“CREACIÓN Y PRESERVACIÓN DE EVIDENCIA EN DELITOS VINCULADOS CON LAS TIC´S”

Maria Alejandra Juana Hillman, Arsenio Antonio Cardone y Gustavo Jose Guayanes
Miembros del Poder Judicial de Córdoba – Ministerio Público Fiscal – Policía Judicial – Sección Informática Forense
acardone@justiciacordoba.gov.ar

Abstract: La obtención y preservación de evidencia dentro de un proceso penal coadyuvan a la investigación para dar base a la acusación o determinar el sobreseimiento del supuesto autor del delito. Por lo tanto, los elementos vinculados con tecnologías de la información y comunicación a recolectar, en el trabajo de campo y de laboratorio, poseen características que requieren un pronto accionar y tratamiento. No disponiendo de un marco legal específico que reglamente la forma de proceder, la heterogeneidad de los escenarios tecnológicos que impiden trazar un límite ciertamente definido y la imposibilidad de aplicar técnicas forenses tradicionales; genera desafíos. Debiendo además, utilizar herramientas y maniobras que en principio no fueron concebidas para uso forense y apelar a la aplicación de buenas prácticas; para poner la evidencia obtenida a disposición de la investigación. Demostrando la diversidad de medios tecnológicos (ordenadores, dispositivos móviles, mails, cámaras fotográficas/filmadoras, archivos electrónicos, sitios de internet, redes sociales, otros) que puede participar en dicha labor, en distintos escenarios y su incidencia al momento de la creación y preservación de la evidencia.

Keywords: TICs-Móviles-Forense-Informática-Casos Prácticos-Córdoba

1 Introducción

El presente trabajo se desarrolla dentro del marco de la experiencia adquirida por los autores en escenarios de campo o lugares de un suceso y en el laboratorio, sobre dispositivos informáticos, sistemas en general, dispositivos móviles, sitios de internet, cuentas de correo electrónico del tipo corporativo y/o de acceso público, redes sociales, entre otros elementos; desde el año 1998 de acuerdo a las funciones establecidas en la Ley 8123 - Código Procesal Penal de la Provincia de Córdoba, en su art. 321[1] para la

[1] Artículo 321 - Función. La Policía Judicial por orden de autoridad competente o, en casos de urgencia, por denuncia o iniciativa propia, deberá investigar los delitos de acción pública, impedir que los cometidos sean llevados a consecuencias ulteriores, individualizar a los culpables y reunir las pruebas útiles para dar base a la acusación o determinar el sobreseimiento. Si el delito fuere de acción pública dependiente de instancia privada, sólo deberá proceder cuando reciba la denuncia prevista por el artículo 6.

Dirección General de Policía Judicial de Córdoba[2], dependiente del Ministerio Público Fiscal de Córdoba[3] específicamente en el Fuero Penal.

Al cabo de ese período de tiempo, se pudo observar el comportamiento creciente en la demanda del servicio de justicia, con relación a la evolución tecnológica vinculada a aspectos socio-económicos.

Inicialmente los elementos motivo de análisis que ingresaban y tenían relación con la concreción de un hecho delictivo, estaban claramente diferenciados desde el punto de vista tecnológico en base a la función específica que cumplían, ejemplo, una computadora habitualmente no estaba integrada a una red, una cámara fotográfica y una fotografía, una cámara filmadora y un video, un equipo de audio y el material vinculado, eran objetos aislados entre si.

Conjuntos de elementos de hardware (ejemplo: Placas digitalizadoras de audio, de video) y software (programas para conversión de formatos), permitían la conversión de formatos mientras crecía con ello el protagonismo de las PC's (computadoras personales).

Mientras tanto, el desarrollo de las empresas prestatarias en servicios de telefonía fija y móvil, generó un avance en las comunicaciones con la incorporación de la telefonía celular y las conexiones dedicadas a internet[4], cobrando protagonismo las redes departamentales con acceso a éste último recurso tecnológico.

La vigencia de normas internacionales en distintas regiones del mundo como las FCC[5], UL[6], ANSI[7], aplicadas en la fabricación de cualquier artefacto, como la estandarización de formatos en sistemas de archivos; provocó de forma casi explosiva la masificación del uso de la tecnología. Que en forma gradual incorporaron las organizaciones irrigándose al uso doméstico.

El fenómeno de penetración del uso de la red internet y las telecomunicaciones, aceleró dicho proceso, desencadenando en una integración de tecnologías, volviéndose en muchos casos complejo su análisis de modo particular.

Desencadenando en la actualidad, en aparatos en su mayoría electrónicos y otros electromecánicos, con capacidad de procesamiento, almacenamiento y comunicación; de manera integrada.

Entonces, se pretende desarrollar las adecuaciones en las prácticas forenses para la creación y preservación de evidencia vinculadas a las TIC's[8], en dicho marco de desarrollo, sin descuidar el marco legal inespecífico a la actividad. Evitando la nulidad de la prueba.

[2] http://www.justiciacordoba.gov.ar/site/Asp/PoliciaJudicial.asp y Art.321 del C.P.Penal
[3] http://www.mpfcordoba.gov.ar/institucion_info_instituc.html
[4] Es un conjunto de redes de ordenadores a nivel mundial
[5] http://www.fcc.gov/
[6] http://www.ul.com/argentina/spa/pages/
[7] http://www.ansi.org/
[8] http://es.wikipedia.org/wiki/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_la_comunicaci%C3%B3n

2 Características Generales

En las intervenciones de campo el escenario es incierto hasta el momento de su abordaje, en escasas oportunidades, el personal técnico conoce de antemano la infraestructura y elementos que se van a encontrar para su análisis y que contribuya a la búsqueda de la verdad real.

Es común en el ámbito del Fuero Penal identificar al allanamiento como el trabajo de campo por excelencia; no obstante, existen otras acciones que forman parte de la actividad y de igual modo constituyen labores que se identifican con esta clasificación, ello son los "relevamientos in- situ" o colaboraciones técnicas que se aplican métodos de identificación, recolección y generación de evidencia idénticos a los que se utilizan en un allanamiento, dentro de lo que se denomina investigación penal preparatoria cobran relevancia, y tienen como objeto contribuir a distintas líneas investigativas propuestas.

En la mayoría de las oportunidades en las que se convoca a personal técnico a brindar su asistencia en un trabajo de campo, al inicio del mismo se conocen pocos datos elementales de la causa, instrucciones poco precisas y ausencia de un alcance concreto que permita establecer las cotas o referencias de trabajo.

De todos modos, sea cual fuere la modalidad para la intervención de campo, la incorporación de la prueba por parte del especialista debe estar sujeta a derecho para su introducción en el proceso como tal.

Si bien en laboratorio, las condiciones técnicas, tecnológicas y ambiente de trabajo son mas favorables frente a las que se pueden encontrar en el trabajo de campo, de igual manera en ese escenario no se conocen aspectos puntuales sobre la causa que permitan establecer métodos y procesos forenses específicos, existe además, disparidad en la aplicación de la terminología jurídica con la técnica.

La lógica evolución y recambio de generaciones tecnológicas en exiguos períodos de tiempo, obligan a constantes desafíos que no siempre acompañan a la diversidad de la misma, esto lleva consigo a mayores capacidades de almacenamiento, cantidad de conectores, de elementos interrelacionados a tener en cuenta al momento de su análisis; que ponen a prueba al perito en su labor de obtención y aseguramiento de la evidencia. Debiendo el perito resolver técnicamente y optar conforme a las circunstancias, cual es la mejor alternativa a implementar, sin descuidar en ningún momento los recaudos legales para que la evidencia recolectada sea sustentable en la causa.

Situaciones como Phishing[9], Pharming[10], ataques con botnet[11]s, ponen a prueba los postulados de territorialidad, la asimilación de mail, contactos (de mail y dispositivos móviles), agendas electrónicas (de mail y dispositivos móviles) como correo epistolar, procedimentalmente hablando en muchas oportunidades introducen medidas dilatorias que conspira con la característica de volatilidad de esta clase de evidencia. Y cuando se investigan delitos de instancia privada donde están involucrados damnificados menores de edad, la legislación de cada país define la edad a partir de la cual una persona obtiene la madurez sexual, hace que en un país se lo persiga al supuesto autor mientras que en otro con un valor sustancialmente mas bajo puede no penalizarlo.

4 Consideraciones Jurídicas

Algunas reflexiones sobre la necesidad de marco legal para la obtención, creación, admisibilidad , cadena de custodia , y preservación de la evidencia digital:

La evidencia digital - entendida ésta tanto como objeto de derecho constituido por datos expresados en formato electrónico o como la representación de hechos o actos jurídicos relevantes efectuado en formato digital-[12] requiere de una mirada tecnológica para entender la característica de los medios utilizados y un análisis técnico jurídico que nos dirá como obtener, presentar, interpretar, la prueba y cómo relacionarla con los hechos o actos jurídicos en el juicio.

En materia procesal penal, en Córdoba, el CPP no regula específicamente sobre la evidencia digital , aunque alguna de sus normas admiten el uso de medios digitales para determinadas circunstancias.

El principio de libertad probatoria en la investigación penal Art. 192 del CPP admite la posibilidad de su utilización salvo prohibición expresa por la ley y en los casos de exclusión probatoria (Art. 194 CPP) .- En este supuesto tanto el Fiscal a cargo de la investigación como el Juez tiene permitido la ponderación de otros medios de prueba no contemplados específicamente en la normativa que tratamos, posee la facultad de admitir, ordenar, valorar e interpretar distintos elementos a fin de lograr su convicción sobre los hechos alegados por las partes.

En el curso de la IPP existen determinados procedimientos que implican la utilización de operaciones técnicas (Art. 201 CPP) cuando para mayor eficacia de las inspecciones y reconstrucciones se pueden ordenar todas ellas científicamente

[9] Una modalidad de engaño cibernético, con el objeto de capturar datos personales y con ellos obtener usufructo

[10] Mecanismo de redireccionamiento de dominio, empleado también para capturar datos personales y con ellos obtener usufructo

[11] http://es.wikipedia.org/wiki/Botnet

[12] Rivolta Mercedes: en IV Congreso Argentino de Admnistración Pública en Buenos Aires 2007- pnencia " Medios de prueba electrónicos: estado de avance en la legislación argentina"

convenientes. Además de autorizarse (Art. 213 CPP) la obtención de copias, o reproducciones de las cosas secuestradas cuando éstas puedan desparecer, alterarse, sean de difícil custodia o así convenga . Por otra parte se autoriza la Intercepción de la correspondencia (Art. 214 CPP) sea esta postal o " telegráfica o de todo efecto remitido por el imputado o destinado al mismo, aunque sea bajo nombre supuesto". Asimismo la Apertura y examen de correspondencia y su secuestro (Art. 213 CPP) donde hace mención a la correspondencia o efectos interceptados. También y mas específicamente el art. 216 del CPP regula la intervención de comunicaciones del imputado " cualquiera sea el medio técnico utilizado, para impedirlas o conocerlas".-
Asimismo en relación a determinadas victimas o testigos, la utilización de medios técnicos se haya expresamente contemplada - art. 221 bis CPP- en tanto las alternativas del acto pueden ser seguidas"...a traves de vidrio espejado, micrófono, equipo de video o cualquier otro medio técnico con que se cuente..." y debiendo con posterioridad al defensor imponérsele y posibilitarle el acceso al informe, acta "constancias documentales o respaldos fílmicos del acto..." los que posteriormente son incorporados y elevados para su merituación correspondiente durante el juicio propiamente dicho, evitando la revictimización de los menores al no exigirse su comparecencia.

Otros Códigos procesales como el de La Nación, establece la libertad de prueba (Art. 206), asegurando que no rigen las limitaciones establecidas por las leyes civiles, salvo las relativas al estado civil de las personas. Se admiten a pedido de parte o de oficio por tanto el aporte de evidencia digital, la cual NO ESTA PROHIBIDA. Sería equiparable a la prueba documental. A su vez en el art. 224 admite el uso de medios electrónicos, cuando autoriza la comunicación de la orden de allanamiento en caso de urgencia a su través.

El CPP más avanzado en Argentina respecto a contemplar expresamente la evidencia digital es el de Chubut.- Parte del principio de libertad probatoria (Art. 165) y contempla específicamente el uso de medios electrónicos para producir prueba . Ej: art. 210 regula el reconocimiento de personas o cosas a traves de medios técnicos. El art. 169 en uso de medios técnicos para reconocimientos, reconstrucciones, registros, requisas, inspecciones y allanamientos. El art. 129 respecto a la documentación señala que los actos deberán registrarse de modo que se garantice fidelidad, acceso, conocimiento posterior y posibilidad de reproducción por escrito en papel o en sistemas de información computarizados, imágenes o sonidos. La documentación de actos por imágenes o sonidos sólo podrá adoptarse mediante sistemas que impidan su alteración posterior, y en tales casos se consignará la ratificación de todo lo actuado en un documento que así lo exprese. Admite el uso de grabaciones (Art. 131) imágenes y sonidos o grabaciones digitalizadas para documentar total o parcialmente actos de prueba o audiencias. A tal fin, prohíbe toda forma de edición, tratamiento o modificación de los registros, e impone la obligación de asegurar su autenticidad e inalterabilidad.

Es notable que todas las disposiciones mencionadas se apoyan en el concepto de equivalente funcional, sin mencionar la tecnología específica aplicable, acorde con las modernas tendencias internacionales , permitiendo mantener un conjunto de normas procesales actualizadas.

Por otra parte, podemos afirmar que respecto a las animaciones computadas y simulaciones - su aceptación en juicio el CPP de Chubut en su art. 131 lo autoriza expresamente para documentar total o parcialmente actos de prueba o audiencias, siempre prohibiéndose toda forma de edición tratamiento o modificación de los registros, asegurándose su autenticidad e inalterabilidad.- Igualmente en el supuesto de nuestro CPP 221 bis, que podrá ser presentado durante el juicio habiendo gozado del contralor estricto de la defensa en su producción.

El Fiscal o Juez puede ordenar otros mecanismos a utilizar en concepto de medidas pertinente y útiles a la investigación y/o el juicio propiamente dicho. Así como el CPP de la Nación en su art. 475 autoriza al juez , a ordenar a pedido de parte o de oficio la ejecución de reproducciones fotográficas , cinematográficas o de otra especie, de objetos documentos o lugares, con empleo de medios o instrumentos técnicos . La realización de exámenes científicos necesarios para el mejor esclarecimiento de los hechos controvertidos, y en la reconstrucción de hechos, para comprobar si se han producido o pudieron realizarse de una manera determinada.

En la Argentina, como en otros países de latinoamérica – Ecuador por ejemplo[13]- no se ha formalizado una guía o manual con relación a la ED de admisibilidad de la misma, o manejo de la prueba, esto es para la obtención, presentación y valoración de la evidencia digital, reservándose al criterio de los operadores judiciales, o peritos, siempre que se respeten los requisitos mínimos de seguridad, autenticidad, integridad y confidencialidad.

Existen trabajos en nuestro país disponibles como la " Guía operativa en procedimientos judiciales con secuestro de tecnología" de Leopoldo Sebastián Gómez[14] y reciente elaborada y presentada para su aprobación por ante la Fiscalía General de la Provincia de Córdoba (Diciembre 2010) Pautas Informativas y Procedimentales en Ciberdelitos"- con la finalidades de garantizar la legítima obtención o creación , el buen manejo, análisis y preservación de la evidencia digital durante el transcurso de la investigación penal preparatoria.-

Es trascendente concretar la difusión de dicho material de abordaje de la evidencia digital, a todos los operadores jurídicos y personal policial que intervenga en la investigación de los delitos, a fin de legitimar a ésta como prueba, formadora de convicción judicial, y lograr el afianzamiento de la justicia mediante el justo castigo al sujeto traído a proceso como responsable del ilícito, en su caso.

[13] La Fiscalía General del Estado posee el "Manual de manejo de evidencias digitales y entornos informáticos, procedimientos de operaciones estandart" de Santiago Acuario Del Pino 8.12.2009 – ver en ISUU 29 de enero 2011 DRAGONJAR.

[14] Ver en AR Revista Derecho Informatico en Alfa –redi N° 095 Junio del 2006

5 Casos prácticos sobre sistemas de información y dispositivos informáticos

Es un caso de "Estafa", el cual fue perpetrado mediante el uso de una aplicación[15], valiéndose de una atribución que disponía un empleado de una organización acorde a su función, le permitió autorizar el pago de una suma de dinero, en forma indebida a favor de una determinada persona connivente.

Una vez constatado el desapoderamiento y la maniobra, se solicita colaboración para establecer el autor de la maniobra y desde donde lo había realizado.

El relevamiento de campo determinó que se empleo un sistema de información que funcionaba en cuatro provincias de Argentina, pero que a su vez se utilizaba en otras ciudades de países limítrofes. Estableciendo en base a logs, que la maniobra se había realizado en una provincia del norte de la república Argentina, y que para determinar el origen de la transacción se debía analizar los registros (logs) de la empresa prestadora del servicio, que solo poseía administración del mismo en cada país donde funcionaba, pero los registros estaban alojados en la casa matriz la cual se encontraba en un país limítrofe.

Entonces, considerando la propiedad de volatilidad de esa clase de evidencia, se instrumentó el envío de un oficio hacia la casa matriz, solicitando puntos específicos necesarios para establecer el usuario que realizó la operación.

El análisis conjunto del resultado del trabajo de campo en una de las sucursales en república Argentina, en una oficina representante del sistema de información en Argentina, los registros aportados por un técnico en el transcurso del trabajo de campo y registros aportados desde la casa matriz, permitió construir la evidencia para demostrar que usuario y desde donde se efectuó la transacción.

La evidencia obtenida se conformó de fojas impresas y archivos electrónicos aportados en CD's en dos ejemplares idénticos.

Considerando en este caso al CD como un medio idóneo de solo lectura que impide la modificación de su contenido (según la forma de grabación) y la cantidad "dos" ejemplares[16] representa una adaptación de buenas prácticas forenses y del Código Procesal Civil y Comercial de la Nación en el inciso 6 del artículo 125, que trata sobre la grabación fonográfica de las audiencias de prueba, bajo determinados requisitos. La decisión respecto de la posibilidad de utilizar esta tecnología es del Tribunal, debiendo realizarse en dos ejemplares, uno que se

[15] Análogo a sistema de información

[16] www.asociacionag.org.ar/pdfcap/4/Rivolta,%20Mercedes.doc

certifica y queda en el juzgado y el otro para consulta de las partes. Lo que resulta una adaptación a la labor forense para la presentación de evidencia.

Tal como se señaló anteriormente, este ejemplo técnico plantea un nuevo paradigma en cuanto a la territorialidad de los hechos y el lugar donde se recolecta la evidencia.

El siguiente ejemplo tiene vigencia tanto en un allanamiento como en laboratorio.

Cuando se somete a búsqueda de vocablos, empleando técnicas forenses, por ejemplo mediante el uso de editores hexadecimales[17] o sobre imágenes forenses[18], y algunas coincidencias se encuentran en mails, archivos de agendas o contactos, se imprime contenido de aquellas coincidencias que no es ninguna de esas situaciones hasta tanto no se disponga de la autorización pertinente de un juez.

Se plantea dicha situació, pues la intención al momento de recolectar evidencia es ponerla a disposición de la investigación con la mayor celeridad posible. Pudiendo citar como ejemplo de prontitud extrema un caso de "Secuestro Extorsivo".

En este ejemplo se presenta una creación de evidencia partiendo de un archivo de evidencia forense. Significa, que habiendo obtenido el archivo de evidencia forense del contenido del disco rígido y en función de las coincidencias obtenidas, se recuperan los archivos "notables[19]" para la investigación.

Estos archivos en si, conforman evidencia digital resultante del archivo de evidencia forense obtenido del disco rígido. A los mismos se calcula valor de hash[20] (MD5[21], SHA1[22], SHA2[23]) y se resguardan en CD/DVD en dos ejemplares idénticos; de igual modo que el ejemplo anterior.

Toda esa maniobra es destreza del perito, adecuando las herramientas para lograrlo conservando los postulados forenses de inalterabilidad de la evidencia.

Una dificultad que se presenta en la mayoría de los delitos de instancia privada, es la identificación de las víctimas menores de edad vinculadas al mismo,

---

[17] Programa informático diseñado para editar sectores de datos, que permite ver datos que de otro modo están ocultos.

[18] Copia bit a bit de un almacenamiento de datos

[19] Valores encontrados con relevancia para el hecho que se investiga.

[20] Algoritmo que calcula en función de un flujo de bits un valor numérico fijo.

[21] Algoritmo para obtener valor de hash de 128 bits empleado en mecanismos criptográficos e integridad de archivos

[22] Algoritmo para obtener valor de hash de 160 bits empleado en mecanismos criptográficos e integridad de archivos, mas seguro que MD5.

[23] Algoritmo de características parecidas a SHA1 que mas complejo.

como así también aquellas que según la legislación en la república Argentina no debe superar los dieciséis años.

Independientemente de las apreciaciones subjetivas a fin de determinar ese rango de edad, lo importante es contar con la colaboración de personal abocado a la investigación, que conoce sobre la misma y sus actores. Este desarrollo sirve como aclaración a la hora de construir la evidencia.

Por ejemplo para aportar el material fotográfico o fílmico estrictamente vinculante a la causa. Caso contrario la forma de presentación de la evidencia se vuelve una labor muy extensa y poco comprensible.

El volumen de archivos de fotografía digital que se puede encontrar el muy extenso. Si se pretende aportar de manera impresa el contenido de fotografías para incorporar en el expediente, demanda elevadas cantidades de insumos (papel, toner o tinta). Y en el caso de archivos de video digital, si se adopta la misma forma de trabajo, solo se podrá aportar una impresión de un filmograma por vez.

A su vez, que se aporte en otro soporte adicional en CD/DVD en dos ejemplares idénticos, los mismos archivos.

6 Casos prácticos sobre dispositivos móviles

Para el caso de los dispositivos móviles[24] empleados como medio para cometer un hecho delictivo, por la experiencia recogida, en un alto porcentaje de las causas recibidas se refiere a delitos contra la propiedad, el resto, se observa en delitos contra las personas, escasas oportunidades se ha establecido un vínculo con delitos que a la fecha han sido modificados por la Ley 26388, como la denegación de un servicio en el Artículo Nº 184 de C.P.

Conforme a ello, en todos los casos, la información primigenia deviene de relevar las características específicas y constructivas del dispositivo, marca, modelo, número de serie, aspectos técnicos especiales, conexión con una red de trabajo o no, en este último caso, será importante conseguir por relevamiento físico de la identificación unívoca del dispositivo para determinar su operación en el momento de interés para la causa.

Dirigiendo el enfoque hacia dispositivos móviles con conexión a una red de telefonía inalámbrica con un ámbito territorial determinado y circunscrito al interés propio de la causa, es muy importante establecer parámetros que garantizarán unívocamente la relación o no del dispositivo con el escenario en el cual se ha llevado a

[24] http://es.wikipedia.org/wiki/Dispositivo_m%C3%B3vil

cabo un delito, esos parámetros son el I.M.E.I.[25] del equipo y el número de tarjeta S.I.M[26]., ambos, determinan que un número de abonado (SIM) ha efectuado transacciones de información con un determinado dispositivo (IMEI), ello se consigue en virtud que el sistema de alcance global de las telecomunicaciones móviles denominado G.S.M.[27] al iniciar una sesión de inicialización al dispositivo, le exige que el mismo se identifique antes de recibir el servicio de comunicación, mediante el envío de un conjunto de datos hacia el controlador central de la red. Toda esta información será útil para obtener además de los datos administrativos del servicio, transacciones de mensajes de texto, registros de llamadas entrantes y salientes, con ubicación geográfica dentro del radio de cobertura de la antena que permitió el servicio de comunicación con un terminal de la red propia o de otra, dentro del mismo ámbito geográfico nacional o internacional, en éste último sólo se podrá ubicar al emisor o al receptor, en cambio en el otro caso ambos pueden ser localizados con el rango de cobertura de la antena sólo para comunicaciones de voz, en el caso de mensajes de texto sólo se guarda los números de abonado pero no el contenido.

La información contenida en un dispositivo puede agruparse en los siguientes estratos perfectamente diferenciados, agenda almacenada en tarjeta SIM y dispositivo, mensajes de texto enviados y recibidos, con datos de número de abonado y contenido existente en la tarjeta SIM y dispositivo, imágenes propias tomadas con el dispositivo o de terceros recibidas y/o almacenadas en el dispositivo y/o tarjeta de memoria tipo flash, filmaciones propias tomadas con el dispositivo o de terceros recibidas y/o almacenadas en el dispositivo y/o tarjeta de memoria tipo flash, recordatorios existentes en la agenda del dispositivo, información contenida en grabaciones de voz tomadas con el mismo dispositivo o recibidas y/o almacenadas en el dispositivo y/o tarjeta de memoria tipo flash.

Desarrollo de situaciones:

Para el caso de los dispositivos móviles a operar en el trabajo de campo se deben tener en cuenta los siguientes ítems:

1. Observar señales características externas del mismo (ej. visor con daños, golpes, marcas, stickers, presencia de funda, otros).
2. Observar la operatividad del dispositivo.
3. Recabar de algún modo si el dispositivo tiene contraseña fijada por el usuario del mismo, en caso positivo se deberá tomar nota de la misma para luego colocarla en el acta que reflejará las acciones llevadas a cabo en el trabajo de campo.

[25] del inglés International Mobile Equipment Identity, en español Identidad Internacional de Equipo Móvil

[26] del inglés Subscriber identity module, en español módulo de identificación del suscriptor

[27] Sistema global para comunicaciones móviles. Soporta voz, datos, mensajes de texto y rouming en varios paises.

4. Una vez cumplimentado el punto anterior, mediante los mandos del teclado se presiona la secuencia numérica *#06#, sobre la pantalla se observará el número de IMEI con el cual se encuentra programado el dispositivo.
5. Luego se desmonta la tapa posterior del dispositivo junto con la batería, se toma nota del número de IMEI colocado en el stiker de identificación existente en el habitáculo de la batería.
6. La numeración del punto 4 y 5 deben coincidir atento a que en el ámbito mundial el número de IMEI es único para un único dispositivo, si no coinciden se hará constar.
7. Si como trabajo se ha encargado sólo el secuestro de material para su posterior análisis en laboratorio, toda la información recabada hasta el momento se plasmará en el acta respectiva y posterior remisión a la instancia requirente, la que si resulta necesario solicitará previa autorización al Juzgado de Control que corresponda por jurisdicción.
8. Si es necesario se coloca nuevamente batería y tapa posterior del dispositivo en el lugar que le corresponde, en este punto es muy importante contar con una bolsa de faraday que impida la acción del dispositivo con la red del prestador, una vez inserto en la misma, se inicia ciclo de encendido mediante la presión de la tecla identificada como tal, luego de completar la secuencia, sobre el visor se observará el fondo correspondiente a la pantalla principal y si no un cuadro de diálogo que exige el ingreso de un código PIN, de la tarjeta SIM o del dispositivo, en el primer caso, se deberá requerir a la empresa prestataria del servicio el código de desbloqueo PUK1, cual permitirá reiniciar por una secuencia numérica conocida, para continuar con el encendido, de igual manera se puede repetir la misma situación fondo de pantalla principal o cuadro de diálogo que permite el código personal de usuario, éste puede permitir miles de combinaciones, siendo éste último caso difícil de obtener por fuerza bruta.

9. Una vez transcurrida la inicialización del dispositivo, se comenzará explorar con el mayor cuidado posible los contenidos del menú, para acceder a sus distintas partes con la máxima precaución de no alterar por ninguna situación el contenido. En este punto resulta importante relevar el horario del dispositivo y su ubicación respecto del UTC[28] ya que para la investigación puede resultar primordial ese dato para fijar el tiempo de ejecución del hecho.
10. Como el dispositivo se encuentra aislado inalámbricamente, es factible efectuar un relevamiento de la información empleando aparatología existente en el mercado y diseñada con estos fines pero respetando el concepto “forense”, del cual se desprende generalmente una serie de archivos electrónicos fabricados por el dispositivo que permite el relevamiento de la información o bien si éste no es

[28] Coordinated Universal Time, en español Tiempo Universal Coordinado

compatible con el dispositivo, toda la información deberá transcribirse registro por registro y de una manera ordenada en el contexto que corresponda por formalidad.

Dentro de cualquier contexto legal, la evidencia tiene igual tratamiento en las acciones a tomar por parte del técnico en el ámbito del laboratorio, independientemente si el material ha intervenido personal capacitado o no durante las acciones que llevaron a la incautación del material aportado para estudio; para el primer caso, se han respetado los ítems enunciados anteriormente desde el punto uno al siete, y se procede a continuación con el desarrollo del resto de los puntos, ocho, nueve y diez, la información resultante, se plasmará en el contexto de un informe si corresponde a registros transcriptos por métodos de observación en visor en forma directa, si se contempla el uso de métodos asistidos por hardware y/o software forense, el resultante de las acciones pueden ser conjuntos de archivos con extensiones propias (ej, jpg, jpeg, mpeg, 3gp, otros), sumados a un archivo que contiene el resto de la información almacenada en el dispositivo.

Todo el conjunto se aporta como prueba de la siguiente manera:

1. Para el caso del contenido referente a mensajes de texto, registros de llamadas (entrantes, salientes, perdidas), citas de agenda como evento recordatorio, agenda de contactos, en el caso de los primeros, se asemejan a contenido epistolar o papeles privados cuyo contenido para ser incorporado a un proceso se encuentra protegido por leyes nacionales[29], provinciales[30], por lo que es motivo de nulidad si esta acción no está autorizada por Autoridad competente, para el resto de los registros su mera trascripción es válida para el proceso.
2. Si de análisis del dispositivo surge la existencia de archivos multimedia (fotografías tomadas con el dispositivo o existentes en el mismo, conversaciones grabadas con el dispositivo o existentes en memoria, filmaciones grabadas con el dispositivo o existentes en memoria), se colocan en una carpeta que identifica al informe o pericia, y dentro de la misma se agrupan los archivos en una carpeta con el nombre de la ruta en la que se encontraba originalmente. Todo este material se graba en idénticas copias si corresponde en disco compacto, dvd, o múltiples copias de cada uno, según el volumen total del contenido, se identifica en forma externa cada uno de los ejemplares en relación al número total.
3. De igual manera se procede que en el punto anterior con los archivos resultantes del análisis de un dispositivo mediante hardware y/o software forense, la carpeta que aglutina a los mismos se colocan en sendos ejemplares idénticos en

[29] Constitución Nación Argentina, Art. 18
[30] Código Procesal Penal de Provincia de Córdoba, Art. 215. Constitución Provincia de Córdoba Art. 46

soporte CD o DVD, siguiendo los mismos procedimientos de identificación enunciados.

Lo enunciado hasta aquí corresponde a situaciones que son homogéneas en el tratamiento de los dispositivos móviles, pero es común que se comporten de manera heterogénea, de modo tal que ciertos ítems pueden ser obtenidos por una combinación de métodos, empleando el hardware y software forense en conjunto con la trascripción literal de los contenidos desde el visor del dispositivo, y en algunos casos poco frecuentes surge como única alternativa el uso de herramientas de software no forense con hardware no forense, pero que tomando los recaudos necesarios para que no se produzca una invasión al contenido de la prueba, por citar una situación, necesidad de obtener archivos multimedia almacenados en el dispositivo y llega a una única opción extraer los mismos mediante la configuración como dispositivo de almacenamiento masivo, conexión cable de datos a PC, explorador de Windows, previo bloqueo de posibilidad de escritura de puertos USB, se obtienen los archivos de interés y luego se efectúa el tratamiento de la evidencia construida según las pautas enunciadas anteriormente.

7 Conclusiones

Tras el desarrollo del presente trabajo surge a los autores la necesidad de destacar la diversidad de elementos de hardware y software que son pasibles de análisis para demostrar o no su vínculo en un hecho delictivo, más aún, si se tiene en cuenta que en el mercado tecnológico los elementos tienen múltiples usos, ejemplo: un teléfono celular sirve: para establecer comunicaciones dentro de la P.S.T.N (Public Switched Telephone Network) o Red Pública Conmutada, tomar imágenes o filmar a través de la cámara nativa en el mismo, grabar conversaciones propias o de un ambiente, navegar en contenidos, acceso a redes sociales, a través de la red internet, usando la conexión propia que brinda el proveedor o inalámbrica que pueda acceder, navegar en un territorio utilizando el receptor G.P.S. nativo en el mismo, transferir y recibir contenidos mediante tecnologías bluetooth y/o Irda.

Esta transversalidad de propiedades en un solo elemento, en contraste cuando eran componentes estancos por su función específica, ha llevado a generar constantes desafíos del conocimiento, sin fronteras aparentes desde el punto de vista tecnológico como en la diversidad de jurisdicción, ya que se pueden producir acciones delictivas que emplean recursos relacionados a TIC`s y repercuten en distintas provincias y/o ciudades dentro o fuera del país, situaciones que obligan a los Poderes Judiciales en su misión de castigar a los culpables, a tomar la iniciativa de formular actos de cooperación entre ellos, como así también con entes privados y públicos que faciliten hacer palmaria una realidad que de otro modo no tendría una respuesta a la sociedad.

Entonces, la propuesta ante ese escenario tecnológico tan cambiante y heterogéneo, se basa en formular normas que regulen la creación, preservación y cadena de custodia de evidencia que este relacionada a las TIC's. Tal como la " Guía operativa en procedimientos judiciales con secuestro de tecnología" de Leopoldo Sebastián Gómez[31], y reciente elaborada y presentada para su aprobación por ante la Fiscalía General de la Provincia de Córdoba (Diciembre 2010) Pautas Informativas y Procedimentales en Ciberdelitos"- con la finalidades de garantizar la legítima obtención o creación , el buen manejo, análisis y preservación de la evidencia digital durante el transcurso de la investigación penal preparatoria.

Si las fuerzas de la ley y los operadores judiciales, al menos dentro del ámbito de la república Argentina, conformaran y aunaran formas de trabajo para la manipulación (en el mas amplio sentido del término) de evidencia vinculada a las TIC's, conforme a derecho, la misma se introduciría en la causa sin mayores dificultades.

8 Bibliografía

1. Jeimy José Cano Martínez, "El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas"
2. Riquert Marcelo, "Delincuencia Informática"
3. RFC 2350 y 3227

[31] Ver en AR Revista Derecho Informatico en Alfa –redi N° 095 Junio del 2006