puede comenzar a extraer datos de la UICC.
En el caso de las UICC la realización de una imagen forense no es posible, por los mecanismos de protestación con los que cuenta el módulo. En cambio, la herramienta

de análisis forense envía comandos a la tarjeta llamados Application Protocols Data Units (APDU´s) a los fines de llevar a cabo una extracción lógica sin realizar modificaciones, de cada carpeta de los datos del sistema. Como se ve, los protocolos APDU son un simple intercambio de comandos y respuestas. Cada elemento contenido en la carpeta de sistema definido en estándar GSM, cuenta con un número de identificación asignado, el cual es único. Éste identificador puede ser utilizado para navegar entre las carpetas del sistema y realizar diversas operaciones tales como leer el contenido.
Dado que las UICC son dispositivos altamente estandarizados, existen pocas variaciones entre unas y otras, por lo que el relevamiento de los datos contenidos en las mismas, rara vez se presentan inconvenientes a la hora de realizar una extracción lógica. El punto más importante en el relevamiento de UICC es la selección de la herramienta de análisis forense correcta. Existen alguna que sólo extraen los datos que suelen ser más importantes en una investigación, mientras que otras extraen la totalidad de la información, lo que llevará a que el analista forense luego deba darle valor o no a la información obtenida. (SWGDE, 2020).

Equipo Tangencial

Se entiende por equipo tangencial a los dispositivos con capacidad de almacenamiento de datos, que pueden estar vinculados o contener datos de un teléfono celular. Se encuentra englobados en tres categorías. Tarjetas de memoria o discos externos, computadoras, laptos o notebooks que se encuentren sincronizadas con el celular y almacenamientos basados en el sistema de “nube”. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Tarjetas de Memoria

Las tarjetas de memoria son pequeños dispositivos que sirven como unidades de almacenamiento adicional de un celular y pueden contener una gran cantidad de datos de relevancia para una investigación. Las primeras tarjetas de memoria lanzadas al mercado tenían una capacidad de almacenamiento de 128MB, pero conforme los avances tecnológicos, las tarjetas de memoria son cada vez más pequeñas y con mayor capacidad de almacenamiento.
Además de incrementar la capacidad de memoria interna del celular, las tarjetas de memoria permiten compartir la información con otros dispositivos en forma rápida. Generalmente no se almacena allí datos de usuarios, claves o contraseñas, si no archivos multimedia tales como fotos y videos, que dependiendo del tipo de investigación que se esté llevando a cabo, pueden ser de mucha utilidad.
El contenido de éste tipo de memorias es de fácil adquisición y puede ser realizada mediante el uso de una herramienta forense clásica. En caso de una extracción lógica, los datos eliminados no podrán ser recuperados. Las tarjetas de memoria se trabajan de manera similar a un disco externo o extraíble, por lo que puede crearse una imagen forense y relevar los datos desde la misma.

Si por el contrario se realiza una extracción física de información, será posible recuperar información que ha sido eliminada. Un inconveniente que puede presentarse en éstos casos, es que la información referida al equipo móvil tal como mensajes SMS pueden requerir una decodificación manual. (Ayers, R., Brothers, S. and Wayne, J, 2014)

Equipos sincronizados o vinculados

Por otro lado, la información contenida en un celular, muchas veces también se encuentra presente en otro dispositivo. Esto es lo que se llama sincronización de dispositivos. La sincronización hace referencia a un proceso de resolución de diferencias de determinadas clases de información que se encuentre almacenada en dos o más tipos de dispositivos diferentes. De manera tal que las modificaciones que se realicen en uno de los dispositivos, sea vean reflejadas en todos los dispositivos vinculados al primero.
La sincronización puede ser realizada a nivel de archivos o de registro. A efectos prácticos ambas funcionan de manera similar. Cualquier discrepancia entre la fecha y hora de última sincronización, resulta en el reemplazo de los datos por la última versión de los mismos y su consiguiente reflejo en todos los dispositivos vinculados. El software de sincronización y las carpetas en las cuales se almacenará la información, dependerá del dispositivo móvil de que se trate. Cada software tiene una carpeta de almacenamiento por defecto en la computadora o notebook, pero también puede ser seleccionada por el usuario.
Usualmente estos dispositivos serán computadoras de escritorio, notebooks o tablets, pero con el advenimiento de televisores, consolas de juegos y electrodomésticos inteligentes, la sincronización de una celular abarca un sin número de dispositivos posibles.
Ahora bien. ¿Cuál es el beneficio de contar con un dispositivo vinculado al teléfono celular del cual se quiere relevar información? Dependiendo del dispositivo vinculado de que se trate, la extracción de la información puede resultar menos complicada. En especial si se trata de una computadora de escritorio o notebook. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Servicios de almacenamiento basados en la "Nube"

Los servicios de almacenamiento en la "Nube" permiten almacenar información de un teléfono celular en un servidor de internet, evitando ocupar espacio en la memoria interna del teléfono. Esta información, puede estar almacenada en diversas partes del mundo. Los entornos de computación en la nube tienen un diseño complejo y disperso geográficamente, por lo que extraer información de un servidor en la nube trae aparejado numerosos inconvenientes que en la mayoría de los casos no justificará su

elección sobre métodos que permitan extraer información directamente del dispositivo. (Ayers, R., Brothers, S. and Wayne, J, 2014).

Extracción Lógica

La extracción lógica obtiene información que se encuentra almacenada en el dispositivo en el cual se esté trabajando. La información es extraída a través del acceso al sistema de archivos. Para ello, se debe conectar el dispositivo del cual se quiera extraer la información, con la herramienta elegida para llevar a cabo la extracción. Ésta conexión puede ser física, mediante cables o puertos, o bien inalámbrica. Es importante elegir correctamente la forma de conexión, ya que la misma puede resultar en alteraciones de la información original. Las herramientas de extracción lógica envían comandos a la interfaz del dispositivo sobre el cual se esté trabajando y éste responde en base al comando enviado por la herramienta. (SWGDE, 2020).

Extracción Física

La extracción física se realiza copiando todo el contenido de la memoria del dispositivo. Éste tipo de extracción permite acceder no sólo a los datos visibles, si no también a los que se encuentran ocultos. Existen varios niveles de los cuales pueden ser recuperados datos que fueron eliminados. El primer nivel es del de los archivos del sistema. El segundo nivel es el de los archivos almacenados en la base de datos del dispositivo. Algunos datos eliminados que pueden encontrarse en la base de datos de un dispositivo son por ejemplo registros de llamadas, mensajes, contactos, etc. Los tipos de datos que se incluyen en la extracción física son contraseñas, datos de ubicación por GPS, aplicaciones que fueron instaladas, archivos de datos multimedia como imágenes, videos y sonidos, correos electrónicos, chats, etc. (SWGDE, 2020).

Extracción Manual

Este método se lleva a cabo visualizando y extrayendo la información directamente del dispositivo. Como su nombre lo indica, este método requiere la manipulación directa del dispositivo por parte del operador que realiza la extracción. Es por ello que puede tener como consecuencia que se alteren, modifiquen o borren datos involuntariamente. No permite recuperar datos que fueron previamente borrados o eliminados.
Generalmente se utiliza como último recurso y en casos en que no existan herramientas compatibles con el dispositivo cuyos datos deben ser extraídos. Esto puede ocurrir porque el dispositivo en cuestión recién sale al mercado y no existen actualizaciones de los softwares forenses que soporten ese dispositivo. Además del inherente riesgo de pérdida o alteración de la información contenida en el dispositivo a relevar, éste método presenta otros inconvenientes. Una extracción manual puede insumir una gran cantidad

de tiempo. Si el dispositivo no puede ser encendido, se encuentra dañado o tiene claves de acceso, no podrá realizarse una extracción manual.
El técnico que realice debe ser sumamente cuidadoso de no alterar la información contenida en el dispositivo. Debe ir registrando todos los pasos que se van realizando y en lo posible ir grabando las pantallas a la cuales accede. Deberá dejar constancia de cualquier incidente que ocurra durante la extracción y en particular cualquier pérdida o adulteración de datos que pudiera haber ocurrido. (SWGDE, 2020)
Como puede apreciarse, la llamada pre visualización realizada en investigaciones penales conducidas por el Ministerio Publico Fiscal de Córdoba, se enrola en éste tipo de método de extracción, con todos los riesgos y obstáculos que inherentemente trae aparejado. A éstos riesgos se le agrega que quien la realiza es personal policial, no un técnico forense.

Análisis de herramientas de extracción

En el mercado informático abundan los software y herramientas que pueden utilizarse para extraer información de un dispositivo móvil. Se acotará el análisis a sólo tres de ellas.

1. Cellebrite Ufed ultimate

El dispositivo Ufed ultimate fue desarrollado por la empresa Cellebrite, la cual, fundada en el año 1999 cuenta con una gran trayectoria en materia de telefonía celular. Son prestadores de servicios de numerosas fuerzas policiales y legales en todo el mundo y es el dispositivo más utilizado en Argentina.
El dispositivo Ufed ultimate fue diseñado para extraer información contenida en tarjetas SIM y teléfonos móviles que utilizan las tecnologías GSM, TDA y CDMA. El dispositivo cuenta con la posibilidad de conectarse al teléfono móvil que quiera relevarse, a través de cable o en forma inalámbrica mediante Bluetooth. El dispositivo cuenta con un sistema operativo con pantalla táctil y varios tipos de cables y puertos para poder conectarlo a equipos de diversos fabricantes de telefonía celular. Asimismo, cuenta con un lector de tarjeta SIM que está protegido para escritura.
El Ufed ultimate permita la extracción, decodificación, análisis y confección de informes de datos contenidos en equipos de telefonía celular. Permite realizar extracciones tanto físicas como lógicas del sistema de archivos y contraseñas, aun cuando han sido eliminados. Cuenta con soporte para relevar una gran variedad de dispositivos, tanto antiguos como modernos, así como también tabletas y dispositivos de GPS. Permite desbloquear numerosos dispositivos que se encuentren protegidos por una contraseña, pero no cuenta con la posibilidad de vulnerar las protecciones de tarjetas SIM mediante uso de PIN o PUK. En este caso se deberá clonar la tarjeta SIM en cuestión.

La herramienta cuenta con diversas aplicaciones, entre las cuales se cuentan la Ufed Phyisical Analyzer, para decodificar información y generar informes; Ufed Phone detective, que identifica rápidamente teléfonos móviles y el Ufed Reader que permite compartir información. Se hace especial mención del Ufed Touch Logical que es una herramienta destinada a personal de primera intervención y permite realizar un relevamiento rápido de una amplia gama de teléfonos celulares.
El principal beneficio de éste dispositivo es la amplia gama de dispositivos que permite relevar. Pese a ello, la evolución del mercado informático es constante y vertiginosa, por lo que éste y cualquier dispositivo de análisis requerirá de actualizaciones constantes para no verse obsoleto.

Se adjuntan a continuación imágenes ilustrativas del dispositivo bajo examen, extraídas del sitio oficial de la empresa Cellebrite:

2. XRY

La herramienta XRY fue desarrollada por la empresa sueca Micro Systemation AB. Fundada en el año 1984, actualmente y desde el año 2003 se dedica casi exclusivamente a brindar soluciones digitales para análisis forense. La empresa ofrece tres tipos de herramientas:

a. XRY Logical: Es el método de extracción más rápido, porque permite acceder y recuperar datos en vivo, así como datos del sistema de archivos del dispositivo encontrado en la escena del crimen. Extrae datos de dispositivos digitales mediante comunicación con el sistema operativo del dispositivo. El servicio es automático, pero equivale a examinar manualmente cada pantalla en el dispositivo y registrar lo que se muestra. Con el formato de archivo XRY patentado, los datos y la

integridad de su evidencia se mantienen a salvo desde la extracción hasta que deban ser utilizados.

XRY Logical es la solución de nivel básico para investigadores forenses ofrecida por la empresa. (XRY Logical — Extracciones Rápidas de Dispositivos Digitales | MSAB)

b. XRY Physical: Incluye una licencia completa de XRY Logical y es el siguiente nivel de licencia para la recuperación física de datos de dispositivos móviles. XRY Physical permite a los analistas eludir el sistema operativo para extraer todos los datos brutos del dispositivo. Este vaciado de memoria le da acceso al sistema, a datos protegidos y borrados, y también permite superar ciertos retos de seguridad y encriptación en dispositivos bloqueados. Utilizando XAMN, usted podrá ver el código hexadecimal rápidamente y, activando el modo fuente, usted podrá verificar los datos brutos originales.(XRY Physical — Extracción física Software XRY | MSAB)

c. XRY Pro: XRY Pro es la herramienta más avanzada ofrecida por la empresa. Permite acceder a algunos de los dispositivos más complejos y seguros, así como realizar desbloqueos y extracciones con las funciones y soluciones innovadoras de MSAB. Cuenta con un paquete de software de exploits de alto nivel, con los que se puede obtener las mejores funciones para acceder a teléfonos y, así, asegurarse de que puede acceder a algunos de los dispositivos más difíciles de vulnerar. (XRY Pro - MSAB)

Galería de Imágenes extraídas del sitio oficial del fabricante:

3. Oxygen Forensics Extractor

Esta herramienta fue creada por la empresa estadounidense Oxygen Software, que se dedica a ofrecer soluciones informáticas respecto de dispositivos móviles de una amplia gama de fabricantes. A diferencia de las dos herramientas anteriores, ésta se presenta sólo como una solución de software, por lo que no incluye ningún tipo de dispositivo propio para realizar la extracción o análisis de datos. Entre otras cosas, Oxygen Forensics extractor permite extracciones en tiempo real, "rootear" dispositivo Android, importar Back Up´s de dispositivos, importar imágenes de Android y IOS, guardar información en un Back Up de Oxygen Forensics y generar reportes con distintas extensiones (PDF, RTF, XLS, HTML, XML). (04-165 Oxygen Forensic Extractor (tamce.net))

Por último, se realizará un análisis comparativo entre las tres herramientas, tomando como punto de partida el análisis realizado en el "Guidelines on Moblie Device Forensics" de Rick Ayers, Sam Brothers y Wayne Jansen, conjugándolo con información extraída de los sitios oficiales de los fabricantes de las diferentes herramientas.

	Ufed Cellebrite Ultimate	**XRY Pro**	**Oxygen Forensics Extractor**
Sistema operativo utilizado	Windows	Windows	Windows
Cantidad de dispositivos soportados por la herramienta	Amplia	Amplia	Amplia
Tiene capacidad realizar una adquisición lógica de la UICC	Si	Si	no
Tiene capacidad para clonar una tarjeta SIM	Si	Si	No
Formas de adquisición	Física y lógica	Física y lógica	Lógica
Permite generar reportes en base a la información obtenida	Si	Si	Si
Redes de telefonía móvil soportadas	GSM, CDMA, iDEN/TDMA	GSM, CDMA, iDEN/TDMA	GSM, CDMA,
Tiene capacidad para realizar análisis de los datos extraídos	Si	Si	Si

Permite analizar datos importados desde otra herramienta	Si	No	No
Cuenta con Hardware para conectar dispositivos	Si	Si	No

Análisis de Encuestas y Entrevistas

Habiendo finalizado con la primera etapa del proyecto, que consistió en un análisis de la bibliografía existente y determinación de pautas para una correcta manipulación de celulares secuestrados, se dio paso a la segunda etapa, que consistió en la realización de encuestas y entrevistas.

Esta segunda etapa del proyecto, a su vez, fue pensada en dos momentos diferentes. En primer lugar, se realizó una encuesta con el objeto de obtener un marco general del modo en que se realiza el secuestro y las previsualizaciones de celulares secuestrados en la Ciudad de Córdoba. La obtención de éste marco general dio paso al segundo momento de ésta etapa del proyecto, que consistió en encuestas realizadas a personal policial comisionado de Unidades Judiciales, dado que, del resultado de la encuesta realizada, surge que son ellos quienes mayormente realizan el secuestro y las previsualizaciones de celulares secuestrados.

Resultado De La Encuesta

Las preguntas de la encuesta estuvieron orientadas a establecer con mayor precisión las prácticas llevadas a cabo por la policía administrativa en el manejo de celulares secuestrados y realizar un relevamiento de los recursos con los que se cuentan para ello.

Primeramente, corresponde destacar que la encuesta estuvo destinada a miembros del Ministerio Público Fiscal de la Provincia de Córdoba, y en concreto a integrantes de Fiscalías de Instrucción y Unidades Judiciales. Se orientó la encuesta a éstas dos oficinas, puesto que ellas nuclean la mayor cantidad de personal de dicho Ministerio y por ser las oficinas que en las cuales se ordena la realización de una pre visualización.

El objetivo de la encuesta, tal como se dijo fue relevar el estado actual de la pre visualización en el marco de una investigación penal preparatoria, el modo en que se realiza, los fundamentos para ordenarla y las principales preocupaciones en torno a la misma.

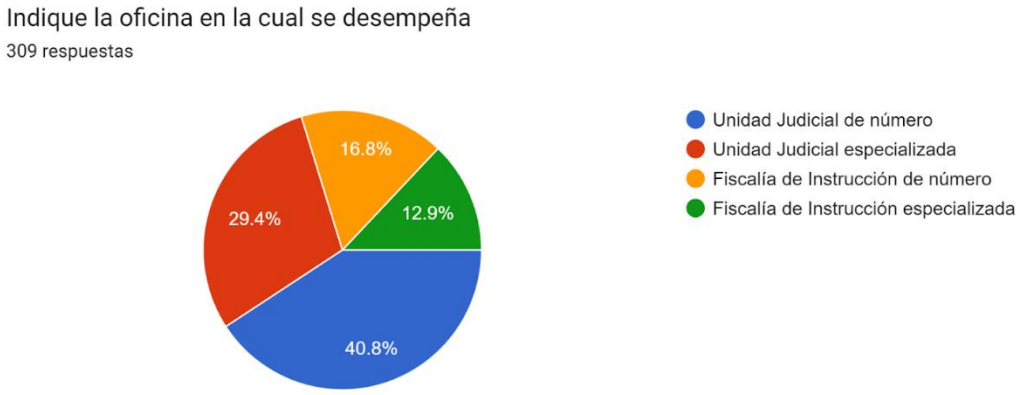
A los fines de obtener esos datos, y no existiendo un marco regulatorio propio de la pre visualización, se recurrió a la experiencia de cada miembro del Ministerio Público Fiscal. Se realizó un cuestionario con preguntas estructuradas, tendientes a establecer primero las características personales de los encuestados y segundo qué conocimiento tiene de la pre

visualización de celulares y la forma en que la misma se lleva a cabo. Por último, se abrió un espacio abierto para que cada entrevistado pudiera plasmar las preocupaciones o ideas que tiene sobre la pre visualización.

El cuestionario, que fue armado en un formulario de Google Forms, fue remitido vía whatsapp y correo electrónico a personal de Fiscalías de Instrucción y Unidades Judiciales de la Ciudad de Córdoba. Fue de carácter anónimo a los fines de resguardar la identidad de los encuestados, habida cuenta la sensibilidad del trabajo que las oficinas mencionadas realizan, pero principalmente para no con condicionar las respuesta de los agentes a lo que se esperaría que contesten y obtener así, una muestra lo más cercana a la realidad posible.

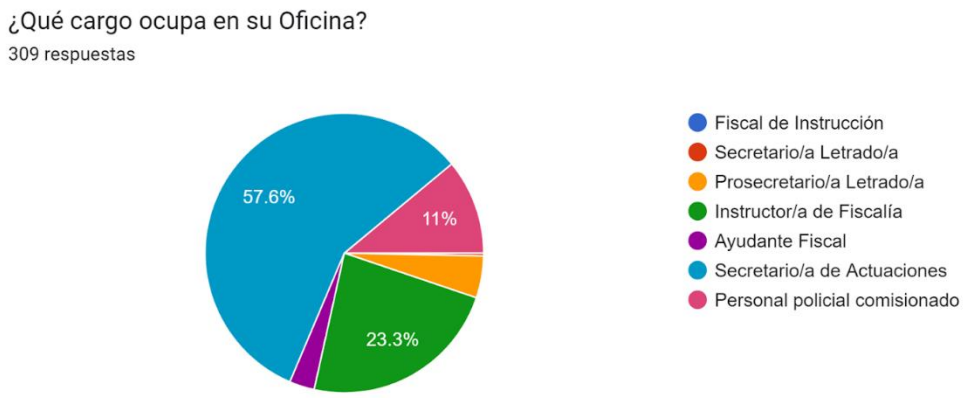
De acuerdo con la página oficial del Ministerio Público Fiscal de la Provincia de Córdoba, la Ciudad Capital cuenta con treinta y nueve Fiscalía de Instrucción y treinta unidades judiciales. Cada oficina tiene un personal aproximado de quince miembros, lo que da un total de aproximadamente mil agentes trabajando en Fiscalías de Instrucción o Unidades Judiciales de la Ciudad de Córdoba.
El cuestionario remitido fue contestado por trescientos nueve agentes, lo que da cuenta de un nivel de adhesión de aproximadamente un treinta por ciento de la planta total, haciendo que la muestra obtenida sea representativa del total de los agentes y por lo tanto generalizable (Hernández Sampieri, 2014)

Figura 1



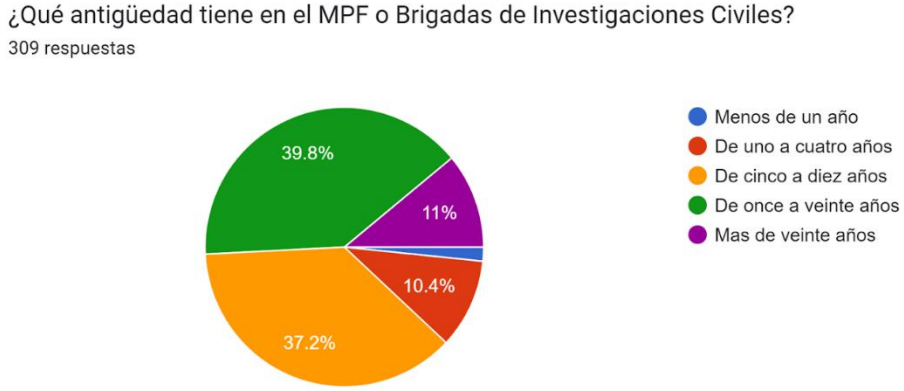
En una primera etapa del cuestionario se abordaron cuestiones personales de los encuestados a los fines de establecer determinadas pautas que abonen el conocimiento que pudieran tener del concepto de previsualización.
Tal como se consigna en la “figura 1”, del total de los encuestados, el 70.2% manifestó desempeñarse en una Unidad Judicial, ya sea de investigación de delitos comunes o especiales y el 30% en Fiscalías de Instrucción, lo que da cuenta que la temática generó mayor interés en el personal de las Unidades Judiciales.

Figura 2



Seguidamente, se consultó a los encuestados el cargo que ocupan en la dependencia en la cual se desempeñan. El 57.6% manifestó ser secretario de actuaciones de unidad judicial, mientras que el 23.3% refirió ser empleado instructor de una Fiscalía de Instrucción. Ambos escalafones representan el eslabón jerárquicamente más bajo de cada oficina y constituyen la mayor cantidad de agentes de cada una. Sólo el 2.9% respondió ser Ayudante Fiscal, Funcionario a cargo de la Unidad Judicial. El 4.9% contestó ser Prosecretario Letrado, Funcionario de Fiscalía de Instrucción y el 11% manifestó ser personal policial comisionado, policías bajo las órdenes de Fiscales y Ayudantes Fiscales encargados de llevar a cabo las directivas impartidas por éstos. Se evidencia una ausencia de respuesta al cuestionario, de Fiscales de Instrucción y Secretarios Letrados, funcionarios superiores de la Fiscalía de Instrucción.

Figura 3



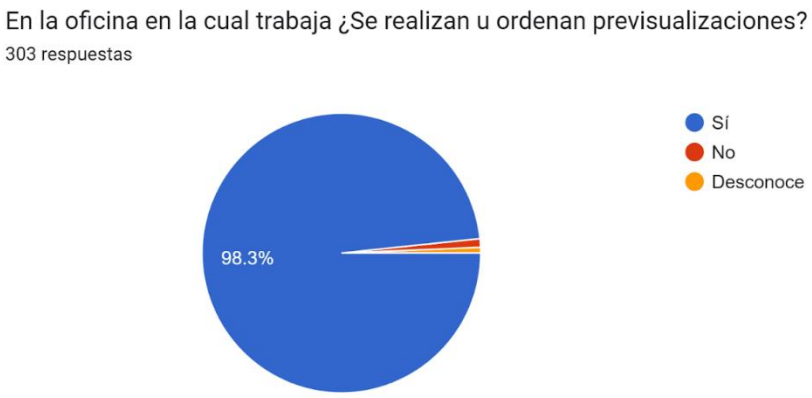
En tercer lugar se consultó a los encuestados la antigüedad que tienen trabajando como agentes del Ministerio Público Fiscal o Brigadas de Investigaciones Civiles. La pregunta tenía como objetivo establecer la experiencia y nivel de conocimiento del público entrevistado respecto de los procedimientos y prácticas comunes llevadas a cabo en una investigación penal llevada a cabo por el Ministerio Público Fiscal. El 3.8% de los encuestados refirió tener una antigüedad en su cargo de entre once y veinte años. El 37.2% manifestó tener entre cinco y

diez años de antigüedad. El 11% tener una antigüedad de más de años, el 10.4% de uno a cinco y sólo el 1.6% tener menos de un año de antigüedad. Tal y como surge de la “Figura 3” que se adjunta continuación, el 88% de la población objetivo cuenta con una antigüedad de por lo menos cinco años en el ejercicio de la función, por lo cual se puede concluir que ese porcentaje de la población contaría con experiencia y conocimientos suficientes para aportar datos confiables respecto de los procedimientos y prácticas del Ministerio Público Fiscal en el marco de una investigación penal.

Figura 4

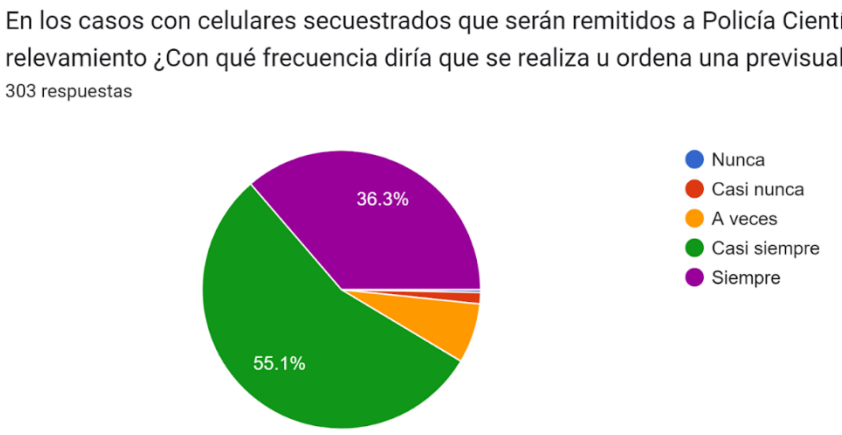
Finalizada la etapa de caracterización personal de los encuestados, se orientó el cuestionario a la temática específica del presente trabajo, es decir la pre visualización de celulares secuestrados. La primera pregunta de éste bloque del cuestionario es si el encuestado se encuentra familiarizado con el concepto de pre visualización. Tal y como muestra la “Figura 4” que se adjunta a continuación, el 97.7% de los encuestados manifestó encontrarse familiarizado con la temática. Tan sólo el 2.3% (siete encuestados) respondió desconocer el concepto mencionado. Dicho número de encuestados concuerda con la cantidad de agentes que respondieron tener menos de un año de antigüedad en el Ministerio Público Fiscal o Brigadas de Investigaciones.

Figura 5



La siguiente pregunta del cuestionario requería a los encuestados consignar si en la Oficina en la cual se desempeñan se realizan (en el caso de las Unidades Judiciales) o se ordenan (en el caso de las Fiscalías). El 98.3% de los encuestados manifestó que en la oficina en la cual trabaja se realizan un ordenan previsualizaciones. Sólo el 1% respondió que no se realizan y el 0.7% respondió desconocerlo. El número total de encuestados que respondieron negativamente o con desconocimiento asciende a cinco, lo que nuevamente concuerda con el porcentaje de la población que cuenta con menos de un año de antigüedad en la función que desempeña.
El porcentaje mayor a 95% dota a los datos recabados en ésta pregunta, de un alto margen de confiabilidad, lo que permitió establecer que la práctica de la pre visualización de celulares secuestrados, es una práctica establecida en el marco de una investigación llevada a cabo por el Ministerio Público Fiscal.

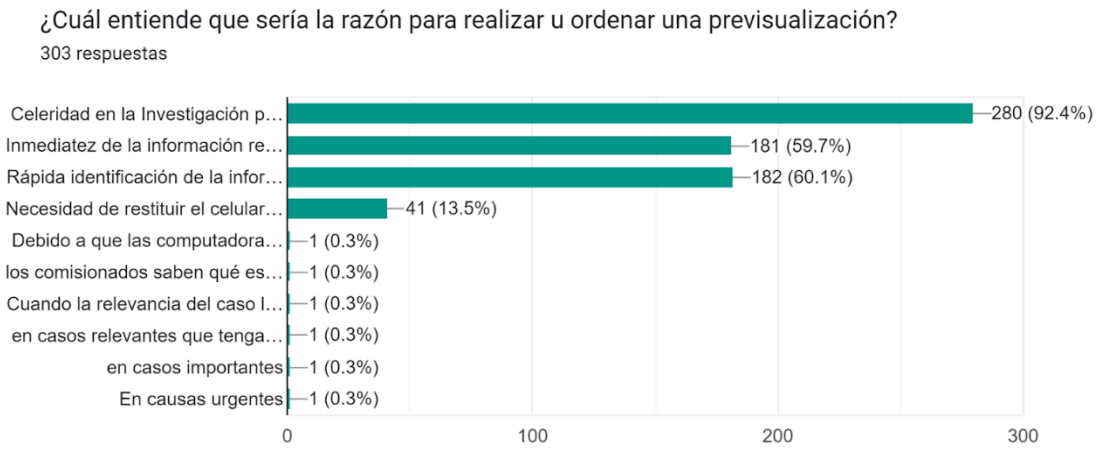
Figura 6



Ya establecido que la pre visualización es una práctica corriente utilizada en una investigación penal; En la tercera pregunta del bloque sobre previsualización del cuestionario, se solicita a los encuestados que precisen la frecuencia con la cual se lleva a cabo ésta práctica. La pregunta tuvo por objetivo establecer si la previsualización de celulares secuestrados, cuya información

será relevada en un gabinete técnico, se solicita en forma excepcional, o por el contrario se ha constituido en la regla a la hora de obtener datos de un dispositivo móvil.
El 55.1% de los encuestados refirió que en el caso en que se requiera obtener información de un celular secuestrado, previo a remitirlo al gabinete especializado, "casi siempre" se ordena o realiza una previsualización. El 36.6% respondió que en el caso planteado "siempre" se solicita previamente una previsualización del contenido. El 6.9% respondió que sólo se solicita "a veces" y sólo el 1.3% respondió que "casi nunca". Ninguno de los agentes encuestados respondió que nunca se solicita una previsualización.

Figura 7



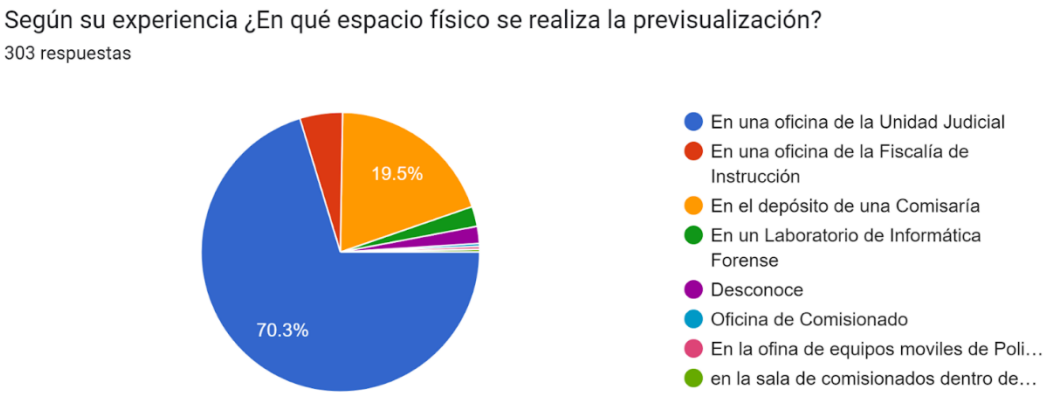
La siguiente pregunta del cuestionario no constituía una pregunta de opción múltiple como las anteriores si no una lista de casillas de verificación, a la cual se agregó un espacio de libre escritura en el cual los entrevistados pudieron incorporar opciones no propuestas en el listado. El objetivo de ésta pregunta fue establecer cuáles son las causas que llevan al titular de la oficina de que se trate, a ordenar la realización de una previsualización. Dada la modalidad de la pregunta, las respuestas no son excluyentes entre ellas y las respuestas pueden superponerse.
El 92.4% de los encuestados contestó que la razón para ordenar una previsualización era "Celeridad en la Investigación por demoras en la realización del informe pericial". La alta tasa de confiabilidad de ésta respuesta da cuenta de que la realización de una previsualización viene a suplir demoras en la confección del informe pericial sobre el teléfono de que se trate.
El 59.7% respondió que la razón también es la "Inmediatez de la información respecto del personal que investiga el caso". El 60.1% respondió que la razón sería la "Rápida identificación de la información relevante para la investigación". Éstas respuestas indican que los responsables de la investigación consideran conveniente que el investigador tenga un contacto directo con el objeto de prueba, en vez de recabar información del informe pericial.
Finalmente el 13.5% de los encuestados consignó que la razón para solicitar una pre visualización sería la "Necesidad de restituir el celular secuestrado".
Por último, se obtuvieron seis respuestas escritas libremente por los encuestados, que no fueron propuestas en el formulario. La primera de ellas reza "Debido a que las computadoras de la uj

no soportan el programa para ver los informes sobre los celulares (celebrate Reader)", lo que da cuenta de que la realización de una pre visualización respondería a falta de equipo adecuado en las Unidades Judiciales. La segunda "los comisionados saben qué es lo que interesa para la causa". Respuesta que si bien no estaba propuesta en el formulario, coincide con el hecho de que los investigadores identifican rápidamente la información pertinente para la investigación". El resto de las respuestas libres hizo referencia a que la causa de solicitar la previsualización del contenido de un celular es cuando la causa que lo motiva es de relevancia o reviste urgencia.

Figura 8

La octava pregunta tuvo como objetivo establecer quién se encuentra a cargo de la realización de una previsualización de celulares secuestrados. Ello para indagar a posteriori sobre las capacidades técnicas de la persona que usualmente realiza aquella actividad.
El 71.6% de los agentes encuestados, manifestó que la persona que realiza la previsualización es un personal policial comisionado, ya sea de una Unidad Judicial, o de una Fiscalía de Instrucción. Por su parte, el 24.4% respondió que quien realiza la previsualización es un Secretario de Actuaciones de Unidad Judicial. Solo el 2% consignó que la tarea es realizada por un miembro de un gabinete especializado y un 2% que la misma se encuentra a cargo de empleado Instructor de Fiscalía de Instrucción. Finalmente cabe aclarar que en ésta pregunta se registraron cuatro respuestas escritas por los encuestados, que no fueron propuestas en el formulario. Las cuatro respuestas son coincidentes en afirmar que la previsualización es realizada por personal policial comisionado o un secretario de actuaciones en forma alternada.

Figura 9



En la siguiente pregunta se solicitó a los entrevistados que consignaran en qué espacio físico se suele llevar a cabo la previsualización. Ello a los fines de constatar con la información recabada mediantes entrevistas, con qué medidas de seguridad y recursos técnicos cuenta el espacio utilizado.

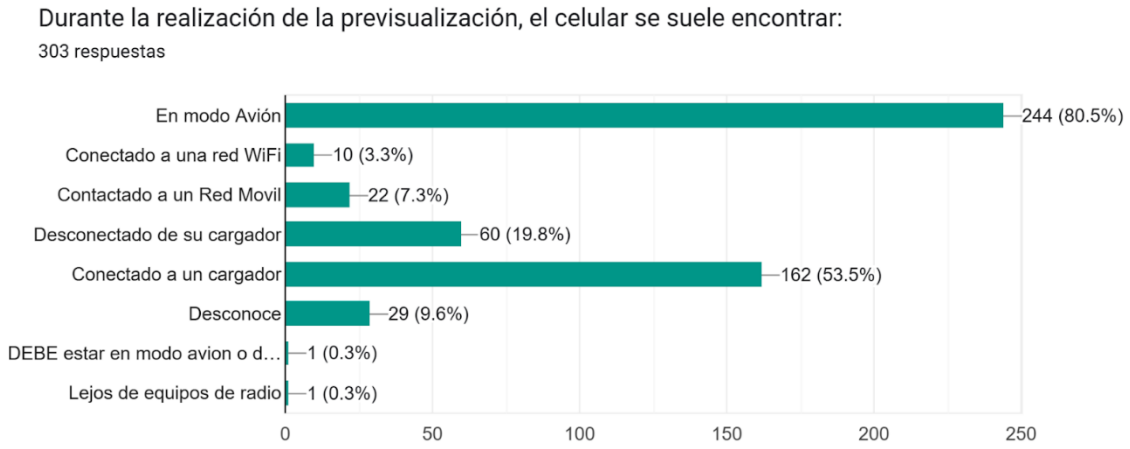
El 70.3% de los encuestados respondió que la previsualización se realiza en una oficina de la Unidad Judicial. El 19.5% manifestó que se realiza en el depósito de una Comisaría, en donde las unidades judiciales generalmente se encuentran edificadas. El 5% respondió que se realiza en una oficina de la Fiscalía de Instrucción y tan sólo el 2.3% respondió que se realiza en un laboratorio de informática forense de la Dirección General de la Policía Judicial. Se obtuvieron tres respuestas escritas por los encuestados que refieren que la previsualización se realiza en la oficina de comisionados, la cual se encuentra dentro de la misma Unidad Judicial.

Figura 10

En la quinta pregunta sobre el modo de realizar la previsualización, se consultó a los agentes si la misma se realiza en un sólo acto o por el contrario en distintos momentos. El 75.2% de los encuestados respondió que la tarea se realiza en varios momentos separados en el tiempo. El 17.2% refirió que se hace en un único acto y el 7.6% manifestó desconocerlo. La pregunta

tuvo como objetivo establecer qué ocurre con el celular entre los momentos en que se realiza la previsualización, en qué condiciones se almacena y por cuánto tiempo.

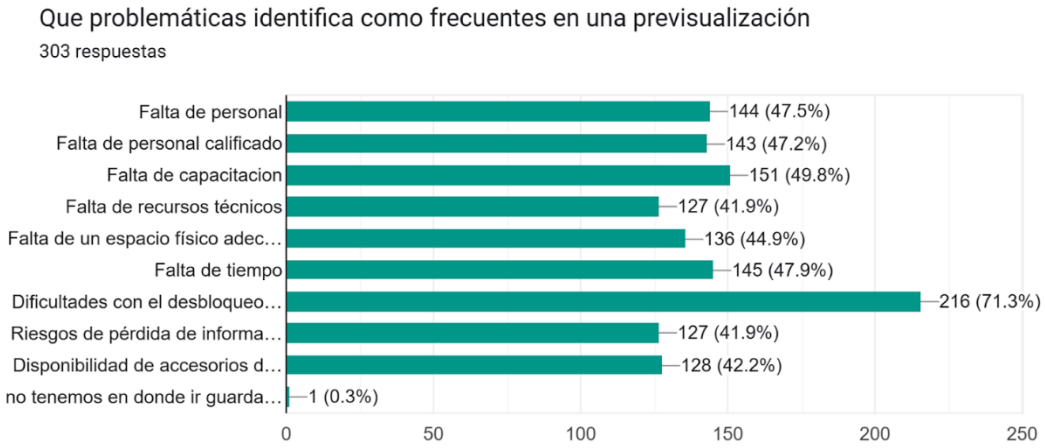
Figura 11



Continuando con la sección específica sobre previsualización, se solicitó a los encuestados que respondan según su experiencia, en qué condiciones se encuentra el celular secuestrado mientras se realiza la previsualización del mismo. El 80.5% de los encuestados respondió que la previsualización se realiza con el celular en modo avión. En contraposición con ésta respuesta, solo el 10% 3.3% respondió que se realiza conectada a una red de WiFi y el 7.3% que se lleva a cabo con el dispositivo conectado a una red móvil. Un 53.5% manifestó que el celular se encuentra conectado a su cargador y el 19.8% que el mismo no se encuentra conectado a una fuente. Tan solo el 9.6% refirió desconocer totalmente las condiciones en las cuales se encuentra un celular mientras se realiza la previsualización del mismo. El objetivo de ésta pregunta fue establecer si existe al menos un nivel de conocimiento mínimo sobre los riesgos de pérdida de la información contenida en un celular durante su manipulación luego del secuestro del mismo.

La conclusión fue positiva, dado que la mayoría de los encuestados refirió que el celular se encuentra en modo avión, lo que disminuye el riesgo de pérdida de información al momento de visualizar la misma. Tan solo el 10.6% (32 encuestados) respondieron que, durante la previsualización de un celular, éste se encuentra conectado a una red móvil o una red Wifi. Situación ésta que, según el análisis de la bibliografía existente, constituye un factor de riesgo de pérdida de información. Habida cuenta de que la encuesta se realizó en base a la experiencia de los encuestados, se puede concluir que en determinadas oficinas, la previsualización de un celular se realiza efectivamente con el celular conectado a una red móvil o WiFi.

Figura 12



La última pregunta, que consistió en casillas de verificación, requirió de los encuestados que respondieran cuáles consideran que son las problemáticas más frecuentes en la realización de una previsualización. El objetivo de la pregunta era establecer el nivel de consciencia existente entre los encuestados, de los riesgos de pérdida de información contenida en un celular, durante la previsualización del mismo, en caso de que ésta se realice de manera incorrecta. Como se observa en la figura 12 incorporada *supra,* se incluyeron numerosas problemáticas, entre cuales se cuenta los riesgos de pérdida de información. El resto de respuestas propuestas constituían problemáticas posibles, pero no estrictamente relacionadas con el objetivo de la presente investigación.

La casilla de verificación que obtuvo mayores respuestas (el 71.3% de los encuestados) fue "dificultades en el desbloqueo del celular". El 47.9% respondió que una problemática frecuente sería la falta de tiempo para realizar la previsualización y el 42.2% respondió que una problemática es la falta de disponibilidad de accesorios, tales como cargadores o auriculares. Éstas tres respuestas, que tienen un marcado tinte operativo al momento de realizar la previsualización, dan cuenta de que la preocupación principal de los encuestados se encuentra dirigida a la obtención de resultados de la previsualización.

El 49.8% manifestó que considera como problemática frecuente, la falta de capacitación del personal que realiza la previsualización de celulares secuestrados. El 47.5% y el 47.2% respectivamente, contestaron que una problemática habitual sería falta de personal y falta de personal calificado. Éstas tres respuestas encuentran relación con la pregunta número 9, en la que la mayoría de encuestados (71.6%) respondió que la tarea de previsualizar un celular, se encuentra a cargo de personal policial comisionado y en menor medida (24.4% de los encuestados) que la tarea se encuentra a cargo de un secretario de actuaciones de la Unidad Judicial. Las respuestas obtenidas en ésta pregunta, dan cuenta de que gran parte de los encuestados considera que tanto el personal policial comisionado como los secretarios de actuaciones, no cuentan con conocimientos técnicos suficientes para realizar una previsualización.

El 44.9% manifestó que encuentran dificultades para realizar una previsualización, respecto del espacio físico dispuesto para ello. Ésto se relaciona con la pregunta número 9, en la cual la mayoría de los encuestados respondió que la previsualización se realiza en una oficina de la Unidad Judicial que se trate. La respuesta evidencia que los encuestados consideran que una

oficina de la Unidad Judicial o el depósito de una Comisaría, es un lugar inadecuado para realizar una previsualización.
Por último, el 41.9% de la población encuestada, respondió que una problemática frecuente son los riesgos de pérdida de información. Ello constituye menos de la mitad de los encuestados, lo que indica que la respuesta propuesta no es una preocupación central entre el personal de las Unidades Judiciales y Fiscalías de Instrucción.

Resultados De Las Entrevistas

En éste segundo momento de la etapa cuantitativa se llevaron a cabo entrevistas a cuatro personas que cumplen funciones como personal policial comisionado en una Unidad Judicial de la Ciudad de Córdoba. La entrevista fue de carácter anónimo, dada la sensibilidad del trabajo que realizan. A los fines de las citas de los resultados obtenidos, se realizó un código de entrevistas que se incorporó como "Anexo 1". La entrevista fue libre, con preguntas abiertas que permitieron un diálogo constante con los entrevistados.
Se solicitó a los entrevistados que comentaran cómo es el procedimiento seguido por personal policial comisionado a una Unidad Judicial al momento del manejo y manipulación de celulares secuestrados en el marco de una investigación.
Del resultado de las entrevistas realizadas, surge que la mayoría de los celulares que se secuestran, son como consecuencia de un allanamiento en algún domicilio particular. Una vez se identifica un equipo móvil que debe ser secuestrado, el mismo se toma del lugar en que se encuentre. En caso de que se pueda identificar quién es el propietario de dicho celular, se le solicita que brinde la clave de desbloqueo o en su caso, que desbloquee el celular, acceda a la configuración del mismo y deje sin efecto la clave. En caso de que el propietario se niegue, el celular permanece bloqueado.
Luego un policía administrativo toma el celular, lo coloca en modo avión y si se encuentra encendido, intenta establecer su número de IMEI mediante la colocación de los dígitos "*#06#". Si se encuentra apagado, lo enciende y realiza el mismo proceso. Luego abre la bandeja de tarjeta SIM y registra el número de IMEI inscripto allí. En el lugar del secuestro no se realiza relevamiento de la información y el celular es trasladado al depósito de una Comisaría, sin medidas de protección particulares. (C.S.-C-E1/13/03/24).
El depósito de las comisarías consta de una habitación cerrada con llave, que no cuenta con aislantes térmicos o de radiofrecuencia. El celular permanece apagado o encendido dentro de una caja, dependiendo del estado en que se secuestró. En caso de que no se ordene una previsualización, el celular es enviado a un laboratorio forense para que realice el relevamiento de los datos. El traslado del celular desde el depósito al laboratorio, es realizado por un policía administrativo, adscrito a la Unidad Judicial que lo lleva en el estado en que se encuentra, sin embalaje ni medidas de protección. (M.T.-C-E1-12/13/24).
La previsualización de un celular se ordena en caso de que se necesite contar rápidamente con la información contenida en el mismo, dado que el informe pericial suele tener demoras de meses. Se solicita a un Juez de Control y Faltas que autorice la previsualización y habiendo obtenido la orden, la realiza un personal comisionado. (M.T.-C-E1-12/03/24).
Para realizar la previsualización, un comisionado retira del depósito de la Comisaría el celular del que se necesite extraer información. En caso de que el celular se encuentre bloqueado, la misma no se realiza porque no se cuentan con elementos para desbloquearlo. Si se encuentra

desbloqueado, apagado y sin batería, el mismo se conecta a un cargador y cuando tiene batería suficiente, se releva la información. Se procede a acceder al celular y luego a las aplicaciones o registros cuya información se requiere para la causa de que se trate. Generalmente se accede a las aplicaciones de Whatsapp, Instagram o Facebook a los fines de observar las comunicaciones que efectuó el tenedor del celular. También se suele ingresar al registro de archivos multimedia. La información se va registrando en un papel, en el celular del comisionado o en el soporte que éste prefiera. Finalizada la tarea, se registra la información relevante en un Acta de Inspección Ocular, la cual se adjunta al expediente, juntamente con una declaración testimonial consignando el proceso realizado. (M.T.-C-E1-12/13/24).

Comúnmente la cantidad de información que debe ser relevada es muy grande, por lo que la previsualización se realiza en varios momentos. En el ínterin, el celular secuestrado es remitido al depósito de la comisaría de que se trate, hasta tanto se pueda retomar la tarea. En ese lapso es común que el celular se quede sin batería y se apague, por lo que hay que cargarlo. (G.R.A.-C-E1-17/03/24).

A los fines de realizar la previsualización de un celular, no se cuenta prácticamente con ningún recurso técnico. No se cuenta con cargador ni auriculares para escuchar los audios. La tarea se realiza generalmente en una oficina de la Unidad Judicial, la cual no cuenta con aislamiento térmico ni de radiofrecuencia. A veces el celular se queda sin batería y se apaga. En las oficinas de las Unidades Judiciales hay computadoras de escritorio que no tienen acceso a internet. Tampoco se cuenta con dispositivos específicos para realizar copias forenses, desbloquear los celulares, preservar la información o ir registrando los datos relevados. Por otro lado, ni la Policía Administrativa ni el Ministerio Público Fiscal brinda capacitaciones sobre el manejo de celulares secuestrados ni la realización de una previsualización. (D.C.-C-E1-15/03/24).

Conclusiones

Del diálogo cuali - cuantitativo producto de la información obtenida durante las distintas etapas del proyecto, surge que el manejo de los celulares secuestrados en virtud de una investigación penal llevada a cabo por el Ministerio Público Fiscal de la Ciudad de Córdoba, carece de un marco regulatorio propio, así como también la realización de una previsualización de dichos celulares. Se desprende que en la manipulación y realización de previsualizaciones de celulares secuestrados, intervienen diversos agentes, ninguno de los cuales cuenta con capacitación suficiente para manipular dispositivos de alta complejidad como lo son los teléfonos inteligentes. Tampoco se observa que se confeccione un documento de cadena de custodia o un registro del personal que manipula un celular secuestrado. Producto de todo ello, se desprende un alto riesgo de pérdida o alteración de la información contenida en los mismos, que podría frustrar una investigación o tornar nulos los datos obtenidos.

Como corolario de la falta de un marco regulatorio o protocolos claros de actuaciones, se evidencia una falta de uniformidad en el tratamiento que se le da a los celulares secuestrados, dependiendo éste, de los usos y costumbres de la oficina que lleve adelante la investigación y los recursos con los que ésta cuente.

Se observó también una marcada carencia de recursos técnicos y humanos para secuestrar, trasladar, almacenar y relevar información de un dispositivo de telefonía celular. Este modo dispar, sin protocolos claros de actuaciones y falta de recursos se encuentran en clara oposición

al modo correcto en que deberían llevarse a cabo las actividades mencionadas. Modo que se encuentra contenido en la norma ISO/IEC 27037 y demás trabajos que fueron analizados.
La disponibilidad de recursos técnicos, tales como herramientas forenses, bolsas Faraday o similares, espacios adecuados de almacenamiento y la implementación de un documento de cadena de custodia, dependen de decisiones políticas y exceden el objetivo del presente trabajo. Pese a ello y aún con escasos recursos, puede mejorarse el tratamiento que se le da a los celulares secuestrados y lograr así una aproximación realista entre el ser y el deber ser, que considere la escasez de recursos técnicos y humanos. Escasez que sin duda limita el accionar de la Policía Administrativa al momento de tomar contacto con un teléfono celular y su correcta manipulación y tratamiento para relevar datos.
Es con esos fines que se esbozó una guía práctica sobre buenas prácticas a la hora de manipular un celular secuestrado, la cual está basada en el "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital" del Ministerio de Seguridad de la Nación Argentina, publicado el 1 de marzo del 2023 y el documento "Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition" publicado por el Scientific Working Group on Digital Evidence (SWGDE) en el año 2020.
Al llegar a la escena y una vez identificado un equipo móvil que se quiera secuestrar, se deberán seguir los siguientes pasos:

a. Si el celular se encuentra encendido, se deberá activar el modo avión para aislarlo de sus redes de conexión. Si puede accederse a la configuración del mismo, y de ser posible, desactivar el bloqueo temporal automático. Se deberá procurar que el celular permanezca encendido y con carga. Se deberá evitar interactuar innecesariamente con el dispositivo, salvo que esto sea requerido por la autoridad judicial. En cuyo caso, se deberán registrar todas las actividades realizadas.

Si el celular se encuentra apagado, no deberá ser encendido. De ser posible, remover la batería del mismo. En caso de que el celular se encuentre inmerso en algún líquido, deberá ser secuestrado en ese estado.

b. Se deberá establecer si el celular tiene una Tarjeta SIM colocada, en cuyo caso, la misma deberá ser extraída para aislar el equipo de redes de telefonía. Se consignará el logo y número de la tarjeta SIM. Para el caso de celulares que tengan dos Tarjetas SIM, registrar ambas y consignar en qué slot de la bandeja se encontraba cada una. Finalmente la tarjeta SIM deberá ser adherida al dorso del celular mediante una cinta adhesiva.

c. Se deberá registrar la marca y modelo del equipo. En caso de que no se pueda establecer a simple vista, consignarlo en el acta de secuestro. En ningún caso se deberá encender un dispositivo apagado para establecer marca o modelo, o reiniciar uno que se encuentre encendido.

d. Se deberá procurar establecer el número de IMEI del celular. En caso de que el mismo no se encuentre inscripto en el equipo o etiqueta de datos, consignarlo de tal manera. En ningún caso se deberá ingresar comandos tales como "#*06#" para acceder al número de IMEI.

e. De ser posible, registrar el número técnico del dispositivo, que puede encontrarse en la carcasa del equipo o en la etiqueta de datos. En caso de no poder dar con dicho número, deberá consignarlo en el acta.

f. De ser posible, se deberá consignar el número de serie del celular, que puede encontrarse en la etiqueta de datos o debajo de la batería (en caso de que la misma sea

extraíble). En ningún caso se deberá utilizar el comando "#*06#" o acceder a la configuración del teléfono para ubicar el número de serie.

g. Establecer si el equipo tiene una tarjeta de memoría colocada. En caso positivo se deberá registrar la marca, modelo y capacidad. En caso de que no posea tarjeta de memoria, consignarlo en el acta. No es necesario retirarla del equipo al momento del secuestro.

h. Por último en el acta de secuestro se deberá consignar el estado general de conservación del teléfono (Bueno, Malo o Regular), procurando detallar los daños y características particulares del equipo (pantalla trizada, pintura desgastada).

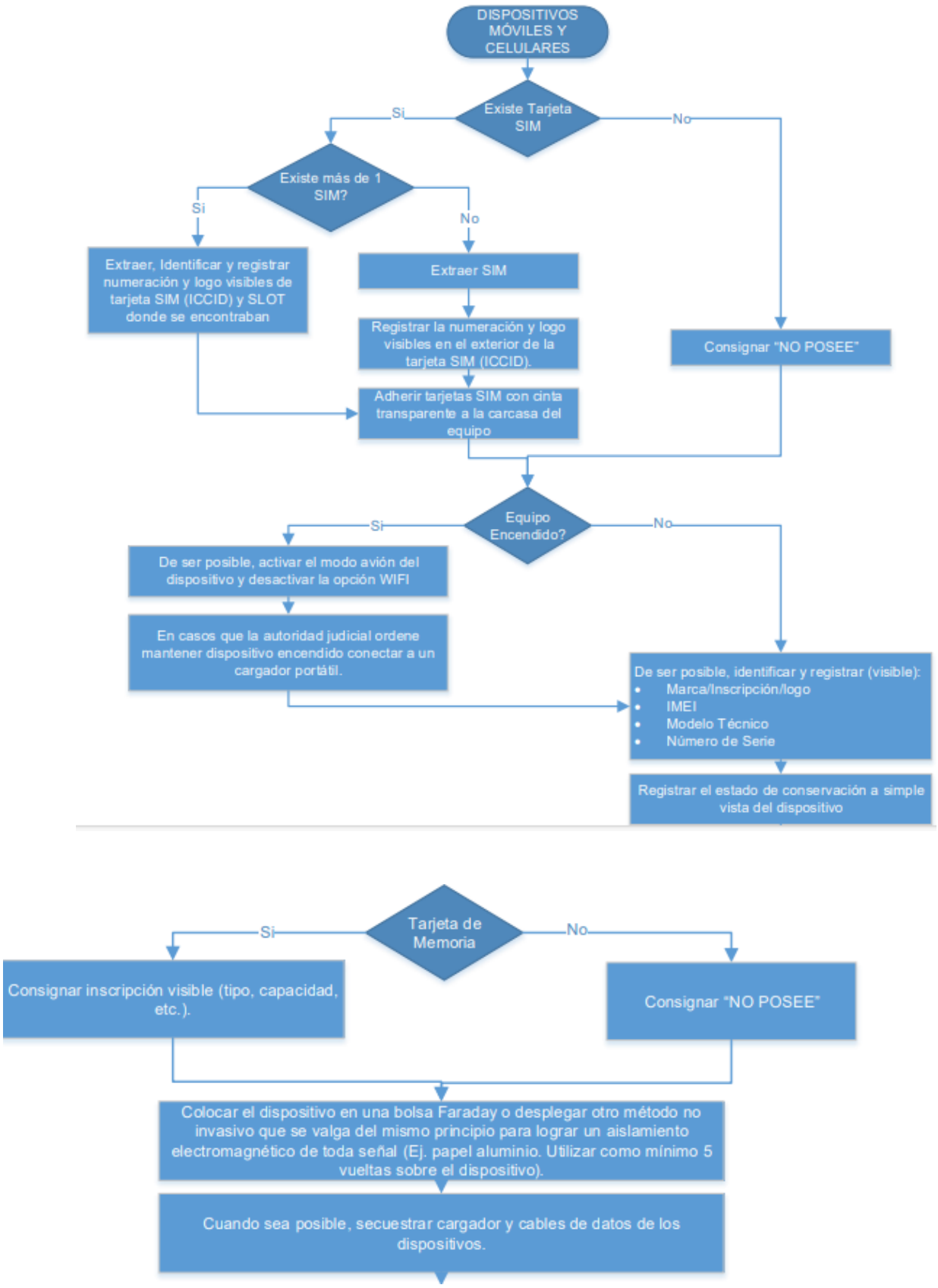
i. Si la autoridad judicial solicita un relevamiento de datos in situ o un triage de dispositivos para establecer la conveniencia del secuestro, se deberán documentar todas las operaciones realizadas sobre el teléfono, ya que las mismas serán registradas por el equipo. Si el equipo se encuentra apagado, deberá ser encendido y mantenido en ese estado. Procurando evitar encenderlo y apagarlo sucesivamente o que el mismo se quede sin batería.

j. En caso de que el tenedor del equipo secuestrado voluntariamente brinde la clave de desbloqueo del teléfono, consignarla en el acta. No se deberá acceder al menú de configuración para retirar la clave. Bajo ninguna circunstancia se deberá requerir al tenedor del teléfono que desbloquee manualmente el equipo, desactive la clave o interactúe con el dispositivo de cualquier forma.

k. Finalizados los pasos anteriores, se deberá aislar el dispositivo de impulsos electromagnéticos, colocándolo en una bolsa Faraday o similar. En caso de no disponer de una, se puede envolver el equipo en papel aluminio. Tener en cuenta que se requieren al menos cinco vueltas de papel aluminio para obtener un aislamiento efectivo. Desde el secuestro y hasta su traslado al laboratorio forense, el equipo deberá permanecer en ese estado.

l. En caso de ser posible, se deberá secuestrar juntamente con el dispositivo, su cargador y cables de datos.

Finalmente se incorpora a continuación un diagrama de flujo ilustrativo, extraído del "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital" del Ministerio de Seguridad de la Nación Argentina.


DISPOSITIVOS MÓVILES Y CELULARES
Existe Tarjeta SIM
Si
No
Existe más de 1 SIM?
Si
No
Extraer, Identificar y registrar numeración y logo visibles de tarjeta SIM (ICCID) y SLOT donde se encontraban
Extraer SIM
Registrar la numeración y logo visibles en el exterior de la tarjeta SIM (ICCID).
Consignar "NO POSEE"
Adherir tarjetas SIM con cinta transparente a la carcasa del equipo
Equipo Encendido?
Si
No
De ser posible, activar el modo avión del dispositivo y desactivar la opción WIFI
En casos que la autoridad judicial ordene mantener dispositivo encendido conectar a un cargador portátil.
De ser posible, identificar y registrar (visible):
Marca/Inscripción/logo
IMEI
Modelo Técnico
Número de Serie
Registrar el estado de conservación a simple vista del dispositivo
Tarjeta de Memoria
Si
No
Consignar inscripción visible (tipo, capacidad, etc.).
Consignar "NO POSEE"
Colocar el dispositivo en una bolsa Faraday o desplegar otro método no invasivo que se valga del mismo principio para lograr un aislamiento electromagnético de toda señal (Ej. papel aluminio. Utilizar como mínimo 5 vueltas sobre el dispositivo).
Cuando sea posible, secuestrar cargador y cables de datos de los dispositivos.

Referencias

1. Cafferata Nores, Jose I. La Prueba en el Proceso Penal 5° edición. Buenos Aires: De Palma 2003.
2. Darahuge, M. E. y Arellano, L. E. (2005). Manual de Informática Forense. Buenos Aires, Errepar.
3. NIST-1 (2014), Ayers, R., Brothers, S. and Wayne, J., Guidelines on Mobile
4. Forensics, SP 800-101 Revision 1, http//dx.doi.org/10.6028/NIST.SP.800-101r1.
5. Ley Orgánica del Ministerio Público Fiscal. Ley 7.826. Córdoba, 20 de septiembre de 1989 Boletín Oficial, 26 de octubre de 1989 Vigente, de alcance general.
6. Código Procesal Penal de la Provincia de Córdoba, Ley 8.123. Córdoba 05 de diciembre de 1991, Boletín Oficial, 16 de enero de 1992. Vigente, de alcance general.

Bibliografía

a. Cafferata Nores, Jose I. La Prueba en el Proceso Penal 5° edición. Buenos Aires: De Palma 2003.

b. Ruben A. Chaia (2010). La prueba en el proceso penal. Buenos Aires, Hammurabi.

c. Darahuge, M. E. y Arellano, L. E. (2005). Manual de Informática Forense. Buenos Aires, Errepar.

d. Di Iorio (Dir.) (2017). El rastro digital del delito. Mar del Plata: Universidad FASTA.

e. Di Iorio, (2016) Guía Integral de Empleo de la Informática Forense en el Proceso Penal, Universidad Fasta.

f. Forensics, SP 800-101 Revision 1, http//dx.doi.org/10.6028/NIST.SP.800-101r1.

g. Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012.

h. Hernanez Sampieri, Roberto. Metodología de la Investigación. Sexta Edición. 2014

i. Ministerio de Seguridad de la Nación. Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital.

j. L. S. Gómez "Protocolo de Actuación para Pericias Informáticas". Poder Judicial de la Provincia de Neuquén.

k. L. S. Gómez, "Pericias informáticas sobre telefonía celular" Poder Judicial de la Provincia de Neuquén.

l. NIST-1 (2014), Ayers, R., Brothers, S. and Wayne, J., Guidelines on Mobile

m. Sergio Gomez Bastar. Metodología de la Investigación, 2012.

n. SWGDE, 2020. "Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition"

o. SWGDE, 2020. "Best Practices for Mobile Device Forensic Analysis".

Anexo 1. Código de entrevistas

Nombre Codificado	Episodio	Fecha	Función/Rol
M.T.	E1	12/03/24	C (comisionado)
C.S.	E1	13/03/24	C (comisionado)
D.C.	E1	15/03/24	C (comisionado)
G.R.A.	E1	17/03/24	C (comisionado)