PROTOCOLIZACION
FECHA 31/03/16
Dra. Daniela Viana Gallo
Subsecretaria Letrada
Procuración General de la Nación

PROCURACIÓN GENERAL DE LA NACIÓN
FOLIO
Nº 1

Procuración General de la Nación

Resolución PGN N° 756 /16.

Buenos Aires, 31 de marzo de 2016.

VISTAS:

Las atribuciones conferidas a la Procuradora General de la Nación por el artículo 120 de la Constitución Nacional y por la Ley Orgánica del Ministerio Público Fiscal de la Nación (ley n° 27.148),

Y CONSIDERANDO QUE:

El Dr. Horacio Juan Azzolin, actual titular de la Unidad Fiscal Especializada en Ciber-delincuencia (resolución PGN 3743/15) ha sometido a consideración de esta Procuración General de la Nación un documento titulado "Guía de obtención, preservación y tratamiento de evidencia digital".

La elaboración de ese documento fue una de las misiones que se le otorgaran al nombrado al ser designado con anterioridad punto focal del organismo en materia de ciberdelincuencia (resolución PGN 2035/14).

El instrumento fue presentado y aprobado en el marco de la XVII Reunión Especializada de Ministerios Públicos del Mercosur, celebrada en Buenos Aires los días 18, 19 y 20 de noviembre de 2014.

El trabajo señala una serie de herramientas de investigación como forma de reforzar la actividad del Ministerio Público Fiscal en los casos en que se cuente con evidencia digital. Concretamente, aborda el modo en el cual se debe obtener, conservar y tratar la evidencia digital para mejorar los niveles de eficiencia en materia de persecución penal, en tanto resulta ser un eje central de preocupación de la comunidad internacional para la investigación transfronteriza del delito.

En ese marco, no pretende abarcar la totalidad de procedimientos a tener en cuenta, sino brindar recomendaciones utilizadas a nivel mundial para incautar, analizar y preservar evidencia digital que deben ser consideradas por los operadores judiciales.

Asimismo, la guía repasa diferentes documentos internacionales que dan cuenta de la relevancia a nivel mundial del fenómeno de la cibercriminalidad y remarca las características advertidas por la Organización de Las Naciones Unidas. Entre ellas menciona la transnacionalidad de esta modalidad, su relación con el crimen organizado

y la necesidad de una legislación uniforme para una adecuada cooperación internacional y una efectiva respuesta estatal.

Por todo lo expuesto, este instrumento que obra como Anexo a la presente, se inserta en los lineamientos de persecución penal definidos por este Ministerio Público Fiscal con el objetivo de elevar la eficiencia en la investigación criminal.

En consecuencia, y en ejercicio de las atribuciones conferidas por la Ley Orgánica del Ministerio Público Fiscal n° 27.148;

LA PROCURADORA GENERAL DE LA NACIÓN

RESUELVE:

Artículo 1°: APROBAR el documento "Guía de obtención, preservación y tratamiento de evidencia digital" que obra como Anexo a la presente.

Artículo 2°: RECOMENDAR a todos/as los/as magistrados/as del Ministerio Público Fiscal que ajusten su proceder a los lineamientos de este documento, en todos los casos en que resulte aplicable.

Artículo 3°: Protocolícese, publíquese y, oportunamente, archívese.

ALEJANDRA GILS CARBÓ
PROCURADORA GENERAL DE LA NACIÓN

"GUÍA DE OBTENCIÓN, PRESERVACIÓN Y TRATAMIENTO DE EVIDENCIA DIGITAL"

INTRODUCCIÓN

En el año 2005 se celebró el Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.

El documento elaborado como consecuencia del mismo sostiene que *"Las tecnologías de la información y las comunicaciones están cambiando las sociedades en todo el mundo al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales y modificar la velocidad y el flujo de capitales. Sin embargo, este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática".*

Allí, también se afirma que *"La investigación de la delincuencia informática no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales, que suelen ser volátiles y de vida corta. También se plantean problemas legales en relación con las fronteras y las jurisdicciones. La investigación y el enjuiciamiento de delincuentes informáticos ponen de relieve la importancia de la cooperación internacional[...]La creciente densidad de tecnologías de la información y las comunicaciones también aumenta la frecuencia de la delincuencia informática nacional, obligando a las naciones a establecer legislación nacional. Puede que se requieran leyes nacionales adaptadas a la delincuencia cibernética para responder eficazmente a las peticiones externas de asistencia o para obtener asistencia de otros países. Cuando se elabora legislación, la compatibilidad con las leyes de otras naciones es una meta esencial; la cooperación internacional es necesaria debido a la naturaleza internacional y transfronteriza de la delincuencia informática. Se necesitan mecanismos internacionales formales que respeten los*

derechos soberanos de los Estados y faciliten la cooperación internacional. Para que la asistencia judicial recíproca funcione con éxito, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de otras...".[1]

Cinco años después, en el Duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal[2] estas conclusiones fueron ampliadas. Se sostuvo en esa ocasión que *"El hecho de que el delito cibernético ocupe un lugar destacado en el programa del 12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal pone de relieve la gran importancia que sigue teniendo este tema y los serios retos que plantea, a pesar de los debates que se vienen sosteniendo al respecto desde hace casi medio siglo [...]En los últimos 50 años se han examinado y elaborado diversas soluciones para hacer frente a la cuestión del delito cibernético. En parte, el tema sigue siendo problemático porque la tecnología evoluciona constantemente y los métodos utilizados para cometer esos delitos también cambian.".*

Entre los retos del delito cibernético, se destacó la falta de información fidedigna sobre el alcance del problema y la necesidad de una reacción efectiva del sistema de administración de justicia, también su dimensión trasnacional, la necesidad de una asistencia jurídica internacional eficaz[3] y de una legislación penal compatible a nivel global[4]. Específicamente

[1] Para mayor información ver *http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf*. Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia)

[2] Para mayor información, consultar http://www.un.org/es/comun/docs/?symbol=A/RES/65/230 Duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 12 al 19 de abril de 2010, Salvador (Brasil).

[3] Por eso se afirmó que *"Las dificultades que el elemento transnacional plantea para la investigación del delito cibernético son parecidas a las que entrañan otros delitos transnacionales. Como consecuencia del principio fundamental de la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial para la investigación de los delitos cibernéticos. Otra dificultad importante se relaciona con el poco tiempo disponible para llevar a cabo las investigaciones de esos delitos. A diferencia de lo que ocurre con las drogas ilícitas, que, según el medio de transporte que se utilice, pueden tardar semanas en llegar a su destino, los correos electrónicos se envían en segundos y, si se tiene acceso a un ancho de banda adecuado, es posible descargar grandes ficheros en algunos minutos... [...]".*

[4] *"...un efecto práctico de la arquitectura en red de Internet es que los autores de los delitos cibernéticos no necesitan estar presentes en el lugar del delito. Por ello, impedir la existencia de refugios seguros para los delincuentes se ha convertido en un aspecto clave de la prevención del delito cibernético. Los delincuentes utilizarán refugios seguros para obstaculizar las investigaciones. Un ejemplo bien conocido es el gusano informático "Love Bug", desarrollado en*

sobre la cooperación internacional, se afirmó que *"...La cooperación tempestiva y eficaz entre las autoridades de diferentes países es fundamental también porque en los casos de delitos cibernéticos las pruebas suelen suprimirse automáticamente y al cabo de poco tiempo. Los procedimientos oficiales prolongados pueden obstaculizar seriamente las investigaciones..."*

Se tuvo presente también que en los delitos informáticos pueden intervenir grupos delictivos en dos aspectos: el uso de las tecnologías de la información por parte de grupos delictivos tradicionales o la comisión de delitos cibernéticos por grupos delictivos organizados[5], que abre la posibilidad de utilizar instrumentos tales como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional[6].

En cuanto a la respuesta a esta modalidad delictiva, se destacó que las organizaciones internacionales, las naciones y las fuerzas de seguridad abordaban el fenómeno de diversas formas, que incluyen medios legislativos, de aplicación de la ley y de fomento de la capacidad. Concretamente respecto a la aplicación de la ley, se dijo que depende en gran medida *"[...] de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros*

Filipinas en 2000, que al parecer infectó a millones de computadoras en todo el mundo. Las investigaciones locales se vieron impedidas por el hecho de que, en esa época, el desarrollo y la difusión intencionales del programa informático dañino no estaban debidamente penalizados en Filipinas[...]La cuestión de la convergencia de la legislación es sumamente pertinente, puesto que un gran número de países fundamenta su régimen de asistencia judicial recíproca en el principio de la doble incriminación, según el cual un delito debe ser considerado como tal tanto en el Estado que solicita la asistencia como en el que la presta[...]".

[5] *"[...] los grupos delictivos organizados tradicionales que no tienen antecedentes de actividades delictivas relacionadas con Internet están utilizando la tecnología de la información para coordinar sus actividades y aumentar su eficacia en la comisión de delitos... En estos casos, la tecnología de la información se utiliza para mejorar la eficiencia del grupo delictivo organizado en su campo de actividad tradicional. Ello incluye la utilización de las comunicaciones electrónicas, que le permiten, por ejemplo, hacer uso de la tecnología de cifrado y comunicar en forma anónima...Los informes indican que los grupos delictivos organizados tradicionales están tendiendo a emprender nuevas formas de actividades delictivas en la esfera de los delitos de alta tecnología. Ello incluye la piratería de programas informáticos y otras formas de violación de los derechos de autor. Pero también otras esferas del delito cibernético, como la pornografía infantil y los delitos relacionados con la identidad, están vinculados a menudo con la delincuencia organizada [...]"*

[6] *http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf*

suprimidos) y programas informáticos o bases de datos de gestión de la investigación (por ejemplo, con valores "hash" para imágenes de pornografía infantil conocidas)."

En 2015 se realizará el Trigésimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y entre los temas de sus talleres está incluida la respuesta de las agencias de persecución estatal al fenómeno de la delincuencia informática[7].

Otra iniciativa internacional que merece destacarse es la elaboración del Convenio sobre la Ciberdelincuencia (Budapest, 2001) Entre los fundamentos de su creación está la de *"...aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional"* El convenio aborda la temática vinculada con los delitos cometidos a través del uso de nuevas tecnologías de la información y las comunicaciones. Tiene tres secciones principales: (i) Derecho Penal: en la que los estados parte se comprometen a ajustar su legislación interna para sancionar como delitos determinadas conductas que se mencionan, (ii) Derecho Procesal Penal: en ella, los estados parte se comprometen a ajustar su ley procesal para permitir la realización de diversas diligencias de prueba. En términos muy generales se tiende a poder preservar e interceptar determinados datos contenidos en sistemas informáticos (datos de tráfico, datos de contenido, etc.) y (iii) Cooperación Internacional: en esta sección, se establecen diversos mecanismos de cooperación internacional entre los estados parte para compartir y obtener información mediante las vías formales, aunque se establecen canales para que el intercambio de información pueda hacerse rápidamente de ser necesario.

Por otra parte, el 28 de mayo de 2014, en la sede de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) en Madrid, los representantes de los gobiernos de Guatemala, Nicaragua, Portugal, Perú y Uruguay firmaron el "Convenio Iberoamericano de

[7] http://www.unodc.org/documents/congress//background/13thCCDiscussionGuide.pdf

Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia"[8].

Los cuatro primeros países mencionados, a los que se sumó la Argentina, suscribieron además la "Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia"[9], con la finalidad de lograr un impacto en la legislación nacional de los países miembros de la COMJIB.

Respecto de la importancia de los textos firmados, el Secretario General de la COMJIB, Fernando Ferraro, señaló: *"El Convenio aporta una amplia definición de Ciberdelincuencia que permite que los instrumentos de cooperación internacional se puedan aplicar para muchos tipos de delitos; y la Recomendación se presenta como un aporte adicional a los Estados para que puedan actualizar y modernizar sus legislaciones penales para combatir de forma efectiva la cibercriminalidad, y evitar que estos hechos delictivos queden en la impunidad, contribuyendo a la modernización de las legislaciones penales internas de los países."*[10]

A nivel del MERCOSUR, los delitos informáticos han sido abordados en el ámbito de las Reuniones Especializadas de Ministerios Públicos del Mercosur (REMPM) con la creación de un sub-grupo de trabajo (XV REMPM, 2013, Montevideo, Uruguay) dentro del Grupo Especializado sobre el Crimen Organizado Transfronterizo -GECOT- (VII REMPM, 2009, Asunción, Paraguay).

Además, en el marco de la XVI Reunión Especializada de Ministerio Públicos del Mercosur (REMPM) celebrada en octubre de 2013 en la Isla de Margarita, Venezuela, la delegación del Ministerio Público Fiscal de la República Argentina se comprometió a elaborar un documento que aborde la temática relativa a la obtención y preservación de evidencia digital para ser presentado y discutido en la reunión siguiente, a celebrarse en ese país.

---

[8] *http://www.comjib.org/sites/default/files/CONVENCION_CIBER.pdf*
[9] *http://www.comjib.org/sites/default/files/Ciberd_Recomendacion_28052014_0.pdf*
[10] *http://www.comjib.org/contenido/paises-iberoamericanos-firman-convenio-y-recomendacion-sobre-ciberdelincuencia-en-madrid*

También se ha distribuido entre los países participantes un cuestionario elaborado por Uruguay, coordinadordel subgrupo, que tiende a (i) facilitar las instancias de cooperación internacional, (ii) armonizar las legislaciones, (iii) capitalizar las experiencias ajenas para acelerar los procesos de actualización y (iv) facilitar el intercambio de información y el diseño de planes de capacitación internacionales sobre el tema.

Lo expresado hasta aquí permite graficar la relevancia a nivel mundial del fenómeno de la cibercriminalidad, y de cómo todas las características tenidas en cuenta por el organismo de Naciones Unidas en 2010 –transnacionalidadde esta modalidad y su relación con el crimen organizado, necesidad de una legislación uniforme para una adecuada cooperación internacional y efectiva respuesta estatal – permanecen inalteradas en la actualidad.

Muchos de esos aspectos están siendo abordados por el sub-grupo ya mencionado. Las respuestas que se brinden al cuestionario elaborado por Uruguay permitirán establecer nuevas líneas de trabajo en ese sentido.

Uno de temas que puede tocarse desde ahora es el relativo a la evidencia digital, ya que su adecuada obtención, conservación y tratamiento es un elemento clave, entre muchos otros, para asegurar el éxito de las investigaciones, eje central de preocupación de la comunidad internacional para la investigación transfronteriza eficaz de estos delitos.

Fue por eso que Argentina se comprometió a elaborar este documento que ahora sometemos a discusión, para que contemos con un conjunto de reglas comunes.

Durante su redacción se ha tenido en cuenta el material que nos han enviado los colegas de los países participantes y guías de trabajo utilizadas por otras agencias de la ley a nivel mundial. El trabajo no pretende abarcar la totalidad de procedimientos a tener en cuenta, ni ahondar en cuestiones técnicas reservadas a los expertos en seguridad y en informática, sino brindar recomendaciones utilizadas a nivel mundial para incautar, analizar y preservar evidencia digital que deben ser tenidas en cuenta por los operadores judiciales.

LA EVIDENCIA DIGITAL[11]

Puede definirse la evidencia digital como el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico.

Una de las características de la evidencia digital es su volatilidad. Esto conlleva a que la misma, por su propia naturaleza, sea frágil, fácil de alterar y dañar o directamente de destruir. Especialistas en informática forense la asimilan a la evidencia de ADN o a las huellas dactilares por ser un tipo de prueba latente. Con esto nos estamos refiriendo a que dicha evidencia, en su estado natural, no nos deja entrever qué información es la que contiene en su interior, sino que resulta ineludible para ello, examinarla a través de instrumentos y procesos forenses específicos.

---

[11]Las definiciones, conceptos y reglas prácticas fueron tomados de los siguientes documentos:
1) U.S. Department of Justice, Office of Justice programs, National Institute of Justice (NIJ), *"Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition"*disponible en https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
2) Association of Chief Police Officers (ACPO) from England, Wales & Ireland, *"Good Practice Guide for Computer-Based Electronic Evidence, V. 4.0"* quepuedeconsultarse en el siguiente enlace:
http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
y el mismo documento, en su versión siguiente (5.0) que puede descargarse de este link:
http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf
3) U.S. Department of Homeland Security, United States Secret Service, *"Best Practices For Seizing Electronics Evidence V.3.0"* quepuedeconsultarse enhttp://www.forwardedge2.com/pdf/bestPractices.pdf
4) Ecuador, *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. 1. Manual de Manejo de Evidencias Digitales y Entornos. Informáticos. Versión 2.0.* que puede consultarse en www.oas.org/juridico/english/cyb_pan_manual.pdf
5) Ministerio Público de Venezuela, Manual Único de Procedimientos en Materia de Cadena de Custodia de Evidencias Físicas, disponible en *http://www.mp.gob.ve/c/document_library/get_file?uuid=85f4a05f-3c5d-4b1b-91ef-84193658f83d&groupId=10136*
6) Australia, *"Guidelines for the Management of IT Evidence"*http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf
7) U.S. Department of Homeland Security, "Best Practices for Seizing Electronic Evidence" version 2.0, https://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/downloads/other/bestpractices.pdf/view
8) Informática Forense: Recogida de evidencias, http://www.sticc.com/articulos/ver.aspx?Id=35

Por lo expuesto, resulta imperativo tomar precauciones especiales al momento de recolectar, manipular, documentar y examinar la evidencia digital, ya que de lo contrario, dicha prueba puede tornarse inválida a los fines judiciales, o en su caso, mostrarse imprecisa a efectos de esclarecer el hecho delictivo.

Principios de tratamiento de la evidencia digital

Varios documentos han abordado esta temática, entre ellos se destaca la norma ISO/IEC 27037:2012[12] que brinda lineamientos para la identificación, recolección, obtención y preservación de la evidencia digital de forma tal de poder ser utilizada como evidencia útil[13]. Para algunos autores, la regla indica que la evidencia digital es gobernada por tres principios fundamentales[14]: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital.

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra característica fundamental, que busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital. Es decir, que la

---

[12]La ISO (International StandarizationOrganization) es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo, brindando estándares internacionales. La regla citada puede adquirirse en *http://www.iso.org/iso/catalogue_detail?csnumber=44381*

[13]Para abordar este tópico se consultó también *http://insecuritvit.blogspot.com.ar/2013/09/reflexiones-sobre-la-norma-isoiec.html*. *http://www.copitec.org.ar/comunicados/CAIF2014/CAIF-Presman.pdf*y *http://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/*yAltmark, Daniel Ricardo y Molina Quiroga, Eduardo,"*Tratado de Derecho Informático*", La Ley, Buenos Aires, 2012.

[14]Otros hablan de cuatro: aplicación de métodos, proceso auditable, proceso reproducible, proceso defendible, aunque los contenidos son similares. Ver *http://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/*

evidencia que se extraiga u obtengasea lo que deba ser; y que si un tercero sigue el mismo proceso, deberá obtener resultados similares, verificables y comprobables.

Finalmente, el principio de suficiencia, se relaciona con la completitud de pruebas informáticas. En otras palabras, significa que con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos y priorización de esfuerzos.

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO ha determinado que estos tres establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados y sometidos a contradicción según el ordenamiento jurídico donde se encuentren.

Otros documentos hablan deprincipios básicos[15] o "reglas de oro" en materia de evidencia digital, que deben tenerse en cuenta a lo largo de todo el procesamiento de este tipo de prueba[16].

---

[15] Association of Chief Police Officers (ACPO) from England, Wales & Ireland, "*Good Practice Guide for Computer-Based Electronic Evidence, V. 4.0*"quepuedeconsultarse en este enlace: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

[16]El Código Procesal Penal del Ecuador trata la cuestión en su artículo 500 en los siguientes términos:
"El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
En la investigación se seguirán las siguientes reglas:
1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.
2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

Estos son:

(i) Al llegar a la escena donde se va a obtener evidencia digital, lo primero que debe hacerse es evitar su contaminación, retirando del lugar a toda persona ajena al procedimiento que se está llevando a cabo;

(ii) En segundo lugar, ninguna acción de las fuerzas de seguridad o de sus agentes debe alterar los datos contenidos las computadoras o dispositivos de almacenamiento informático que luego serán utilizados como elementos de prueba;

(iii) Si las circunstancias del caso hacen necesario que se deba acceder a los datos o información contenida en las computadoras o dispositivos de almacenamiento informático, la persona que efectúe dicha tarea debe ser idónea, es decir, contar con los conocimientos técnicos informáticos que la situación merece y, a su vez, capaz de explicar el motivo por el cual debió interactuar con la evidencia digital –por lo general, la urgencia del caso-, y los pasos llevados a cabo;

(iv) Finalmente, se debe auditar y registrar fehacientemente todo el proceso relativo a la manipulación de la evidencia digital, precisando detalladamente las medidas y acciones llevadas a cabo, teniendo como eje central, la preservación de la cadena de custodia.

Recolección y preservación de la evidencia digital.

1. Presupuestos generales.

---

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto."

Es necesario destacar que, al momento de analizar la escena del crimen, podemos encontrarnos con diversos panoramas, y es por ello que serán distintas las respuestas para cada situación en particular para aumentar cualitativamente y cuantitativamente los datos e información a capturar y, asimismo, asegurar su integridad para conformar el futuro escenario probatorio.

Lo primero que se debe hacer, tras asegurar el lugar, es documentar cualquier tipo de actividad que esté teniendo lugar en la computadora, componentes externos a ella y/o dispositivos de almacenamiento informático.

Acto seguido, se debe confirmar el estado de la computadora, es decir si se encuentra prendida o apagada, ya que en virtud de ello el procedimiento diferirá sustancialmente.Debe tenerse en cuenta que algunas veces el ordenador parece apagado pero en realidad se encuentra "suspendido" (*sleepmode* o modo de ahorro de energía), cuestión que generalmente puede detectarse a simple vista cuando el monitor de la pantalla se encuentra apagado pero los leds (diodo emisor de luz) frontales de la CPU (unidad central de procesamiento) se encuentran activos (ej. aquél que muestra la actividad del disco duro - lectura y escritura-) y/o cuando se detecta actividad de los ventiladores (*coolers)*. En estos casos es el mismo agente especializado el que debe decidir si corresponde "despertar" o no al equipo y continuar con el procedimiento. De ser afirmativa la respuesta, se recomienda utilizar el movimiento del mouse para reactivar la computadora, evitando hacer clics con el mismo o utilizar el teclado, ya que podría activar algún programa de protección, encriptación o inclusive borrado de datos.

Antes de tener contacto con cualquiera de los elementos informáticos, se deberá fotografiar, filmar o en su defecto confeccionar un croquis de la escena del crimen en su totalidad, individualizándose cada aparato electrónico. En lo que respecta específicamente a la computadora, debe fotografiarse la parte frontal y trasera, incluyendo la imagen que se

muestra en el monitor de la misma, y a su vez, la parte posterior en la que se observarán los cables y conexiones pertinentes.

Podemos tener, entonces, diversos escenarios:

(i) El escenario más simple lo encontramos cuando la computadora se encuentra apagada. De ser así, los pasos a seguir son los siguientes:

a. Bajo ninguna circunstancia encender el equipo.

b. Remover el cable de alimentación de la computadora desde la parte posterior de la misma, no directamente desde la toma de corriente de pared. En el caso de las computadoras portátiles se debe además remover la batería de la misma.

c. Desconectar el resto de los cables y dispositivos USB o de almacenamiento informático que se encuentren conectados a la computadora.

d. Asegurarse de que la lectora de diskettes, CD o DVD estén cerradas, detallando si las mismas contenían algún soporte en su interior (en el caso de que se encontrasen abiertas)

e. Encintar todas las entradas de puertos, cables de alimentación y otros, lectoras de CD, DVD y diskettes, a fin de asegurar que las mismas no sean utilizadas, y por ende, se altere la información contenida en la computadora.

f. Registrar la marca, modelo y números de serie como así también cualquier otro tipo de identificación de la computadora y sus periféricos.

(ii) Otra situación se da cuando la computadora se encuentra encendida. Generalmente, la opción más segura para preservar la evidencia digital contenida en la computadora es eliminando la alimentación de energía de la misma (de la forma descripta anteriormente para trabajar sobre un equipo apagado).

Hay algunos casos en los cuales esta acción debe realizarse inmediatamente:

a. Si a simple viste se detecta, según la información o actividad mostrada en el monitor de la computadora, que los datos están siendo eliminados o sobrescritos.

b. Si hay indicaciones de que este teniendo lugar un proceso de destrucción en los dispositivos de almacenamiento de información, tanto internos -ej. discos duros- como externos -ej. *pendrives*-.

Debe tenerse en cuenta que al desconectar la computadora directamente desde el cable de alimentación en la mayoría de los sistemas operativos -ej. Windows-, se logra preservar, en muchos casos, información que puede ser gran utilidad. Por ejemplo: el último usuario que se logueó (persona que se registró con usuario y contraseña para ingresar al sistema operativo), a qué hora lo hizo, datos sobre los últimos comandos ejecutados, documentos utilizados por éste, etc. Asimismo, se asegura que ningún otro dispositivo con alimentación de energía propia pueda seguir escribiendo o eliminando información en la computadora.

Hay casos en los que la computadora se encuentra encendida, pero no se recomienda su apagado inmediato, ellos son:

a. cuando a simple vista se observa en pantalla información que puede ser de valor probatorio para la investigación o,

b. cuando existen indicaciones ostensibles de que se encuentran activos programas de mensajería instantánea, blogs, documentos abiertos que muestren registros financiero o de procesamiento de datos (Word, Excel, PowerPoint, etc.), datos encriptados, imágenes de pornografía infantil y/o cualquier actividad ilegal.

En estos casos, donde parece conveniente manipular la información volátil del sistema informático, se recomienda dejar expresamente constancia de tal decisión, utilizando para tal fin un dispositivo de captura volátil de datos que tenga bloqueada la escritura, a fin de no modificar u alterar la información, como ser un USB *flash drive*, USB *hard drive*, etc.

2. Principios especiales.

(i) Computadoras en red y conexiones inalámbricas (WI-FI / Bluetooth)

Cada vez resulta más frecuente el uso de computadoras en red en situaciones domésticas, las mismas tienen comúnmente el fin de compartir recursos entre diversos dispositivos informáticos de manera simultánea y rápida (ej. conexión a internet, acceso a archivos o dispositivos periféricos).

Como se grafica más abajo[17], generalmente las redes domésticas se encuentran formadas por los siguientes elementos:

- Una o más computadoras (con sus respectivas placas de red);
- Un módem;
- *Switches* o *routers* (o dispositivos que combinan ambas funciones);
- Puntos de Acceso inalámbricos (*Wireless Access Points*);
- Dispositivos con conexión Bluetooth o Wi-Fi (ej. teléfonos inteligentes, agendas electrónicas, televisores inteligentes (Smart TV), discos duros y otros) e impresoras, *scanners*, cámaras digitales, etc.

[17]Imagen extraída de la presentación de las jornadas *"Herramientas informáticas para la investigación"* que tuvieron lugar en el ámbito del Ministerio Público Fiscal de la Nación, a cargo del ingeniero Santiago Vallés y el Fiscal Horacio J. Azzolin.

Conexión Estándar

Modem **Router + Access Point** **Red LAN**

Para estos casos se debe detallar y precisar las conexiones entre los dispositivos (tal como se ha expuesto anteriormente), y a su vez, considerar que puede estar teniendo lugar una conexión de acceso remoto con los dispositivos en cuestión por medio de otro aparato electrónico, como por ejemplo a través de una computadora que no se encuentre físicamente en la escena o inclusive desde un teléfono celular, agenda electrónica o tableta. Por ello, de detectarse esa situación, el agente deberá registrar y detallar dicha actividad y en su caso, inmediatamente desconectar la red o bloquear el acceso a ella a fin de preservar la evidencia digital que pretendemos recolectar. Lo expuesto, siempre encontrará variantes en razón de la estrategia que se adopte en cada circunstancia.

Se recomienda al agente, tanto para los casos en que se encuentre una computadora en solitario (*stand alone*) o en red, la obtención de información relativa a: el listado de procesos, servicios y aplicaciones utilizadas, el registro de logueo y usuarios identificados, información de red -en su caso- que incluya el detalle de los puertos (*ports*) abiertos y cerrados,

información contenida en el cache del sistema, información del registro del sistema operativo (*registry*) y en casos específicos el volcado de memoria RAM (*memorydump*)[18].

Una vez realizadas estas operaciones, deben tratarse todos los elementos que componen la red al igual que una computadora en solitario, tal como fue detallado en los puntos precedentes.

(ii) Otros dispositivos electrónicos a tener en cuenta.

No pueden dejarse de lado aquellos dispositivos que pueden contener potencialmente evidencia digital de utilidad para la investigación, como por ejemplo los que se detallan a continuación: teléfonos celulares, identificadores de llamada, *pagers*, agendas electrónicas, tabletas, tarjetas de memoria (SD, micro SD, flash, PCMCIA, etc.), *pendrives*, grabadores de audio, GPS, chips, tarjetas electrónicas, reproductores de música y video en diversos formatos (ej. IPod), etc.

Salvo en situaciones de emergencia que así lo ameriten, estos elementos no deben ser operados, y por ende, deben ser resguardados de forma inmediata tal como se describe en el próximo punto.

3. Embalaje, traslado y resguardo de la evidencia digital.

Al momento de empacar la evidencia deben tenerse en cuenta las siguientes cuestiones:

(i) Asegurar que toda la evidencia digital recolectada se encuentre debidamente documentada, etiquetada, marcada, fotografiada, filmada o esquematizada (croquis) e

[18]El volcado de memoria RAM puede ser de gran utilidad por ejemplo para los casos de pedofilia mediante los cuales se utilizan computadoras de cibercafé o de acceso público; eso, si es localizado al momento del hecho. Lo que permite esta función es recabar información volátil que se encuentra en la memoria de acceso aleatorio de las últimas horas en la computadora, en estas situaciones debe aclararse explícitamente la fecha y hora en la que se coloca el dispositivo para hacer el volcado, a fin de que no quede ninguna duda en la pericia a realizar posteriormente.

inventariada. También se recomienda individualizar cada uno de los cables conectores (de alimentación y de transferencia de datos) para facilitar la futura reconexión de los dispositivos en el lugar donde se llevará a cabo la pericia informática.

(ii) Considerar en todo momento que la evidencia digital puede también contener evidencia latente, rastreable e inclusive biológica. La copia forense de los discos duros deberá llevarse a cabo con anterioridad al resto de las mencionadas (ya se detallará el proceso de copia forense más adelante).

(iii) Embalar toda la evidencia digital en paquetes, envoltorios o bolsas antiestáticas o en su defecto, de papel madera o cartón; evitando el uso de elementos plásticos, ya que pueden generar energía estática y permitir que la humedad o condensación se desarrolle y dañe o inclusive destruya la evidencia.

(iv) Asegurarque el modo en que es recolectada la evidencia no permita ralladuras, doblamiento de materiales o cualquier otro tipo de deformación de los dispositivos.

(v) En caso que resulte sumamente necesario que el aparato continúe encendido hasta que se efectúe la pericia, se recomienda cubrir los teléfonos celulares inteligentes en material que bloquee la señal de transferencia de datos. Para ello pueden utilizarse las denominadas jaulas de aislación Faraday[19] que permiten mantener encendido el aparato electrónico al mismo tiempo que bloquean cualquier trasmisión de datos -ingreso y egreso- con el exterior. A su vez, existenbolsas especialmente diseñadas para esto –que incluso vienen preparadas para

[19]Es conocido como jaula de Faraday el efecto por el cual el campo electromagnético en el interior de un conductor en equilibrio es nulo, anulando el efecto de los campos externos. Esto se debe a que, cuando el conductor está sujeto a un campo electromagnético externo, se polariza, de manera que queda cargado positivamente en la dirección en que va el campo electromagnético, y cargado negativamente en el sentido contrario. Puesto que el conductor se ha polarizado, este genera un campo eléctrico igual en magnitud pero opuesto en sentido al campo electromagnético, luego la suma de ambos campos dentro del conductor será igual a 0. http://es.wikipedia.org/wiki/Jaula_de_Faraday

conectar el equipo para ser analizado mientras permanece en la bolsa encendido-; en caso de no poseerlas, hay otras formas de generar el mismo efecto: utilizar un mosquitero de alambre para recubrir todo el dispositivo, una lata de pintura vacía con su respectiva tapa, un horno de microondas, papel aluminio, etc. Cabe destacar que generalmente esta operatoria no es necesaria ya que con la ulterior pericia informática se recaba de igual manera la información que interesa a la investigación.

(vi) Recolectar todo tipo de fuente de energía que se vincule con los dispositivos (cables, baterías, etc.).

(vii) Recordar que la evidencia potencialmente significante como fechas, horas, y ciertos datos de configuración del sistema pueden perderse si se resguarda el dispositivo electrónico por tiempo prolongado y su batería o fuente de energía que preserva dicha información falla o se agota.

Por último, debe tenerse en cuenta al momento del traslado y preservación lo siguiente:

(i) Mantener la evidencia digital fuera del alcance de campos magnéticos, vibraciones fuertes, humedad, polvo, temperaturas extremas o cualquier otro tipo de elemento que pueda ocasionarle daño o destruirla.

4.Manipulación idónea del hardware.

El análisis y examen de los dispositivos de almacenamiento de información deberán realizarse en establecimientos que dispongan de áreas acondicionadas las cuales deberán ser zonas seguras antiestáticas, constituyendo jaulas de Faraday a los fines de evitar cualquier intromisión por medio de WI-FI o Bluetooth u cualquier otro medio de acceso remoto.

Asimismo, debe ponerse en consideración que algunas piezas de los dispositivos electrónicos suelen ser extremadamente sensibles, como por ejemplo: microprocesadores, memorias, discos rígidos, etc. Dichos dispositivos suelen trabajar con bajo voltaje, es por ello que se sugiere que el personal que procederá a su manipulación emplee no solo guantes de látex o similares, sino también – de ser posible- pulseras antiestáticas o brazaletes antiestática de descarga a tierra, a fin de evitar que una descarga involuntaria del operador pueda dañar o inutilizar el equipo bajo estudio.

5. Imagen o copia forense y uso de *hash*.

Se entiende por imagen o copia forense a aquella que replica en forma completa (por sector, bit a bit) la estructura y contenido de un dispositivo de almacenamiento, como ser los discos duros.

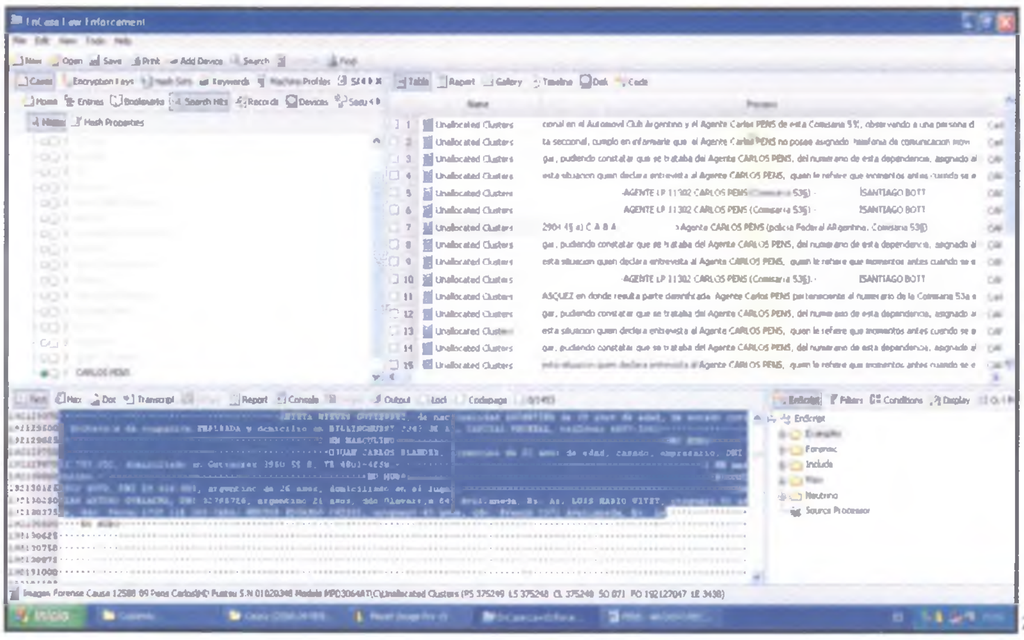
La imagen forense puede obtenerse de forma directa: se extrae el disco rígido físicamente del ordenador y se procede a realizar la copia o; indirecta: se conecta un dispositivo externo al ordenador a fin de evitar la extracción del disco rígido y se hace la copia de idéntica manera.

Esta operación resulta fundamental a los efectos de poder analizar profundamente la evidencia digital colectada ya que nos permitirá recabar los datos y metadatos -atributos de los archivos-contenidos en los dispositivos al igual que si lo estuviéramos haciendo con el original, pero con una importante diferencia:no estaremos alterando la evidencia original.

La copia forense puede realizarse por medio de un copiador de hardware, lo que permite una mayor velocidad en la transferencia de datos (siendo uno de los más conocidos los de

marca Tableau). Otra opción es utilizar un software (Encase, FTK, y herramientas de software libre como el programa DD).

El análisis *per se* de los datos que se extraen de los dispositivos de almacenamiento informático se hace exclusivamente a través de cualquier herramienta de software avalada internacionalmente (Encase, por ejemplo). Actualmente las fuerzas de seguridad locales utilizan dichos programas por su óptimo y confiable rendimiento, y por contar con el aval del NationalInstitute of Standards and Techonolgy (NIST)[20].


[21]

Hay dos cuestiones que resultan de carácter obligatorio en este procedimiento:

---

[20]*www.nist.gov*

[21]Imagen extraída de la presentación efectuada por el Jefe de la División Informática Judicial de la Gendarmería Nacional Argentina, Ing. Leonardo Rafael Iglesias, en al ámbito de las *"Jornadas de capacitación sobre el trabajo en la escena del crimen* "del Ministerio Público Fiscal de la Nación. La misma es una captura de pantalla sobre el programa ENCASE en pleno funcionamiento.

(i) Por un lado, utilizar un bloqueador de escritura al momento de realizar la copia forense ya que este dispositivo permite operar la computadora asegurando que no se modifique absolutamente la más mínima información, es decir, nos restringirá a la mera lectura y copiado de los archivos.

(ii) y por otro, una vez finalizado el copiado, el agente debe realizar el cálculo *hash* de dicha copia forense.

El *hash* se define como la conversión de determinados datos en un número de longitud fijo no reversible, mediante la aplicación de una función matemática -algoritmo- unidireccional. Tiene como funciones primordiales la autenticación (permite corroborar la identidad de un archivo) y preservación de integridad de los datos (asegura que la información no haya sido alterada por personas no autorizadas u otro medio desconocido), resultando entonces de vital importancia a los fines de controlar la preservación de la cadena de custodia y evitar planteos de nulidad.

Calcular el *hash* de la copia forense permitirá verificar si la misma fue alterada con posterioridad a su obtención. Si pasado un tiempo de realizada la misma alguien plantea que fue alterada, bastará calcular el *hash* para ver si es el contenido es el mismo del originalmente obtenido (en este caso, se demuestra que la copia no fue manipulada).

[22]

Este procedimiento también puede utilizarse para cualquier otra evidencia digital obtenida por los investigadores y que no necesariamente haya sido incautada. Un ejemplo de ello son los registros de tráfico de comunicaciones entregados por la empresa que brinda el servicio en un formato que puede ser modificado. Con el *hash* calculado al recibir la prueba, cualquier modificación de la evidencia se notará en el futuro al repetir la operación.

[22]Imagen extraída de la presentación efectuada por el Jefe de la División Informática Judicial de la Gendarmería Nacional Argentina, Ing. Leonardo Rafael Iglesias, en al ámbito de las "Jornadas de capacitación sobre el trabajo en la escena del crimen "del Ministerio Público Fiscal de la Nación. En la misma se puede observar la adquisición de dos certificaciones Hash (MD5 y SHA1) por medio del programa ENCASE, sobre el archivo de una copia forense.

6. Aspectos a tener en cuenta al momento de analizar la evidencia digital recolectada en función de los delitos a investigar en los que el medio informático puede ser relevante.[23]

A continuación se detallará un listado de la evidencia digital que puede ser recolectada de los dispositivos de almacenamiento informático secuestrados, y que, dependiendo de cada delito en particular, merecerá un mayor análisis, a saber:

(i) Defraudaciones y estafas informáticas:

-Información contable de acciones en línea;

- Software y documentos contables;
- Datos de tarjetas de crédito;
- Correos electrónicos y notas varias;
- Registros financieros de activos, cheques y órdenes de pago;
- Libros de direcciones y calendarios.

(ii) Abuso infantil y pornografía:

- Registros de chats y blogs;
- Software de reproducción, captura y edición de video;
- Imágenes y videos de contenido sexual;

-Juegos infantiles o de contenido sexual;

-Registros de actividad en internet;

---

[23]Se consultó:1) U.S. Department of Justice, Office of Justice programs, National Institute of Justice (NIJ), "*Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*"disponible en https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.
2) U.S. Department of Homeland Security, United States Secret Service, "*Best Practices For Seizing Electronics Evidence V.3.0*" quepuedenconsultarse enhttp://www.forwardedge2.com/pdf/bestPractices.pdf

- Directorios de archivos encriptados o no visibles mediante los cuales clasifica el contenido de las distintas víctimas;
-Correos electrónicos, notas y cartas varias.

(ii) Acceso no autorizado a sistemas informáticos

-Software específico (ej. programas autoejecutables, troyanos, registradores de teclas, etc.);
- Software y códigos de programación;
- Registros de actividad en internet;
- Archivos de texto y documentos con nombres de usuario y contraseñas;
- Registro de sesiones de chat y blogs;
- Listado de computadores a las cuales accedió;
- Registro de direcciones IP (*internet protocol*).

(iv) Copia ilegal de software:

-Registros de chat;
- Correos electrónicos y notas:
- Software específico (ej. generador de claves o códigos de activación; herramientas de cracking);
- Archivos de texto y documentos con números de serie y usuarios.

(v) Homicidios:

- Lista de direcciones;
- Correo electrónico, cartas y notas varias;
- Registros financieros;
- Registro de actividad en internet;

- Documentos legales y testamentos digitalizados;
- Registros de chats;
- Mapas;
- Fotos y/o videos de la víctima.

(vi) Amenazas y/o acoso vía correo electrónico:

- Libros de direcciones;
- Diarios íntimos;
- Correos electrónicos, notas y cartas;
- Registro de actividad en internet;
- Registros telefónicos;
- Investigación sobre el historial (*background*) de la víctima;
- Mapas de las locaciones de las víctimas;
- Imágenes, videos y/o cualquier tipo de registro de vigilancia;
- Documentos legales.

(vii) Investigaciones referidas a estupefacientes:

- Libros o Agendas de Direcciones;
- Correos electrónicos, notas y cartas;
- Calendarios;
- Bases de Datos;
- Prescripciones médicas;
- Documentos falsos para acreditar la identidad;
- Registros financieros;
- Registros de actividad en internet.

(viii) Fraude de telecomunicaciones:

- Software específico de clonado y de programación de teléfonos celulares;
- Bases de datos de clientes;
- Números de serie electrónicos;
- Números de identificación de celulares;
- Correos electrónicos, notas y cartas;
- Registros financieros;
- Registros de actividad en internet;
- Archivos extraídos de diversas tarjetas SIM.

(ix) Violencia doméstica:

- Libros o agendas con direcciones;
- Diarios íntimos, entradas en Blogs personales o comentarios en redes sociales;
- Correos electrónicos, notas y cartas;
- Registros financieros;
- Registros telefónicos.

INDICE