GUÍA INTEGRAL
DE EMPLEO DE LA INFORMÁTICA FORENSE
EN EL PROCESO PENAL

Segunda edición, revisada - Abril 2016

El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) es una iniciativa conjunta de la Universidad FASTA, el Ministerio Público Fiscal de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon, que nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores científicos y tecnológicos, profesionales y técnicos altamente calificados, con el objeto de desarrollar soluciones a las demandas en el campo de la Informática Forense y su aplicación.
El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) es la sede del Grupo de Investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense *InFo-Lab*
Ministerio Público Fiscal Provincia de Buenos Aires. Universidad FASTA. Municipalidad de General Pueyrredon.
Universidad FASTA. Avellaneda 3341. Mar del Plata. Argentina.
info-lab@ufasta.edu.ar
(+54-223) 499-5200

Guía Integral de Empleo de la Informática Forense en el Proceso Penal
Ana Haydée Di Iorio... [et al.]. - 1a ed. - Mar del Plata.
Universidad FASTA, 2015.
Libro digital, PDF

Archivo Digital: descarga
ISBN 978-987-1312-73-3

1. Derecho Procesal. 2. Derecho Penal. 3. Aplicaciones Informáticas.
I. Di Iorio, Ana Haydée
CDD 347.05

Segunda edición, revisada, Universidad FASTA, 2016.
Libro digital, PDF

GUÍA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL

I. ÍNDICE DE CONTENIDO

I. ÍNDICE DE CONTENIDO 3

II. PRESENTACION 5

III. PROTOCOLO DE ACTUACIÓN INFORMÁTICO FORENSE 9

FASE DE RELEVAMIENTO E IDENTIFICACIÓN 13

FASE DE RECOLECCIÓN 16

ADQUISICIÓN DE DATOS VOLÁTILES 21

CADENA DE CUSTODIA Y PRESERVACIÓN 23

ADQUISICIÓN DE MEDIOS DE ALMACENAMIENTO PERSISTENTES 25

LABORES PERICIALES 27

IV. ANEXO I 35

EVIDENCIAS EN MEDIOS TECNOLÓGICOS 35

V. ANEXO II 41

A. ACTA DE LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL 41

VI. ANEXO III 47

I. MODELO PURI 47

II. TÉCNICAS Y HERRAMIENTAS DE INFORMÁTICA FORENSE 58

VII. ANEXO IV 63

ASPECTOS LEGALES Y ESTRATÉGICOS DEL EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL 63

A. CONCEPTOS GENERALES 63

B. LA INFORMÁTICA FORENSE EN EL PROCESO PENAL 65

C. CUESTIONES DE JURISDICCIÓN Y COMPETENCIA. COOPERACIÓN INTERNACIONAL 69

D. INTERVENCIONES EN LA ESCENA DEL HECHO 71

E. LA IDENTIFICACIÓN DE EVIDENCIA 71

F. CADENA DE CUSTODIA 72

G. COORDINACIÓN DE EXPERTOS, INVESTIGADORES Y FISCALES 73

H. DESTINO DE LAS EVIDENCIAS 74

VIII. ANEXO V 76

GLOSARIO 76

IX. ANEXO VI 82

FUENTES BIBLIOGRÁFICAS 82

FUENTES NORMATIVAS EXTRANJERAS Y LOCALES (NACIONALES Y PROVINCIALES) 87

II. PRESENTACION

En el marco de lo previsto en el *Convenio 5/14 de Investigación y Desarrollo en Informática Forense*, suscripto el 29 de mayo de 2014 entre la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, la Universidad FASTA y la Municipalidad de General Pueyrredón, por el cual se integró el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense y se acordó el desarrollo de los proyectos **INVESTIGA**, **FOMO** y **PAIF-PURI**, se comunica la conclusión y publicación de la versión validada y revisada del producto de este último, post implementación piloto, en el tiempo y formas previstos.

El Proyecto PAIF-PURI (Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de Información) tenía como objetivo el desarrollo de un Protocolo de Actuación en Informática Forense para ser adoptado y promovido por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo, en base a lo establecido en el Proceso Unificado de Recuperación de Información (PURI), oportunamente desarrollado por el Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA.

Acreditación

Es importante destacar que este Proyecto "Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de Información - PAIF-PURI" fue acreditado por el Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación e incorporado al Banco Nacional de Proyectos de Desarrollo Tecnológico y Social de la República Argentina, mediante Res. 062/14 de la Secretaría de Articulación Científico-Tecnológica.

Desarrollo del proyecto

A partir del 1 de junio de 2014 se trabajó, conforme lo planificado, en la determinación de los instrumentos e instancias formales necesarias para la definición, formalización y posterior validación de un Protocolo de Actuación Forense. A medida que el equipo de investigadores fue avanzando en el desarrollo del protocolo, fueron haciéndose evidentes otras necesidades (colaterales al protocolo pretendido) que se transformaron en nuevos requerimientos planteados por las autoridades del Ministerio Público que validaban el producto. En particular, en lo que respecta a los lineamientos referidos al abordaje de los casos, la planificación y gestión de la investigación penal y la litigación. En este sentido, se extendió el proyecto original para contemplar estos aspectos en el protocolo validado resultante, que se ha denominado ***GUÍA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL.*** Esta versión preliminar de la guía fue presentada el jueves 30 de abril de 2015 en el 3er Taller Técnico de Validación del *InFo-Lab*, con la presencia de autoridades de las tres instituciones integrantes del Laboratorio.

Asimismo, durante el trabajo de investigación, surgieron otras necesidades del Ministerio Público Fiscal, íntimamente vinculadas con la informática forense, que exceden el marco del proyecto, tales como la estimación de requerimientos para la creación y el funcionamiento de un laboratorio de informática forense, la elaboración y mantenimiento actualizado de un listado de contactos clave en la materia y la capacitación de personal en la especialidad. Existe un proyecto de trabajo complementario relativo a la primera de estas temáticas, es decir, los requerimientos y la gestión de los laboratorios de informática forense. Las restantes cuestiones serán consideradas en la agenda de trabajo del *InFo-Lab* a los efectos de evaluar la posibilidad de su desarrollo en el mediano plazo.

Respecto del Documento

En cuanto al documento de la Guía, en aras de respetar la necesaria visión de conjunto de la problemática, reconociendo a la vez la gran diversidad de tareas y usuarios implicados, ha sido estructurado en módulos, manteniendo un corpus principal altamente formalizado, vinculado con la labor informático-forense, bajo la forma de protocolo de actuación pericial, sujeto a estrictos estándares técnico-científicos, considerando el debido procedimiento de cadena de custodia. La guía integral contempla los diversos roles que pueden desempeñar los especialistas informáticos, conforme sus diferentes niveles de experticia (Rol de asesoramiento, Rol investigativo y Rol pericial) y las diversas responsabilidades (Identificación, Recolección, Adquisición y Pericia).

Existen otras funciones y servicios que resultan necesarios para la eficacia de las investigaciones vinculadas con evidencia digital y/o datos informáticos. Con frecuencia, los especialistas en informática deberán interactuar con ellos para poder desempeñar su labor. Si bien su regulación excede el área de incumbencia informática y los alcances de este Protocolo, se hace mención de los mismos para contar con un panorama general de las necesidades de un sistema eficiente de búsqueda y empleo de evidencia digital:

- ✓ *Punto de contacto permanente* (cf. art. 35 del Convenio de Budapest sobre cibercriminalidad): En el citado Convenio europeo se prevé la conformación de una red de puntos de contacto de los distintos Estados Parte, localizable las 24 horas del día, y los siete días de la semana, para asegurar la asistencia inmediata en la investigación. Sus funciones son las de aportación de consejos técnicos, la conservación de datos, la recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos. Si el punto de contacto no depende de las autoridades responsables de la cooperación internacional o de la extradición, deberá establecerse un procedimiento acelerado que asegure la actuación coordinada. Es importante que en Argentina se establezca una red semejante en el ámbito interjurisdiccional interno, y en relación con otros Estados.
- ✓ *Analistas de información criminal*: La utilidad de esta experticia no se agota en el estudio de problemáticas delictivas y en la ayuda para establecer prioridades y estrategias en materia de políticas de persecución penal. Su empleo también puede ser muy provechoso a la hora de analizar e interpretar grandes volúmenes de datos en casos complejos, o cuando se intenta detectar patrones delictivos asociables al accionar de un grupo criminal o sospechoso, asociar casos conexos, dar consistencia al material probatorio, etc.
- ✓ *Punto neutro judicial*: Se trata de infraestructuras únicas que permiten accesos directos a aplicaciones y bases del sistema judicial, de organismos estatales y de otras instituciones, facilitando y agilizando la obtención de información en tiempo real, la gestión de comunicaciones y solicitudes entre distintos organismos, etc.
- ✓ *Desarrolladores de herramientas de análisis forense*: Su campo de acción representa un insumo para la realización de las labores regidas por este protocolo. Es especialmente necesario cuando las prestaciones del software de análisis disponible no abarcan determinadas tareas o no son del todo fiables.

Asimismo, se han confeccionado y agregado guías complementarias relativas a temáticas que están sujetas a la permanente evolución tecnológica y/o a posibles cambios normativos o institucionales. Para facilitar su actualización sin necesidad de modificar el protocolo, se las ha incorporado en tres anexos técnicos: Anexo I - Evidencias en Medios Tecnológicos, Anexo II - Actas de levantamiento de soporte de evidencia digital y de levantamiento de evidencia digital, y Anexo III – Modelo PURI - Técnicas y Herramientas de Informática Forense.

En el Anexo IV se hacen una serie de consideraciones complementarias referidas a los aspectos legales y estratégicos del empleo de la informática forense en el proceso penal por parte del Ministerio Público Fiscal. Se han elaborado también diversas recomendaciones para ser tenidas en cuenta por los diferentes tipos de usuarios del instrumento. De esta forma, se ha procurado aportar en este anexo una visión integral del contexto en el cual se inserta la demanda y la utilización de la actividad informático-forense, dando cuenta de sus potencialidades, límites, exigencias, condicionamientos, costos y riesgos.

Por último, y con el propósito de facilitar la lectura e interpretación de los documentos principales, se ha incorporado en el Anexo V un glosario de términos, y en el Anexo VI un compendio de las fuentes bibliográficas y normativas consultadas.

Marco Legal

En cuanto al marco legal, el protocolo tiene como referencia básica el Código Procesal Penal de la Provincia de Buenos Aires y, ante la ausencia de regulación específica y de líneas jurisprudenciales firmes sobre las cuestiones vinculadas con la evidencia digital en el ámbito nacional, se ha tenido especialmente en cuenta la normativa constitucional y los aportes provenientes del derecho comparado. Es por tal motivo, que la guía integral y el protocolo en particular pueden representar un estándar válido para modelos procesales similares al bonaerense, adaptable a diferentes modelos procesales, incluso extranjeros, constituyendo un aporte sin precedentes y sumamente valioso para el sistema procesal penal en general.

Validación y Revisión

La primera versión de este documento fue formalmente entregada ante el Dr. Homero Alonso, a cargo de la Secretaría de Política Criminal, Coordinación Fiscal e Instrucción Penal, en el mes de mayo de 2015. Una vez analizada por las autoridades, con fecha 30 de noviembre de 2015, la Sra. Procuradora General dictó la Resolución General No 1.041/15 por la cual dispuso la aplicación de la Guía Integral de Empleo de la Informática Forense en los Departamentos Judiciales de Mar del Plata y Mercedes, a efectos de su evaluación por parte de los Ingenieros a cargo de las Oficinas Periciales correspondientes, en los siguientes términos:

Artículo 1: Disponer la aplicación de la "Guía Integral de empleo de la Informática Forense en el Proceso Penal" que se encuentra adjunta como ANEXO de la presente resolución en las tareas periciales informáticas que corresponda y se realicen en las Fiscalías Generales de los Departamentos Judiciales de Mar del Plata y Mercedes, a partir del 2 de diciembre de 2015.

Artículo 2: En el término de 90 días corridos a partir de la puesta en marcha del Protocolo de Actuación en Informática Forense basado en el Proceso Unificado de Recuperación de Información (PAIF-PURI) contemplado en la mencionada "Guía Integral de empleo de la Informática Forense en el Proceso Penal" deberá efectuarse, a través de las Fiscalías Generales que coordinarán la experiencia, un informe que contenga la evaluación de sus resultados a esta Procuración General con la finalidad de avanzar en la implementación en el resto de la provincia.

Cumpliendo con este cometido, los Ingenieros Fernando Greco (Departamento Judicial Mar del Plata) y Rubén Cangelosi (Departamento Judicial Mercedes) implementaron la Guía siguiendo rigurosamente sus indicaciones en sus respectivos departamentos y casos, validando la aplicabilidad y concluyendo en la extrema utilidad de la misma. En esta primera revisión se contemplan las recomendaciones que surgieron de los respectivos informes, dando lugar a la versión 2.

Asimismo, se ha tomado en consideración el *Protocolo de Cadena de Custodia* aprobado por Resolución General Nº 889/15, a fin de integrar sus disposiciones en todo cuanto sea compatible con esta Guía.

A los fines de facilitar la labor técnica de los especialistas, en relación a su desempeño forense, se decidió agregar como Anexo el modelo PURI actualizado, que servirá de guía rápida a esos fines.

Durante el proceso de revisión se han evaluado, además, otros documentos y guías de reciente producción para actualizar esta segunda versión , y se han recibido comentarios técnicos de otros expertos que accedieron al documento original.

Cumplida la validación de la Guía y su revisión, a los 12 días del mes de abril de 2016, se entrega a la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires esta versión 2 a efectos de que se recomiende su observación en el ámbito del Ministerio Público de la Provincia de Buenos Aires.

Equipo de Proyecto

El equipo técnico que desarrolló esta guía estuvo dirigido por la Ing. Ana Haydeé Di Iorio, e integrado por los siguientes investigadores: Ing. Bruno Constanzo (FI-UFASTA), Ing. Julián Waimann (FI-UFASTA), Ing. Ariel Podestá (FI-UFASTA y MGP), Ing. Fernando Greco (FI-UFASTA MP), Dr. Pablo Cistoldi (MP), Dra. Sabrina Lamperti (MP), Sr. Luciano Núñez (FCJS-UFASTA y MP) y Dra. María Fernanda Giaccaglia (FCJS-UFASTA).

Corresponde destacar la valiosa y comprometida participación del Ing. Roberto Giordano Lerena (FI-UFASTA), el Ing. Renato Rossello (MGP), el Dr. Fabián Uriel Fernández Garello (MP), la Ing. Daniela Barbera (MP) y el Dr. Esteban Lombardo (MP). Sus contribuciones y apoyo fueron claves para el desarrollo y éxito del proyecto.

III. PROTOCOLO DE ACTUACIÓN INFORMÁTICO FORENSE

Breve introducción

En este instrumento se presentan los aspectos básicos a considerar en las labores de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales en el proceso penal, a fin de garantizar la validez y eficacia probatoria de dichas actividades.

En el plano técnico, este protocolo se basa en el Proceso Unificado de Recuperación de Información – Proceso, en adelante PURI, desarrollado por el grupo de investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. PURI se nutre de procesos y guías de buenas prácticas en informática forense nacionales e internacionales, adaptándolas e integrándolas en un esquema de fases, etapas, tareas, técnicas y herramientas recomendadas. Se contemplan, de este modo, la planificación previa, identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

Lo relativo a los equipos de telefonía celular es objeto de tratamiento genérico, sin formularse mayores precisiones respecto de las específicas técnicas y herramientas de análisis pericial. Esta última cuestión está siendo objeto de otro proyecto de investigación y desarrollo.

Este protocolo deberá ser cumplido por los especialistas e idóneos informáticos (en sus distintos niveles y roles), ya que refleja consensos técnicos en la materia y ofrece suficiente respaldo jurídico para su labor. Fiscales e investigadores judiciales deben conocer adecuadamente el protocolo. El mismo es, por un lado, una herramienta para planificar y controlar el curso de una investigación penal. Por el otro, poder invocar su observancia otorga un importante sustento para la presentación eficaz de evidencias digitales y dictámenes periciales durante la labor de litigación.

Para desarrollar las tareas informático-forenses y utilizarlas procesalmente es imprescindible alinear la dimensión técnica con sus aspectos jurídico, estratégico y organizacional. Por tal motivo, el protocolo sólo podrá ser aplicado e invocado en forma eficiente teniendo debidamente en cuenta las nociones y recomendaciones generales que obran en el Anexo IV (Aspectos Legales y Estratégicos del Empleo de la Informática Forense en el Proceso Penal).

Consideraciones generales

La evidencia digital

Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.). Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. La evidencia digital presenta características que la diferencian de las restantes clases de evidencia física. Se la puede duplicar de manera exacta (permitiendo manipular la réplica sin alterar el original), está sujeta a riesgos específicos de posible alteración y/o eliminación, su localización puede ser muy dificultosa, entre otras. Asimismo, el empleo de la evidencia digital en los procesos judiciales -especialmente en los casos penales- presenta complejos problemas jurídicos vinculados con el derecho a la intimidad y al secreto de las comunicaciones, las posibles afectaciones a terceras personas, etc.

Roles y niveles de actuación procesal

A lo largo de la actividad estratégica del Ministerio Público Fiscal, y de acuerdo con las particularidades de cada caso, podrán ser necesarios distintos tipos de aportes de la informática forense. Los especialistas podrán entonces desempeñar diversos *roles procesales*:

- ✓ **Rol de Asesoramiento**: En ocasiones, el fiscal o el director de la investigación puede necesitar la opinión de un experto para desarrollar tareas investigativas o probatorias. Por ejemplo, planificar la ejecución de un registro domiciliario y/o evacuar consultas durante el procedimiento, precisar los datos que han de requerirse a un proveedor de servicios, fijar puntos de pericia o interrogar al perito de la contraparte. Todas estas actividades requieren contar con asesoramiento técnico.
- ✓ **Rol Investigativo:** En algunos casos y/o momentos de un proceso, suele requerirse la intervención de un especialista informático para ejecutar medidas de investigación (ej.: secuestro de equipos informáticos, volcados de memoria, obtención de imágenes de disco, etc.).
- ✓ **Rol Pericial:** Bajo este rol, el experto aporta sus conocimientos especiales para conocer o apreciar algún hecho o circunstancia pertinentes a la causa (art. 244 del CPP).

Debemos tener presente que los expertos no tienen a su cargo ciertos roles o responsabilidades, tales como la custodia de evidencia (más allá del tiempo que insuma la labor técnica), o el rol de fedatario.

Por otra parte, no siempre es requerido el mismo nivel de conocimientos y habilidades. En el protocolo se distinguen cuatro niveles:

- ✓ **Responsable de Identificación (RI):** Persona idónea para las tareas de identificación, no necesariamente es un especialista informático.
- ✓ **Especialista en Recolección (ER):** Persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital. Puede necesitar el auxilio de un Especialista en Adquisición.
- ✓ **Especialista en Adquisición (EA):** Está autorizado, entrenado y calificado para recolectar dispositivos y para adquirir evidencia digital de éstos (ej.: imágenes de disco, volcados de memoria).
- ✓ **Especialista en Evidencia Digital (EED):** Experto que puede realizar las tareas de un Especialista en Adquisición, y además tiene conocimientos específicos, habilidades y aptitudes que le permiten manejar un amplio rango de situaciones técnicas, tales como la realización de una pericia (cf. art. 244 del CPP; arts. 2° y 7° inc. 13 de la ley 13.016 de Ejercicio de las Profesiones en Ciencias Informáticas).

Principios generales en el manejo de Evidencia Digital

Existen reglas comunes que rigen la labor de los especialistas e idóneos en las diferentes fases de actuación. La evidencia digital debe poseer cuatro características esenciales: relevancia, suficiencia, validez legal y confiabilidad.

- ✓ **Relevancia.** La evidencia debe ser útil para las necesidades investigativas y/o los puntos probatorios de cada caso concreto. Ha de revestir pertinencia respecto de dichos fines y no ser sobreabundante o superflua (ver art. 338 del CPP). Este principio opera fundamentalmente como criterio de selección de evidencia. El experto debería saber qué lugar ocupa una determinada evidencia en el plan de investigación penal y/o en la actividad de litigación del Fiscal en cada caso concreto. Ante la duda, o si se estimara que podría ser útil, el especialista debe consultar con el director de la investigación, aportándole su opinión técnica.
- ✓ **Suficiencia.** Este principio complementa al anterior. Las evidencias obtenidas y eventualmente analizadas de-

berían ser suficientes para lograr los fines investigativos buscados mediante ellas, y/o para convencer al tribunal acerca de los puntos para los cuales fueron ofrecidas como prueba. Frente a situaciones dudosas, deberá consultarse con el director de la investigación.

- ✓ **Validez legal.** Para que la evidencia sea admisible, debe haber sido obtenida respetando las garantías y formas legales. Por ello:
  - El experto debe cumplir con las disposiciones legales y reglamentarias propias de su actuación.
  - Cuando una acción implique injerencia en derechos fundamentales (secuestro de dispositivos, análisis de comunicaciones personales, etc.), se deberá constatar la previa autorización judicial o la orden del director de la investigación.
  - No debe adoptar decisiones ni llevar a cabo acciones que sean ajenas al área de la propia incumbencia.
- ✓ **Confiabilidad.** La evidencia debe ser convincente, apta para probar lo que se pretende con ella. Esto se refiere no sólo a las características que una evidencia digital posee en sí misma, sino también a los procedimientos de obtención, preservación, análisis y presentación ante el tribunal.

  Para asegurar la confiabilidad, el proceso de manejo de evidencia digital debe ser justificable, auditable, repetible y reproducible:
  - **Justificable:** Se debe poder justificar todos los métodos y acciones realizadas en el manejo de la posible evidencia digital. La justificación puede darse demostrando que las acciones y métodos utilizados son el mejor curso de acción posible, u otro especialista validar y verificar el proceso realizado.
  - **Auditable:** El Especialista en Adquisición (EA) y el Especialista en Evidencia Digital (EED) deben documentar todas las acciones que realizan y justificar todas sus decisiones en las etapas del proceso. Se busca que cualquier especialista externo (consultor o perito de parte) pueda ser capaz de evaluar el proceso y determinar si se ha aplicado una metodología, técnica o proceso adecuado.
  - **Repetible:** Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con las mismas herramientas, en las mismas condiciones, en cualquier momento. Si un EA o EED repite los procedimientos documentados, debe arribar a los mismos resultados que el Especialista que realizó el análisis.
  - **Reproducible:** Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con herramientas distintas, en condiciones distintas, en cualquier momento.

  A fin de cumplir con esas cuatro reglas de manejo de la evidencia digital, se han de observar las siguientes pautas:
  - Debe minimizarse el manejo de la evidencia digital original con valor investigativo y/o probatorio. Si es necesario acceder a los datos originales, el especialista debe ser competente para hacerlo y capaz de atestiguar explicando la importancia y las implicaciones de sus acciones.
  - Cualquier acción que implique una alteración irreversible de la evidencia debe ser previamente informada al director de la investigación, y debidamente documentada (ver art. 248 del CPP).
  - Quien realice cada acción o cambio vinculado con evidencia digital debe responsabilizarse de lo actuado y documentarlo en forma fidedigna.

Procedimientos de consulta

Con frecuencia será necesario que el especialista informático realice consultas al agente fiscal o al director de la investigación. Por ejemplo: para determinar cuáles evidencias son relevantes, fijar un orden de relevancia, esta-

blecer cuándo la evidencia es suficiente para un determinado propósito investigativo o probatorio, conocer los límites de una autorización legal o judicial respecto de un acto o procedimiento concreto, elaborar criterios o pautas para el filtrado de datos, adoptar decisiones respecto de evidencia volátil, realizar o no determinadas operaciones que pueden alterar o destruir evidencia, actuar en forma coordinada con expertos de otras disciplinas, aclarar puntos de pericia, etc.

Al efectuar una consulta, el especialista debe informar la situación suscitada, los posibles cursos de acción (con sus riesgos y probables beneficios) y, cuando lo estimare conveniente o le fuere requerido, formular las sugerencias o recomendaciones que se consideren pertinentes desde la propia incumbencia. Se hará constar la decisión adoptada, con mención de día y hora, medio de comunicación empleado y magistrado o funcionario consultado.

Frente a situaciones de urgencia que no admitan demora o impidan la consulta, se documentará tal circunstancia y se indicará el curso de acción escogido, con breve mención de las razones que motivaron esa opción. El especialista interviniente deberá estar preparado para justificar su decisión en audiencia testimonial y/o en informe escrito.

Fases de intervención informático forense

Las actividades informático-forenses han sido divididas en diferentes fases.

Las fases descriptas en este protocolo no necesariamente se vinculan en forma secuencial. La labor investigativa y procesal suele estar sujeta a una constante retroalimentación. El resultado de cada paso, o la acción de los restantes protagonistas del proceso penal, pueden tornar necesario reformular las medidas previstas de antemano (por ejemplo: el resultado de una pericia informática puede llevar a solicitar un nuevo registro domiciliario o una nueva intervención telefónica). No obstante, cada una de las fases aquí identificadas puede ser vista como un proceso de trabajo específico, con un núcleo de tareas altamente estandarizable. Las fases o procesos de trabajo son los siguientes:

1. ***Relevamiento e Identificación*** de los equipos, dispositivos y todo otro tipo de medio de almacenamiento cuya obtención y/o examen se considere pertinente y útil para una investigación penal.
2. ***Recolección*** de equipos, dispositivos y medios de almacenamiento.
3. ***Adquisición de datos volátiles***. Se trata de la obtención de datos existentes en dispositivos encendidos que pueden perderse definitivamente al ser apagado el artefacto.
4. ***Cadena de custodia y preservación.*** Por cuestiones de índole práctica, se los trata como proceso de trabajo separado, pese a que suelen atravesar varias de las otras fases.
5. ***Adquisición de medios de almacenamiento persistentes***.
6. ***Labores periciales***.

En el Anexo III.I (Modelo PURI) se ofrece una guía introductoria de las labores a desempeñar por el área técnica de informática forense. Dicha referencia es complementada con las dimensiones jurídica y estratégica, y con la división de roles y niveles de actuación.

FASE DE RELEVAMIENTO E IDENTIFICACIÓN

Concepto y requisitos generales

Esta fase consiste en la *identificación de los equipos, dispositivos y todo otro tipo de medio de almacenamiento* cuya obtención y/o examen se considere pertinente y útil para aspectos específicos del plan de investigación penal delineado en un caso concreto por el Fiscal y/o su equipo. Dicho proceso de trabajo suele ser necesario en investigaciones o etapas investigativas de carácter planificable. Pese a que esta fase no está destinada exclusivamente a informáticos, se considera oportuno su detalle dado que en casos complejos puede requerirse que el experto brinde asesoramiento. Por otra parte, frecuentemente esta será la ocasión para que los integrantes del equipo informático forense hagan un primer relevamiento del caso y se familiaricen con lo actuado hasta ese momento. Cuando se prevean varias instancias de intervención informático forense, es recomendable confeccionar una ficha del caso, que irá siendo actualizada durante el curso del proceso.

Básicamente, el propósito de las labores de identificación es el de preparar adecuadamente las fases de recolección y/o adquisición, para garantizar que la evidencia digital que se procura obtener sea *relevante, suficiente, confiable y legalmente válida:*

- ✓ Los criterios de relevancia deben ser establecidos en forma coordinada entre el equipo de investigación y el Responsable de Identificación (RI). Desde esta perspectiva, se ha de realizar un relevamiento de los elementos que podrían ser útiles para alcanzar las metas investigativas previamente trazadas (esclarecer los hechos, reunir pruebas para sustentar la hipótesis trazada, decomisar bienes, etc.), y establecer la clase de proceso de trabajo exigida para cada elemento (recolección, volcado de memoria, empleo de herramientas de triage, obtención de imágenes de disco, etc.). Es recomendable, asimismo, que en esta fase se establezca un orden de relevancia o prioridad entre todas las evidencias a obtener.
- ✓ Para cumplir el requisito de suficiencia de la evidencia, se deberá atender principalmente a evitar la pérdida de los datos, priorizando los objetos de mayor interés y las fuentes de evidencia más volátil. Además debe tenerse en cuenta que muchos objetos informáticos pueden ocultar información, de modo que su función puede no resultar tan notoria. Por lo tanto, se recomienda considerar todas las situaciones y decidir, en función del caso, qué acciones se pueden llevar a cabo y qué tipo de dispositivos puede abarcar la identificación.
- ✓ La adecuada identificación de los equipos y dispositivos a los que se busca acceder y el conocimiento previo del lugar donde los mismos se encuentran, permiten planificar eficazmente los procesos de recolección y/o adquisición. De esta forma, se podrá contar con personal debidamente preparado y equipado para obtener evidencias de alto grado de confiabilidad probatoria.
    - Poder prever cuáles dispositivos son transportables y cuáles no (por su volumen, número, limitaciones legales, etc.) permite encomendar un procedimiento a la clase y número de especialistas necesarios. Los dispositivos transportables serán objeto de recolección, para posterior análisis en el gabinete pericial. Los no transportables serán procesados y/o adquiridos en el lugar.
    - Asimismo, determinar la fecha y horario ideal para realizar un procedimiento, ayuda a establecer si será necesario o útil proceder a la adquisición de datos volátiles.
- ✓ En esta fase, lo relativo a la validez legal de la prueba es responsabilidad exclusiva del Fiscal o Ayudante Fiscal interviniente.
- ✓ La evidencia relevante puede hallarse en memoria, disco, dispositivos móviles, red, sistemas de almacena-

miento en la nube, etc.[1] Según el tipo de investigación, se analizará si es necesaria la obtención de uno o varios de estos tipos de evidencia, de acuerdo con lo que cada una de éstas puede aportar. En especial, cuando el director de la investigación lo solicite, los especialistas prestarán asesoramiento acerca de la pertinencia técnica de la interceptación y/u obtención de evidencia en la nube (datos de tráfico, comunicaciones, contenidos).

Medios de Identificación

La evidencia digital puede residir en equipos (disco rígido, memoria), red y otros dispositivos electrónicos. Cada clase de contenedor presenta exigencias especiales para su obtención. Para contar con un panorama más completo, se debe consultar el Anexo I, "Evidencias en Medios Tecnológicos", que integra el presente Protocolo.

Previo a la realización de medidas tales como un registro domiciliario, pueden utilizarse variadas técnicas para identificar los equipos y dispositivos donde se podría hallar evidencia digital y/o determinar un usuario involucrado. A modo de ejemplo se detallan algunos medios de identificación, enunciación que no es exhaustiva:

- ✓ Identificación de dirección IP:
  - Las direcciones IP asignadas a un equipo están registrados en los correos electrónicos enviados y en la navegación efectuada en Internet (en el caso de los correos electrónicos de proveedores web como Gmail, Yahoo!, Hotmail, las direcciones IP están encriptadas; para obtener esta información se debe enviar un oficio judicial al Proveedor de Correo). El Proveedor de Internet que brinda el servicio (Proveedor ISP, por ejemplo, Speedy de Telefónica de Argentina, entre otros) guarda los registros de asignación de direcciones IP de sus clientes.
  - En el sitio web http://www.lacnic.net/ [2] se podrá determinar qué Proveedor de Servicios de Internet (ISP) tiene asignada una determinada dirección IP.
  - Una vez identificado el Proveedor ISP, podrá consultársele a éste por los datos personales del cliente a quien se asignó una IP en una fecha y hora determinada[3].
- ✓ Identificación de dirección MAC:
  - Debe solicitarse esta información al administrador de red. Una alternativa es realizar un análisis de volcado de red de los equipos intervinientes. Este análisis se realiza dentro de un ámbito determinado (instituciones, locutorios, etc.) para conocer cuál es el tráfico de una red en un segmento de tiempo, y así determinar a posteriori las comunicaciones de los dispositivos intervinientes.
- ✓ Identificación de teléfonos celulares y fijos:
  - Determinar titularidad y domicilio de facturación a través de las empresas prestatarias del servicio de telefonía.
- ✓ Identificación de objetos y/o información relacionada: Sumado a la identificación del equipo puede ser necesario identificar y determinar qué otros elementos o datos aparecen vinculados, por ejemplo: Usuarios del sistema, Proveedores de Servicio, Software, entre otros. A tal fin se presentan algunas de las acciones que

[1] Ver anexo 1 "Evidencias en medios tecnológicos".

[2] LACNIC (Latin American and Caribbean Internet Address Registry) es uno de los Registros Regionales de Internet, que administra las direcciones IP de la Región de América Latina y el Caribe. Existen otros Registros Regionales como: American Registry for Internet Numbers (ARIN) para América Anglosajona; RIPE Network Coordination Centre (RIPE NCC) para Europa, el Oriente Medio y Asia Central; Asia-Pacific Network Information Centre (APNIC) para Asia y la Región Pacífica; y African Network Information Centre (AfriNIC) para África.

[3] Tener en cuenta el Huso horario de Argentina al momento de pedir información al proveedor de Internet - ISP. Ej: huso horario de Argentina es UTC-3.

pueden colaborar en cada una de estas identificaciones durante toda la etapa de investigación:

- Identificación de usuarios: Requerimiento de información de usuarios, dirigido al administrador de un servicio o de una red (logs de conexión, datos de usuario), entrevistas con personal de la entidad damnificada, etc.
- Identificación de software utilizado: Datos aportados en la denuncia, informes suministrados por la empresa, etc.
- Identificación de dispositivos de red, nombres y claves de Wi-Fi, etc.

✓ Identificación de evidencia en memoria, disco y red. Según el tipo de investigación, se analizará si es necesaria la obtención de todos o algunos de estos tres tipos de evidencias, de acuerdo con lo que cada una de éstas puede aportar.

Cuestiones de jurisdicción y competencia. Mecanismos de cooperación.

Durante la fase de identificación, pueden surgir cuestiones de jurisdicción legal y/o de competencia judicial. También pueden evidenciarse necesidades de cooperación y/o coordinación interjurisdiccional (ej.: procedimientos simultáneos en distintas jurisdicciones). El responsable comunicará al Fiscal interviniente cualquier novedad o dato que pudieren tornar necesario el análisis de estas cuestiones.

Perfil del Responsable de la Identificación

Esta labor puede estar a cargo de un investigador judicial debidamente capacitado en la materia, o personal auxiliar del Laboratorio de Informática Forense. La identificación de equipos y dispositivos de interés es parte de un trabajo en conjunto. El Responsable de Identificación (RI) deberá conocer las finalidades específicas perseguidas mediante las medidas investigativas que se prevé realizar. Asimismo, hará saber al director de la investigación los aspectos concretos de la labor encomendada que pudieren ser relevantes (demoras, costos, riesgos de pérdida de datos, requerimientos técnicos, etc.). El RI requerirá asesoramiento informático forense en las cuestiones específicas que escapen a sus conocimientos, y contará con el auxilio de quien ejerza el rol de nexo con instituciones públicas y privadas.

Pedidos de medidas de injerencia. Control del contenido de la orden.

El RI tendrá en cuenta que, una vez identificados los objetos, equipos (y eventualmente usuarios) relevantes para la investigación, el Ministerio Público Fiscal necesitará acceder a los mismos, documentando su hallazgo y obtención. Frecuentemente, dicho acceso sólo será posible mediante una medida que implique injerencia en derechos constitucionalmente protegidos (por ejemplo: orden de registro y secuestro de evidencia, acceso a datos volátiles, etc.). Salvo en situaciones excepcionales, dicha clase de medidas sólo procede mediante orden judicial, que debe ser solicitada por el Fiscal (o el Ayudante Fiscal) al Juez competente. Ante este escenario, el RI deberá estar disponible para indicar a la Fiscalía la clase de operaciones que se prevé llevar a cabo durante el procedimiento (secuestro de artefactos y/o de otros efectos, adquisición de datos volátiles, acceso a claves, empleo de herramientas de *triage* en el lugar, adquisición de imágenes de disco, etc.), a fin de posibilitar que tales operaciones estén incluidas en la solicitud de orden judicial, y se prevea la modalidad de ejecución más adecuada (ej.: horario del procedimiento, posibilidad de conectar un dispositivo al equipo para adquirir la memoria volátil, generar denegaciones de servicio en redes WiFi, bloquear comunicaciones de red, entre otras).

Los especialistas que vayan a intervenir en el procedimiento deberán corroborar que existe una orden judicial y

que la misma autoriza la realización de las operaciones técnicas previstas.

FASE DE RECOLECCIÓN

Concepto general. Escenarios posibles

Esta fase comprende la recolección de los objetos contenedores de evidencia digital. Dicha actividad puede llevarse a cabo en varias situaciones posibles. Desde el punto de vista temporal, puede ser previamente programada (en cuyo caso está precedida por la fase de identificación), o aparecer como una medida necesaria en un contexto de urgencia. En cuanto a la modalidad de habilitación, puede ser producto de una orden judicial (allanamiento, secuestro, orden de presentación), derivar de una solicitud o autorización de una persona o entidad (sea la víctima o un tercero), o enmarcarse en un procedimiento policial urgente en la escena del crimen. Los niveles de urgencia también inciden sobre la clase de funcionarios que actuará (especialistas informáticos, investigadores, personal policial). Asimismo, los lugares en los que se interviene pueden presentar características muy disímiles. Por otro lado, en algunos casos será necesario desplegar la recolección en forma prácticamente paralela con otras fases o procesos de trabajo (ej.: adquisición de datos volátiles, adquisición de imágenes de disco).

Nota: En este protocolo no se regula la labor policial. Es responsabilidad de los magistrados del Ministerio Público Fiscal instruir debidamente a los organismos policiales y fuerzas de seguridad respecto del procedimiento a seguir en casos urgentes. En tal sentido, se considera recomendable emitir una instrucción general uniforme para toda la Provincia.

Principios básicos de actuación

Objetivos

La recolección debe realizarse de un modo tal que asegure la utilidad procesal de los artefactos recogidos, en sus distintos aspectos. Los principios de relevancia, suficiencia, confiabilidad y validez legal deben ser plenamente observados. En particular, el principio de confiabilidad exige garantizar la identidad e integridad de la evidencia. Eventualmente y a esos fines, será necesaria la inspección y recolección de otros objetos vinculados con los dispositivos.

Procedimiento

El levantamiento debe ser realizado empleando las técnicas y los medios adecuados al tipo de evidencia, como se detalla en el presente documento. El especialista deberá actuar dentro de los límites legales y sin exceder los alcances de la autorización judicial. En caso de duda, consultará al director de la investigación.

Registración

Es indispensable una correcta documentación de lo actuado, conforme la normativa vigente.

Variables a considerar

Los especialistas que intervengan en la fase de recolección deben tener en cuenta diversas variables:

- ✓ Preparación:
  - Cuando la recolección se vaya a realizar en el marco de medidas previamente planificadas (ej.: orden de allanamiento), deberán conocer lo actuado en la fase de relevamiento e identificación, como asimismo el exacto contenido de la orden judicial.

- En dichos casos, procurarán contar con un adecuado conocimiento del lugar (planos del sitio, contacto con víctimas o testigos clave, etc.).
- Prepararán el equipamiento necesario para la labor a desplegar.

✓ Actuación en equipo:

- Si actuaran conjuntamente con especialistas de otras disciplinas y/o en un equipo, se ajustarán a las pautas de intervención propias del rol asignado.

✓ Aseguramiento de la prueba:

- Se deberá evitar la alteración o supresión de evidencia digital, ya sea por la exposición a factores del ambiente (ej.: imanes, campos magnéticos), por la acción de personas presentes o por terceros que pudieren operar a través de herramientas remotas.
- Cuando el procedimiento se lleve a cabo sobre artefactos interconectados, se procurará aislar el perímetro de red dentro de los límites de la autorización judicial.

✓ Inspección de la escena y de los dispositivos:

- El ER tomará nota de las características físicas del área circundante que resulten pertinentes para su labor.
- Al determinarse la ubicación y el estado de las evidencias halladas en el lugar procedimiento, se deberá tomar fotografías y/o grabar video filmaciones, realizar un plano a escala y efectuar las anotaciones pertinentes para el posterior volcado en el acta. En especial, se han de fotografiar las conexiones, cables y frente de los dispositivos. Las tomas fotográficas podrán estar a cargo de un fotógrafo especializado del laboratorio pericial o del mismo especialista en recolección, quienes podrán arbitrar los medios necesarios para tomar las imágenes que resulten relevantes para la investigación. Se coordinará con el responsable del procedimiento (o, en su caso, con el director de la investigación), quiénes y de qué modo llevarán a cabo estas medidas. De acuerdo con la criticidad del caso y de la prueba, se procurará tomar las medidas necesarias para dar fiabilidad a las fotografías y/o filmaciones efectuadas (por ejemplo: obtener el hash de una fotografía, incluirlo en el acta pertinente y almacenarlo junto con la fotografía en un CD).
- La inspección (con su pertinente registración) incluirá:
  - todos los artefactos encontrados, incluyendo a aquellos que no sean recolectados,
  - las conexiones de red y características distintivas de los equipos,
  - los medios externos que puedan contener capacidad de almacenamiento persistente (Ej.: USB, tarjetas de memoria, entre otros).

✓ Evidencias y personas vinculadas con los artefactos a recolectar:

- Deberá prestarse especial atención a eventuales anotaciones, documentación, manuales y otros objetos que pudieren contener información trascendente para el análisis de la evidencia digital. En su caso, se procederá a su fotografiado y levantamiento.
- Cuando en el marco de su intervención, el especialista observare la existencia de soportes digitales conteniendo datos volátiles, consultará si existe autorización para su adquisición en el lugar. En caso afirmativo, procederá a realizarla. Si no poseyere las competencias o equipamiento necesarios, requerirá el auxilio de un Especialista en Adquisición (EA).

- Si en el lugar se hubieren identificado testigos con información potencialmente útil para el desarrollo de la labor, se procurará interrogarlos en debida forma, dejándose constancia y dando conocimiento al director del procedimiento.

✓ Evidencias a recolectar:

- Durante los procedimientos planificados, puede llegar a ser necesario redefinir parcialmente la identificación efectuada previamente. En los casos urgentes y en supuestos de entrega voluntaria, se deberá identificar en el lugar el material a recolectar.
- Se recolectará evidencia suficiente a los fines investigativos y/o probatorios previamente establecidos (principio de suficiencia), evitando, a su vez, recolectar evidencia irrelevante (principio de relevancia).
- Para seleccionar eficazmente los artefactos que serán recolectados, la búsqueda se orientará hacia aquellos equipos que verdaderamente actúen como medio de almacenamiento; obviándose la recolección de los artefactos que carezcan de todo valor investigativo. En tal sentido, descartada la posibilidad de ser fuente de evidencia digital, se evaluarán principalmente estos factores: falta de utilidad pericial, ausencia de rastros materiales de interés en el soporte, carencia de valor probatorio como evidencia material, destino del bien (no decomisable ni restituible a la víctima). En caso de duda, deberá consultarse al director de la investigación. Con ese propósito, se tendrán en cuenta diversas circunstancias y posibilidades, por ejemplo:
  - Identificación de entorno virtual:
    - Detectar la utilización de un servidor externo central, su modo de funcionamiento y si se trata de un cluster y/o un entorno virtualizado.
    - Determinar la presencia de:
      - Hipervisores.
      - Máquinas virtuales.
      - Almacenamiento distribuido.
  - Identificación de almacenamiento en Red Local:

    Establecer si las máquinas involucradas se encuentran en red, si se utiliza hub, switch o router, o un access point, e identificar el servidor central.
- Cuando el material inspeccionado sea muy voluminoso, exista excesiva cantidad de información, se tenga conocimiento preciso de los datos o clase de datos que se buscan, o se encuentren afectados derechos de terceros, se ponderará el uso de herramientas de muestreo rápido (*triage*) para precisar el grado de relevancia de cada dispositivo. En caso de duda, deberá consultarse al director de la investigación.

✓ Manipulación y levantamiento de los objetos:

- Los efectos deben manipularse de modo seguro y de forma adecuada, evitando la exposición personal a descargas eléctricas y/o quemaduras. Es recomendable el empleo de guantes aptos para tales fines.
- Cuando en el procedimiento se estuviere buscando también otro tipo de evidencia (huellas dactilares o rastros de ADN), se utilizarán guantes especiales para no alterar, encubrir o hacer desaparecer dichas pruebas de los equipos o área donde se encuentre un sistema informático.
- Si se advierte que el equipo informático o electrónico está destruyendo evidencia, inmediatamente debe desconectarse e interrumpirse su alimentación eléctrica.

- Si los equipos se encuentran apagados, no deben encenderse, salvo circunstancias justificadas y previa consulta al director de la investigación.
- No deben utilizarse los artefactos que vayan a secuestrarse ni debe buscarse información en ellos, excepto cuando también se prevea adquirir datos volátiles o se efectúen operaciones de *triage.*
- Salvo en los casos en que proceda la adquisición de datos volátiles, se deben desconectar las fuentes de energía del dispositivo. En caso de duda, deberá consultarse con el director de la investigación.
- Si un dispositivo que fue hallado encendido no se apaga al ser removido el cable de alimentación, se localizará y removerá la batería.
- Si el equipo está encendido, deberá fotografiarse la pantalla, con la nitidez suficiente como para visualizar su contenido.
- También debe desconectarse el cable de red Ethernet, si hubiera alguno, ya que puede transmitir energía eléctrica y mantener activas algunas funciones del equipo luego del apagado.
- Las baterías deben ser removidas y guardadas en un lugar seguro y separado de la misma máquina, a fin de prevenir un encendido accidental.
- En la medida de la autorización legal, y previa inspección, se recolectarán manuales, documentación y anotaciones vinculables con los dispositivos y/o con su presunto contenido.
- Si las circunstancias lo aconsejan, se analizará la posibilidad de levantar los componentes de un dispositivo que se consideren relevantes y suficientes (ej.: discos rígidos). En caso de duda, siempre se consultará al director de la investigación.

✓ Recomendaciones para la clasificación, embalaje y rotulado:

- Se ha de recordar que éste será el primer paso del procedimiento de cadena de custodia.
- Se debe registrar todo número de identificación de cada dispositivo.
- Se recolectará todo cable, accesorio o conexión, colocando etiquetas en los cables para facilitar una eventual reconexión.
- Si hay un disco, pendrive, cinta, CD u otro medio de grabación conectado en alguna unidad, es necesario retirarlo, protegerlo y guardarlo en un contenedor adecuado.
- Debe sellarse con cinta cada entrada o puerto de información, como también los tornillos del equipo a fin de que no se puedan remover o reemplazar las piezas internas del mismo. Se recomienda el uso de cinta de evidencia.
- La evidencia recolectada deberá ser clasificada y embalada según los específicos requerimientos técnicos de cada objeto, a los fines de preservar la integridad de continente y contenido.
- Se sugiere utilizar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta con aquéllas, pueden utilizarse bolsas de papel madera). Se evitará el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática, con riesgo de destruir o alterar datos.
- Se procurará que no se incluya en un mismo embalaje, evidencias que tengan diferentes destinos periciales.
- Cada elemento deberá ser rotulado por separado.

- Se recomienda que el rótulo sea preimpreso y de carácter inviolable[4].
- Se debe adherir el rótulo confeccionado al efecto o al embalaje que lo contiene. No debe efectuarse el rotulado sobre el propio elemento o su embalaje.
- El especialista deberá controlar el llenado completo del rótulo, conforme las siguientes reglas:
  - El rótulo debe escribirse con tinta indeleble, de manera concisa, precisa y exacta, con letra clara imprenta, legible y comprensible.
  - Su contenido debe ajustarse a la información verdadera y no debe tener enmiendas ni tachaduras.
  - El registro de lugar, fecha y hora debe consignarse en números arábigos. La fecha se escribirá en la secuencia: día (00), mes (00), año (0000) y la hora en el formato de 00:00 hasta 24:00 horas.
  - Debe contar con la firma del Especialista en Recolección/ Adquisición, de la autoridad judicial a cargo y de, al menos, un testigo.
  - En caso de no contarse con etiquetas, se sugiere llevar planillas preimpresas con nº de investigación, nº de efecto, folio, lugar y lugar para las firmas.
- Al momento de la colocación del rótulo, el ER deberá tener en cuenta:
  - Cuando los equipos o dispositivos han sido embalados en bolsas plásticas, de papel u otro tipo, los rótulos deben adherirse en el cierre de las mismas, como medida de seguridad a fin de evitar alteraciones de su contenido, de tal manera que al abrir la bolsa se rompa el rótulo.
  - Cuando los equipos o dispositivos secuestrados, poseen características tales que no se aconseja su preservación dentro de un embalaje (CPU, notebooks, servidores, etc.) los rótulos diligenciados se colocan en todos los puntos que permitan el acceso sea a su interior (desarme) como también a su manejo (despliegue de pantalla en notebook) o a cualquier puerto de entrada o salida de información que posea (USB, red, lectoras, etc.); confirmando que queden bien adheridos de tal forma que al abrirlos o retirarlos, indefectiblemente se rompan.

✓ Documentación y registro de lo actuado:

- El especialista deberá suscribir las actas pertinentes, que se labrarán cumpliendo las formalidades previstas en el Código Procesal Penal (arts. 117/120) y, en su caso, con las exigencias específicas relativas a la documentación de registros domiciliarios (arts. 219 y 223), requisas (art. 225), secuestros (art. 226), inspección y reconstrucción (arts. 212/213, 216/218).
- El especialista deberá verificar que el registro documental se haga de un modo descriptivo, mediante un relato preciso, detallado, realista e imparcial, y suministre una noción clara del lugar, de toda incidencia que hubiere acontecido durante el procedimiento, de las evidencias detectadas y el estado en que fueron halladas. Constatará, además, que las actas se complementen con fotografías, filmaciones y planos del lugar y del sitio de ubicación de cada efecto, y las consultas efectuadas al director de la investigación, en la medida requerida en cada caso. Todo ello a fin de asegurar que el procedimiento pueda ser reconstruido por terceras personas que deban recrear el momento a posteriori.
- En caso de secuestro o recepción de dispositivos, deberá completarse el Acta de Levantamiento de Soporte de Evidencia Digital (LSED). Al respecto, ver la fase de Cadena de Custodia.
- Se recomienda obtener una copia de las actuaciones en soporte digital, en formato compatible para su

[4] Acerca de los modelos y requerimientos técnicos de cintas y rótulos, puede consultarse al equipo Info-Lab.

eventual incorporación en el Sistema Informático del Ministerio Público (SIMP).

- Es recomendable que cada evidencia recogida sea identificada con un método uniforme de identificador único (código de barras, expresiones regulares, entre otros), consignándose dónde se levantó, en qué estado se encontraba, con cuáles equipos o sistemas estaba conectada, quién efectuó la recolección de la misma y qué recaudos se tomaron; actuándose siempre ante la presencia y la vista de los testigos que hayan sido convocados al procedimiento.
- Deberá asignarse un identificador único para cada efecto, que figurará coincidentemente en el acta de procedimiento, documentación anexa, rotulado y/o embalaje.

Recaudos adicionales para teléfonos móviles

Ante el hallazgo de equipos móviles, y/o cualquier otro dispositivo que utilice la red celular de comunicación, se adoptarán los siguientes recaudos adicionales:

- ✓ Dependiendo de las particularidades del caso y del tipo de dispositivo, puede considerarse la posibilidad de no apagar los equipos, poniéndolos en modo avión. Otra alternativa, que debe ser consultada con el director de la investigación debido a los riesgos que implica, es la de mantener el dispositivo en modo normal hasta no culminar con la medida, dejando para última instancia el detalle de los mismos en cuanto a su identificación, para permitir que durante ese lapso se puedan colectar mensajes de texto y/o el registro de llamadas entrantes de otros posibles involucrados, pero sin permitir que el tenedor del teléfono los borre. A tal fin, se recomienda dejar los equipos a la vista durante el procedimiento.
- ✓ Se debe dejar constancia del secuestro (cuando éste proceda), detallando número de tarjeta SIM e IMEI (Identidad internacional de equipo móvil por su sigla en inglés). El número de SIM está ubicado en uno de los lados del chip en el interior del teléfono.
- ✓ Previamente al embalaje, se ha de separar la batería, cuando ello sea posible.
- ✓ Se recomienda almacenar el equipo en bolsas especiales, que aíslen radiofrecuencia.

ADQUISICIÓN DE DATOS VOLÁTILES

Nociones generales

Este proceso de trabajo consiste en la extracción de datos volátiles, que sólo se encuentran presentes en equipos encendidos y suelen ser eliminados con el apagado: registros y contenidos de la caché, contenidos de la memoria física, estado de las conexiones de red, tablas de rutas, procesos en ejecución, archivos temporales, información remota (logs, remote system), etc.

El análisis de relevancia y suficiencia de los datos considerados de interés se ha de sujetar al plan de investigación.

La confiabilidad de la prueba requiere controles específicos vinculados con el aseguramiento de la fuerza probatoria de las evidencias, en cuanto a su origen, autenticidad e integridad. Ello se debe a que los actos de adquisición de datos volátiles no son reproducibles y, además, pueden generar alguna alteración en la evidencia digital de un dispositivo.

Debe constatarse, asimismo, la validez o admisibilidad legal de las tareas a realizar y de los datos a obtener.

En lo que hace a gran parte de los aspectos generales de la labor (preparación, actuación en equipo, aseguramiento de la prueba, inspección de la escena y de los dispositivos, evidencias y personas vinculadas con los artefactos, documentación y registro de lo actuado), deberán observarse los criterios establecidos respecto de la fase de recolección, en cuanto sean compatibles con los recaudos específicos que se enuncian seguidamente.

Criterios especiales de actuación

- ✓ Aseguramiento:
  - Los datos volátiles requieren recaudos específicos para su aseguramiento, dada su especial fragilidad. Se ha de neutralizar o, cuanto menos, minimizar todo riesgo de eliminación o alteración que puede provenir de factores ambientales (especialmente electromagnéticos), de la acción de terceros (presencial o remota) y/o de las propias prácticas desplegadas durante el procedimiento.
  - La necesidad de aseguramiento persiste durante todo el proceso de obtención de los datos.
- ✓ Inspección:
  - Se deben llevar a cabo las medidas pertinentes de inspección pasiva (fotografiado y descripción de pantallas, conexiones y dispositivos de red, etc.).
  - Según las circunstancias del caso, se accederá a los menús, aplicaciones y archivos activos, para su descripción y captura fotográfica, consignando asimismo la fecha y hora que registra cada dispositivo, y la fecha y hora de la inspección. En todo momento se respetarán los principios de actuación referidos a la manipulación, alteración y/o destrucción de datos.
- ✓ Manipulación, alteración y/o destrucción de datos:
  - Debe procurarse la menor alteración y/o destrucción de datos informáticos.
  - En la medida de lo posible, toda alteración de los sistemas debe estar prevista de antemano. El EA debe asegurarse de contar con directivas o criterios claros respecto de cuáles son las pruebas de carácter prioritario.
  - Ante situaciones no previstas, se deberá consultar al director de la investigación (Art. 248 del CPP Prov. Bs. As.).
  - Debe precisarse en forma documentada en qué ha consistido la alteración, y cuáles son sus efectos sobre el material probatorio adquirido (datos volátiles) y/o sobre la evidencia contenida en medios de almacenamiento persistentes.
- ✓ Orden de levantamiento de datos:
  - El orden en que serán levantados los datos dependerá del previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información.
  - Debe tenerse en cuenta que probablemente existan otros datos importantes en sistemas dispositivos periféricos (router, modem, switch, hub, etc.).
  - Generalmente, será útil recuperar los siguientes datos del sistema en tiempo real: fecha y hora del sistema (contrastada con la hora oficial), procesos activos, conexiones de red, puertos TCP y UDP abiertos, usuarios conectados remota y localmente.
- ✓ Identificación de usuarios:
  - Cuando las circunstancias del caso lo tornaren conveniente, el EA sugerirá al responsable del procedi-

miento la identificación de las últimas personas que utilizaron el dispositivo y/o de quienes habitualmente tienen acceso al mismo.

- ✓ Acceso a datos:
  - Si especialistas de otra área están buscando evidencia material (huellas digitales, ADN, etc.) y el tipo de dispositivo lo admite, puede ponderarse el empleo de artefactos inalámbricos (mouse, teclado, etc.) para acceder a los datos. En caso de duda, se consultará al director de la investigación.
  - Cuando las circunstancias del caso lo aconsejen, se consultará al director de la investigación acerca de la alternativa de poner en estado de hibernación los sistemas de un dispositivo y efectuar su recolección.
  - Si se advirtiere que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal, etc., se efectuará consulta al responsable del procedimiento acerca de los límites legales que pudieren existir para la captura de la información.
- ✓ Registro, documentación y validación:
  - El proceso técnico de extracción de información debe documentarse conforme las disposiciones relativas a la fase de recolección, indicando especialmente las herramientas utilizadas y los resultados obtenidos.
  - Se adoptarán los principios de cadena de custodia al soporte de la información adquirida. Se sugiere obtener un hash para posterior validación, que será consignado en el acta pertinente, con mención de la fecha, hora, lugar, dispositivo de origen, y EA interviniente.
  - Deberá completarse el Acta de Levantamiento de Evidencia Digital (LED). Al respecto, ver fase de Cadena de Custodia.

CADENA DE CUSTODIA Y PRESERVACIÓN

Conceptos generales

La cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que ésta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria. Permite, además, hacer transparente todo eventual cambio o alteración del material probatorio. Asimismo, posibilita un mejor control de la debida reserva de aquella evidencia que pueda contener datos personales o sensibles, o correspondencia electrónica (art. 2° de la ley 25.326 de Protección de Datos Personales; arts. 18, 21, 50 y cctes de la Ley Nacional de Telecomunicaciones n° 19.798; arts. 153 a 157 bis del Código Penal). Deberán seguirse las orientaciones generales establecidas en la Res. 889/15 (“Protocolo de Cadena de Custodia”) en tanto no se opongan a las contenidas en la presente Guía.

La cadena de custodia comienza desde el momento de hallazgo o recepción de la evidencia y finaliza cuando la autoridad judicial competente decide sobre su destino. En este marco, la preservación es el resguardo o depósito seguro de la evidencia, durante los lapsos de tiempo en que ésta no es transportada ni utilizada.

La individualización y preservación de evidencia informático forense presenta particularidades y requerimientos específicos. Es necesario adoptar recaudos no sólo sobre dispositivos o artefactos, sino además sobre la evidencia digital. Esta última puede estar contenida en aquéllos o ser extraída de los mismos. En especial, la evidencia

digital es sensible a fenómenos electromagnéticos, y puede ser eliminada o alterada a distancia. Por otra parte, el depósito y preservación de la evidencia digital y de sus contenedores requiere contar con entornos adecuados (en cuanto a seguridad y reserva de los datos), suficiente capacidad de almacenamiento físico y virtual, y una precisa delimitación de roles. Estas cuestiones generales escapan al manejo de un caso concreto, y van más allá de los límites de esta guía. Sin embargo, no deben ser desatendidas por las autoridades del Ministerio Público Fiscal. Parte de esta problemática es analizada en el proyecto de investigación complementario vinculado con los laboratorios de informática forense (GT-LIF).

En la cadena de custodia participan todos los funcionarios y/o empleados que intervengan durante las diferentes etapas del proceso judicial sobre las evidencias.

Según la estrategia del Fiscal, podrá o no requerirse a uno o más funcionarios que hayan intervenido en la recolección, recepción y/o análisis de dispositivos y/o evidencia digital, que acrediten ante el tribunal el origen e integridad de dicha prueba (ver arts. 342 bis inc. 5° y 360 último párrafo del CPP; art. 55 de la ley 13.634).

El procedimiento de cadena de custodia no obstará a la adopción de otros recaudos complementarios que sean adecuados a cada caso (validación mediante algoritmos de hash, reconocimiento de evidencias por testigos, etc.).

Principios básicos de actuación

Las conductas a adoptar en el procedimiento de la cadena de custodia pueden ser clasificadas como:

1. *Tareas de aseguramiento y preservación.* Los especialistas informáticos deberán observar los recaudos de aseguramiento y preservación de evidencia en todo acto que lleven a cabo sobre evidencia informática y digital.
2. *Actos de control.* El personal técnico deberá constatar el estado en que se encuentra el material recibido, incluyendo sus embalajes, fajas de seguridad, rótulos e identificación. Asimismo, deberá cotejar la correspondencia entre los elementos recibidos y la documentación adjunta (ej.: planilla de cadena de custodia, IPP, remito).
3. *Documentación y registro.* Deberán documentarse las tareas de aseguramiento y preservación, como también el resultado de los actos de control. La documentación podrá ser complementada con registros fotográficos y/o fílmicos. En el caso de haberse observado alteraciones del rótulo, embalaje y/o evidencia, se informará al director de la investigación.

Para documentar los distintos eventos vinculados con una evidencia, se recomienda utilizar una Planilla de Cadena de Custodia. Se sugiere que las Actas de Levantamiento de Evidencia y la Planilla de Cadena de custodia tengan una versión digital, dotada del mayor grado de compatibilidad posible con los registros de “Efectos” y de “Remitos/Recibos” del Sistema Informático utilizado por el Ministerio Público.

Recaudos especiales

- ✓ Durante la fase de recolección, se cumplirán los recaudos de clasificación, identificación, embalaje y rotulado allí establecidos, tareas éstas que se encuentran a cargo del Especialista en Recolección.
- ✓ Al levantarse evidencia, se recomienda labrar el Acta de Levantamiento de Evidencia que sea pertinente al caso:
    - Acta de Levantamiento de Soporte de Evidencia Digital (LSED): Cuando se incautan o reciben de terceros elementos de hardware.

- Acta de Levantamiento de Evidencia Digital (LED): Respecto de la evidencia digital que se obtenga en un acto o procedimiento.

✓ En todo acto abarcado por la cadena de custodia se utilizará el identificador único de cada evidencia.

✓ Si se recibiera un efecto sin abrir el embalaje, se hará constar tal circunstancia.

✓ Quien abra o rompa un embalaje y/o rótulo, deberá hacerlo constar en acta, cumpliendo las exigencias de los arts. 117 a 120 del CPP.

✓ Cuando un especialista entregue un dispositivo o soporte de evidencia digital, deberá informar al receptor acerca de las condiciones de traslado, preservación, almacenamiento y seguridad que éste requiere, dejando constancia de manera clara y concisa.

ADQUISICIÓN DE MEDIOS DE ALMACENAMIENTO PERSISTENTES

Nociones y principios generales

Esta fase comprende toda actividad vinculada con la generación de una o más réplicas exactas del contenido digital alojado en un dispositivo de almacenamiento persistente (ej. discos rígidos, tarjetas de memoria extraíble, dispositivos USB, tarjetas SIM, entre otros). Su finalidad es la de asegurar la confiabilidad de la evidencia digital, ya sea que se la considere en sí misma o como insumo para la labor pericial o la prueba testimonial. Las réplicas o copias forenses permiten trabajar a los peritos sin alterar la evidencia original.

La realización de esta tarea es incumbencia del EA, con excepción de los casos en que integre la labor pericial (en tal supuesto intervendrá el EED designado).

Este proceso de trabajo puede ser llevado a cabo, según el caso concreto y las particularidades de los dispositivos, en distintas modalidades:

a) Como alternativa total o parcial a una labor de recolección (ej.: cuando en el marco de un allanamiento se decide obtener la imagen de algún dispositivo, sin secuestrarlo).

b) Como labor previa a la realización de una pericia de análisis informático.

c) Como parte de una pericia informática.

Previamente a definir la modalidad bajo la cual se va a efectivizar la adquisición de medios de almacenamiento persistentes, el EA deberá comunicar al director de la investigación sus apreciaciones, y sugerirle la alternativa que considere técnicamente más adecuada. La decisión última es responsabilidad del director de la investigación. El desarrollo de la labor se adecuará a los requerimientos propios de cada modalidad.

Se recomienda efectuar una imagen inicial, una copia de trabajo y una copia de resguardo; todas en medios de almacenamiento independientes, sugiriéndose que la copia de resguardo se almacene en un ámbito físico separado. Si hubiere peritos de parte y el director de la investigación lo autorizare, se hará una copia para cada uno de ellos, quienes deberán aportar el medio de almacenamiento para alojarla. El EA dejará debida constancia de la cantidad de copias y de sus destinatarios, para posibilitar la adopción de las decisiones pertinentes sobre el destino de la evidencia en el momento procesal oportuno.

Preparación y desarrollo de las tareas

✓ *Inspección y manipulación*:

- Si la labor se desarrolla en el contexto de un procedimiento, se adoptarán los recaudos establecidos para la fase de recolección.
- Si el dispositivo ya ha sido recolectado:
  - Previamente a su recepción, el EA o el EED revisará el envoltorio que lo contiene y/o las fajas de seguridad de la totalidad del dispositivo.
  - Se examinarán los elementos recibidos y las condiciones en que se encuentran, obteniéndose fotografías.
- Cuando se reciban o inspeccionen equipos, se realizará una inspección del hardware a fin de determinar la presencia de discos rígidos, memorias, discos RAID (Redundant Array of Independent Disks).
- Los dispositivos de almacenamiento serán identificados y, en su caso, extraídos de modo seguro.

✓ *Tareas de adquisición*. Se llevarán a cabo las siguientes tareas:

- Adopción de los recaudos necesarios para evitar toda clase de interferencias que puedan interrumpir el proceso y/o alterar la evidencia (acción de terceros, campos electromagnéticos, etc.).
  - Si estuviera presente alguna de las partes, letrados y/o peritos, se escucharán las medidas que propongan, sus preguntas, observaciones y eventual mención de irregularidades. En caso de duda sobre los alcances legales de tales manifestaciones, se consultará al director de la investigación (art. 279 del CPP).
- Bloqueo del medio de almacenamiento, a fin de evitar escrituras indeseadas.
- En Discos Rígidos: Búsqueda de Host Protected Areas (HPA).
- Captura y resguardo de la imagen: Adquisición de la imagen del medio de almacenamiento.
- Compresión y/o división de la imagen, cuando las circunstancias lo aconsejen.
- Validación del original y la imagen, a fin de garantizar que el contenido de ambos es idéntico.

✓ *Documentación*. Sin perjuicio de los recaudos generales mencionados en el proceso de recolección, se hará constar además, mediante acta de estilo:

- El lugar, fecha y hora de comienzo y de fin de las tareas, las personas presentes y su rol procesal (arts. 276, 278 y 279 del CPP).
  - Cuando se adquiriere la imagen de varios dispositivos, se recomienda asentar la fecha y hora de comienzo y final de cada proceso.
- La descripción y estado de los envoltorios y fajas de seguridad, los equipos y dispositivos inspeccionados. Se recomienda la obtención de fotografías.
- Los procedimientos y herramientas utilizadas, y su resultado.
- Las modificaciones producidas y sus justificativos o causas.
- Mención de la cantidad de imágenes y su destino.
- Resultado de la validación entre el contenido original y sus réplicas.
- Todo otro evento relevante.

✓ *Cadena de custodia*. Se aplicarán a las copias forenses las reglas de cadena de custodia y de preservación de la evidencia, en cuanto fueren pertinentes, y sin perjuicio de la adopción de otros recaudos o procedimientos de validación.

LABORES PERICIALES[5]

Marco procesal e institucional. Principios de actuación

Nociones generales

Los peritos intervienen en un proceso penal cuando es necesario contar con conocimientos especiales en alguna ciencia o arte para averiguar, comprobar y/o interpretar hechos pertinentes al caso (cf. art. 244 del CPP). Las tareas periciales se encomiendan a Especialistas en Evidencia Digital (EED). Las condiciones habilitantes para el ejercicio del rol pericial informático están reguladas en los arts. 2° y 7° inc. 13 de la ley 13.016 de Ejercicio de las Profesiones en Ciencias Informáticas.

En cuanto al tipo de labor encomendada, ésta puede consistir en examinar la evidencia y elaborar un informe, o bien en pronunciarse acerca del dictamen de otro perito (ver art. 249 del CPP).

Durante la investigación penal preparatoria, es generalmente el Fiscal quien dispone las pericias, designa los expertos que intervendrán, establece las cuestiones a dilucidar, y dirige la actuación pericial (arts. 247, 248 y 334 del CPP). En esta etapa, existen dos posibles modalidades de intervención:

a) Los dictámenes escritos que se incorporan en la carpeta formalizada (IPP). Esta forma es especialmente necesaria si las operaciones periciales no son reproducibles en juicio, o cuando se utilizará el dictamen para realizar peticiones ante el Juez de Garantías (ej.: pedido de allanamiento, solicitud de prisión preventiva, requerimiento de citación a juicio).
b) Los simples interrogatorios o consultas al perito, que pueden ser anotados en el legajo reservado del Fiscal (art. 75 de la Ley de Ministerio Público n° 14.442).

En la etapa de juicio, los peritos son interrogados por la parte que propuso su declaración, y contrainterrogados por las restantes, bajo la dirección del presidente del Tribunal (arts. 365, 360 y 342 bis del CPP). Según la estrategia del Fiscal, podrá o no requerírsele que acredite o contribuya a acreditar ante el tribunal el origen e integridad de la evidencia que hubiere analizado (ver arts. 342 bis inc. 5° y 360 último párrafo del CPP; art. 55 de la ley 13.634).

Posición procesal del perito

En el régimen acusatorio, como es el proceso penal provincial, los peritos son considerados de parte. El Fiscal los convoca en función de sus objetivos (la estrategia de abordaje del caso, el concreto plan de investigación delineado y, en la etapa de juicio, la teoría del caso que haya elaborado). Ello no exime a los peritos del Ministerio Público Fiscal de los deberes de actuar con solvencia técnica, objetividad y veracidad (ver arts. 56, 218 y 245 del CPP).

Deber de reserva

El perito deberá guardar reserva de todo cuanto conociere con motivo de su actuación (art. 253 del CPP). Este deber es particularmente relevante en virtud del acceso, según los casos, a grandes volúmenes de datos que pueden contener información sensible, y/o afectar derechos de terceros (cf. art. 2° y cctes. de la ley 25.326 de Protección de Datos Personales; arts. 18, 21, 50 y cctes. de la Ley Nacional de Telecomunicaciones n° 19.798; arts. 153 a 157 bis del Código Penal). En el marco del deber de reserva, el experto deberá disponer la custodia

[5] Para el abordaje conceptual ver "Aspectos legales y estratégicos del empleo de la Informática Forense en el Proceso Penal.

segura de dispositivos, imágenes de disco, etc., durante el tiempo que insuma la labor pericial.

Límites legales

El EED deberá analizar la evidencia dentro de los límites impuestos por la autorización judicial y/o los puntos periciales fijados. Si en el transcurso de su labor, descubriere en forma casual evidencia vinculada con la posible comisión de otro delito, deberá comunicarlo al Fiscal y/o formular la denuncia pertinente en forma separada (art. 287 del CPP).

Etapas

Generalmente, la labor del perito se despliega en diferentes etapas, de un modo acorde con las exigencias técnicas y legales: a) actos y formalidades iniciales; b) preparación del análisis; c) análisis; d) interpretación; e) elaboración del dictamen; f) presentación del perito en juicio oral; g) acciones vinculadas con el destino de las evidencias.

En todo momento se cumplirán los principios y recaudos de preservación, control y registro del procedimiento de cadena de custodia.

Actos y formalidades iniciales

Controles y consultas previas

Con anterioridad al inicio de la labor pericial, el experto:

- ✓ Participará, en caso de ser necesario, en la elaboración de los puntos periciales (tarea a cargo del Fiscal).
- ✓ Deberá informarse acerca del objeto de la investigación, y comprender los propósitos perseguidos a través de la labor pericial en el marco de la estrategia investigativa y/o probatoria. A estos fines, el perito podrá solicitar al director de la investigación que lo autorice a examinar las actuaciones y/o a asistir a los actos investigativos o procesales que estime pertinentes.
- ✓ Hará saber al director de la investigación si para realizar la tarea pericial considerare necesario contar previamente con determinadas pruebas o informes, como por ejemplo: reportes de proveedores de servicios de internet, obtención de contraseñas, elementos de validación del origen e integridad de dispositivos y/o evidencia digital remitidos por terceros (víctimas, proveedores de servicios de internet, empresas, autoridades judiciales de otra jurisdicción), etc.
- ✓ En caso de existir en el Ministerio Público Fiscal una autoridad encargada de fijar el nivel de prioridad de cada caso, solicitará precisiones al respecto. Asimismo, informará al director de la investigación el nivel de demora previsible para el inicio de la pericia, e indicará la duración estimada de la misma.
- ✓ Controlará los límites de la autorización legal y/o judicial para la realización de las tareas encomendadas. En caso de duda, consultará al director de la investigación.
- ✓ Se asegurará de contar con las herramientas técnicas y el equipamiento necesarios para realizar la labor encomendada.
- ✓ Verificará el cumplimiento de las notificaciones a las partes, previstas en el art. 247 del CPP. Tomará además conocimiento de las partes, letrados y peritos que estuviesen autorizados para intervenir en el examen pericial. En su caso, consultará al director de la investigación.
- ✓ Si hubiere peritos de parte y la duración estimada de las operaciones periciales u otras circunstancias imposi-

bilitaren o tornaren inconveniente practicar unidos el examen de la evidencia, el perito del Ministerio Público Fiscal lo hará saber al director de la investigación: en ese caso podrá proponer las alternativas que estime pertinentes (ej.: obtención de duplicados de las copias forenses para el trabajo de los expertos, reuniones periódicas de peritos, etc.).

- ✓ El área pericial no recibirá efectos previamente a la fecha de inicio de pericia, ni deberá conservar los elementos como depósito luego de su culminación.

Formalidades de inicio

La labor pericial se iniciará el día y hora fijados previamente, en la oficina del perito del Ministerio Público Fiscal o en el lugar que se hubiere establecido. Se constatará la presencia de las partes y peritos que hubiesen sido autorizados a intervenir. El comienzo de las tareas periciales se documentará mediante acta (art. 117 y siguientes del CPP prov. Bs. As.).

Previamente a cualquier tarea a realizar, se obtendrá fotografía de los elementos recibidos que serán objeto de examen.

Preparación del análisis

La preparación involucra todos los procedimientos necesarios para generar el entorno de pruebas preciso que permita llevar a cabo en primer lugar la inspección y, eventualmente, la recuperación de la información. Se recomienda la utilización de las técnicas y herramientas que se encuentran mencionadas en el Anexo III de este Protocolo. Esta fase involucra las siguientes tareas:

- ✓ Obtención de imágenes forenses, si no se hubieran obtenido previamente. A estos fines, deben observarse los recaudos establecidos para la fase de adquisición de medios de almacenamiento persistentes.
- ✓ Restauración y validación de la imagen forense. Es el conjunto de tareas a realizar para trabajar sobre la copia forense. La imagen forense puede ser restaurada montándola como unidad de disco, o haciéndola correr con una máquina virtual o bajo una suite de herramientas de análisis forense. Si correspondiere, habrá de realizarse previamente el ensamblado y descompresión de las divisiones de la imagen. Además de la restauración propiamente dicha, se debe controlar la confiabilidad de la evidencia recibida. Según los casos, se llevará a cabo una o más de estas tareas:
  - Validación de la correspondencia entre original y copia forense.
  - Control de la cadena de custodia.
  - Cuando se vaya a examinar evidencia remitida por terceros (víctimas, empresas, autoridades de otras jurisdicciones, proveedores de servicios de internet, etc.), se formularán las observaciones que se estime pertinentes acerca la acreditación del origen, grado de autenticidad e integridad de la evidencia.
  - Si, a juicio del EED, la evidencia recibida careciere de un mínimo de confiabilidad, lo hará saber al director de la investigación antes de iniciar las tareas de análisis.
- ✓ Examen general de la imagen forense:
  - Identificar cantidad y tipo de Sistemas Operativos presentes.
  - Revisar cantidad de discos, particiones y Sistemas de Archivos.
  - Buscar e Identificar Máquinas Virtuales presentes.
  - Opcional: Recomposición de Volumen RAID (si los hubiera).

- Opcional: Identificar y quebrar medios de encriptación (si los hubiera).

✓ Preparación del Entorno de Trabajo (considerando los puntos de pericia y las identificaciones efectuadas en el paso anterior):

- Preparación del Ambiente de Examen: del equipo del Laboratorio Forense que se utilizará para realizar el trabajo pericial.
- Preparación de Extracción Lógica: selección del conjunto de técnicas y herramientas.
- Preparación de Extracción Física: selección del conjunto de técnicas y herramientas.

Análisis

En esta etapa se analiza el contenido adquirido en busca de vestigios de lo que se pretende hallar.

El Análisis Forense comprende las siguientes labores:

✓ *Extracción Lógica*. Se efectúa empleando el sistema operativo del equipo como intermediario para el acceso a los datos (las herramientas de extracción se comunican con el sistema operativo del equipo y es éste quien aporta los datos existentes en el sistema). La extracción lógica comprende las siguientes acciones:

- Recuperación de archivos eliminados.
- Extracción de Información a examinar por tipo de archivo.
- Extracción de metadatos del archivo en el Sistema de Archivos.
- Extracción de metadatos propios del archivo.
- Extracción de archivos protegidos con contraseña.
- Extracción de archivos comprimidos.
- Detección y extracción de archivos encriptadas.
- Búsqueda de Información de Configuración.
- Búsqueda de Información de Procesos en Memoria.

✓ *Extracción Física*. Implica la búsqueda a bajo nivel, directamente sobre los datos presentes crudos en el disco, sin contar con el sistema operativo como intermediario. Este método de extracción permite la adquisición de los datos tal como se presentan en el medio de almacenamiento persistente, posibilitando el hallazgo de archivos ocultos y eliminados parcial o totalmente y que el sistema operativo no haya podido detectar. Esta labor implica una fuerte carga de trabajo con gran cantidad de información. Se recomienda su uso sólo si no se ha podido resolver los puntos periciales con técnicas de extracción lógica. Comprende estas acciones:

- Búsqueda de información en disco.
- Búsqueda de información en el área de paginado.
- Extracción de archivos en espacio no asignado - File Carving.

Interpretación

Si se recuperara o hallara información potencialmente relevante, el perito realizará una tarea de interpretación de la evidencia, en el marco de su incumbencia y en los términos de los puntos de pericia que le hubieren sido encomendados.

Previamente a ello, podrá ser necesario realizar un proceso de triage para centrar la labor en la evidencia relevante, o algún muestreo para agilizar la detección de ésta. Si, pese a no haberle sido ordenado, el perito advirtiere que la interpretación insumirá una demora importante o que existen datos sensibles pertenecientes a terceros, lo hará saber al Fiscal, solicitando en su caso se le informen los criterios selección de evidencia.

De acuerdo con los puntos periciales, podrán llevarse a cabo, entre otras, las siguientes tareas, dentro de los límites de incumbencia del perito informático:

- ✓ Describir los dispositivos de hardware y sus funcionalidades.
- ✓ Identificar software instalado y describir sus funcionalidades: analizar y comparar código fuente, programas y aplicaciones utilizados (en escritorio, dispositivos móviles y/o en la nube).
- ✓ Analizar los sitios web visitados y/o servicios en línea utilizados.
- ✓ Clasificar, individualizar, comparar y sistematizar la evidencia, según los criterios suministrados en los puntos de pericia. Por ejemplo, la evidencia puede ser clasificada según el contenido, función, características, etc.; asimismo, pueden cotejarse distintas versiones y/o fechas de un documento o imagen, etc.
- ✓ Búsqueda de documentos o imágenes con características especificadas en los puntos periciales.
- ✓ Reconstruir líneas de tiempo:
    - Creación, envío, recepción, acceso, reproducción, borrado y/o modificación de archivos, documentos, e-mails y otros medios de comunicación, etc.
    - Entradas y salidas de usuarios sobre uno o más sistemas informáticos.
    - Accesos a páginas o sitios web.
    - Transacciones electrónicas.
- ✓ Reconstruir rutas o caminos seguidos por la información

Existe un segundo nivel de tareas de interpretación de la evidencia digital, que no siempre está totalmente abarcado por las incumbencias del perito informático. Sin embargo, el aporte del experto puede contribuir a extraer significados de la evidencia y/o vincular a ésta con otras pruebas. Algunos de los casos de esta clase de labores son los siguientes:

- ✓ Detección de patrones o rutinas de usuarios sospechosos o víctimas.
- ✓ Búsqueda de palabras clave, léxicos, cadenas regulares, etc.
- ✓ Elaboración de hipótesis sobre un hecho.
- ✓ Identificación de modus operandi delictivos.
- ✓ Individualización personal de usuarios sospechosos.
- ✓ Búsqueda de posibles partícipes, cómplices y/o encubridores.
- ✓ Detección de patrones (usuarios, claves, textos, léxicos, cadenas regulares, rutinas de usuarios, etc.).

En este nivel de la interpretación, el EED deberá conocer el objeto de la investigación y los propósitos perseguidos mediante su labor pericial en el marco de la estrategia investigativa y/o probatoria del Fiscal. Podrá además solicitar el examen de las actuaciones y/o la asistencia a los actos investigativos o procesales que estime pertinentes. Si le fuera encomendado, actuará en forma interdisciplinaria con expertos de otras áreas. Según el caso, deberá explicar al director de la investigación o al Fiscal los alcances y limitaciones de su labor, proponer hipótesis y sugerir otras diligencias o pericias que considerare útiles para precisar o corroborar su dictamen.

Elaboración del dictamen pericial

En general, un dictamen de calidad debe demostrar que las labores periciales se basaron sobre evidencia o datos suficientes y confiables que las operaciones practicadas fueron realizadas utilizando herramientas y métodos fiables; que estos últimos fueron aplicados correctamente, y que las conclusiones se sustentan en el resultado de tales acciones.

Contenido

El dictamen pericial podrá expedirse por informe escrito o hacerse constar en acta y comprenderá:

1. El objeto de la pericia.
2. La descripción de los elementos recibidos y de las condiciones en que se encuentran. Según el caso y el objeto de la pericia, corresponderá brindar un mayor o menor nivel de detalle sobre los elementos obrantes en el interior de los equipos. También se hará una reseña de los documentos, informes y otras pruebas que se hubieren tenido en cuenta en el examen.
3. El detalle de todas herramientas y técnicas utilizadas y de las operaciones practicadas (ya sea en forma general o relativa a cada punto pericial), justificando las opciones escogidas e indicando lugar y fecha de las tareas.
4. La mención de toda circunstancia que pudiera haber incidido en la correcta ejecución de los procedimientos y en el empleo de las herramientas.
5. Los resultados y/o hallazgos obtenidos y las conclusiones a las que hubiere arribado el experto respecto de los puntos de pericia, con fundamento en los principios de la ciencia informática forense. En su caso, indicará:
    - El margen de error de los resultados y/o conclusiones.
    - Las cuestiones que no pudiere responder desde el ámbito de su incumbencia.
    - La necesidad de contar con más elementos (evidencias, documentación, informes o pericias adicionales) para arribar a conclusiones definitivas.
6. Todo otro dato u observación que el perito estime pertinente.

El EED dejará constancia de las condiciones en que se preservará la copia forense, el espacio que ocupa en el servidor de alojamiento, y de la necesidad de disponer sobre su destino final en el momento procesal que corresponda. En caso de haber recibido evidencia original, la devolverá a la Fiscalía, observando las reglas de cadena de custodia.

Forma y redacción

La redacción del informe deberá ser clara y comprensible para personas no expertas en la materia. De acuerdo con las características del caso, podrán acompañarse imágenes y gráficos para facilitar la comprensión. Es asimismo recomendable incorporar en anexos toda aquella información que por su volumen, formato o lenguaje, dificulte la lectura (listados, código de programación, etc.), pudiéndose, en su caso, resaltar las partes consideradas más relevantes.

Sin perjuicio de presentarse la versión impresa del dictamen, se procurará incorporar una versión digital en el Sistema Informático del Ministerio Público.

Cuando los anexos fueran excesivamente voluminosos, se consultará al director de la investigación acerca de la posibilidad de presentarlos solamente en formato digital (CD, DVD), asegurando su autenticidad.

Presentación del Perito en el Juicio Oral

Preparación

El perito que sea citado a declarar en un juicio oral y público deberá estar preparado para acreditar su capacitación y experiencia en el área, la objetividad de su actuación y el cumplimiento de la ley durante su desempeño en el caso.

Es previsible que se interrogue al perito principalmente sobre los puntos o aspectos de su labor pericial que sean objeto de controversia entre las partes. Igualmente, el experto debe estar en condiciones de exponer acerca de todas las cuestiones vinculadas con su tarea pericial en el caso.

El perito solicitará mantener una reunión previa con el Fiscal para interiorizarse del caso, establecer los alcances y límites de su declaración, conocer los lineamientos del interrogatorio y las posibles estrategias de las otras partes.

En particular, el EED deberá saber si el Fiscal le encomendará la presentación y/o validación de evidencia (dispositivos y/o evidencia digital). En tal caso, deberá estar especialmente preparado para exponer acerca de la fiabilidad de los procedimientos y registros de cadena de custodia, y de todo otro procedimiento de validación de la evidencia.

Asimismo, tomará contacto con las pruebas que estuvieren vinculadas con el área informático forense (informes de ISPs, reportes técnicos, etc.), y con los dictámenes que hubieren elaborado los peritos de parte.

Forma de la declaración

El interrogatorio será guiado primeramente por el Fiscal, luego por las partes restantes, y eventualmente por los jueces, es decir que el perito no fijará por sí mismo el orden de su exposición. Los interrogatorios podrán ser organizados de distintas formas: según un orden temático, reproduciendo la secuencia de las labores periciales ya realizadas, yendo de lo general a lo particular, avanzando desde las conclusiones hasta sus fundamentos técnicos y metodológicos, centrándose en las cuestiones más relevantes, haciendo foco en las debilidades reales o presuntas de la evidencia y/o de la labor pericial, etc. El experto deberá estar en condiciones de adaptarse a la modalidad de los interrogatorios.

La objetividad y claridad expositiva del perito son tan importantes como su solvencia técnico-científica:

- ✓ El experto no se expedirá acerca de cuestiones ajenas a su incumbencia profesional.
- ✓ Responderá con veracidad a las preguntas que se le formulen, sin perjuicio de poder pedir aclaraciones cuando estime que una pregunta es capciosa, confusa o no pertinente a su especialidad (art. 101 del CPP).
- ✓ Aportará su saber de un modo comprensible y didáctico ante las partes y los jueces, quienes no conocen en profundidad la disciplina informática. Durante su declaración, podrá consultar su dictamen escrito. Es recomendable el empleo de recursos gráficos y/o tecnológicos para facilitar la comprensión de los jueces (presentaciones o archivos multimedia, máquinas virtuales, etc.).

Cuando hubiere peritos de parte, la recepción de la declaración de los expertos podrá ser efectuada en forma conjunta o sucesiva. En ambos escenarios, el perito deberá estar en condiciones de justificar objetivamente por qué sus conclusiones deben prevalecer frente a las de los otros especialistas. Para ello, tendrá eventualmente que afianzar la relevancia, suficiencia, confiabilidad y validez legal de la evidencia analizada; la fiabilidad de los métodos y herramientas de análisis empleados; la correcta aplicación de dichos métodos y herramientas; y la solidez lógica y científica de los razonamientos que dan sustento a sus conclusiones.

En determinados casos, el EED podrá ser convocado a declarar conjuntamente con peritos de otras especialidades. En tales supuestos, deberá estar preparado para contribuir a una visión interdisciplinaria respecto de las cuestiones que sean objeto del interrogatorio.

Destino de las evidencias y copias forenses

Mediante este proceso se procura dar respuestas ágiles y seguras frente a cuestiones críticas vinculadas con soportes informáticos y evidencia digital (datos sensibles vinculados con terceros, contenidos ilícitos, información vinculada con otros posibles delitos, dispositivos pasibles de decomiso, equipos necesarios para dar continuidad a actividades lícitas, saturación de espacio de almacenamiento en laboratorios informáticos, etc.).

Dispositivos y evidencia material

Una vez finalizada la pericia, el EED remitirá el dictamen y el material recibido a la Fiscalía u organismo de origen, indicando expresamente cuáles son los dispositivos y efectos que a su juicio carecen de interés pericial.

Evidencia digital

Cuando el examen pericial no arrojare hallazgos relevantes, el EED solicitará al Fiscal que decida acerca del destino de las copias forenses.

Si se encontrare evidencia útil para la investigación (sea de cargo o de descargo), se preservará la imagen, pudiéndosela comprimir mediante un método fiable y debidamente documentado que permita garantizar la confiabilidad de la prueba. Sin perjuicio de ello, cuando se presente alguna de las siguientes circunstancias consultará al director de la investigación, a fin de que se adopten los recaudos pertinentes:

- ✓ Cuando se hallare información sensible o confidencial perteneciente a terceros.
- ✓ En los casos en que la pericia se hubiere basado en los datos obtenidos tras un procedimiento de triage, filtrado o muestreo, o cuando la evidencia irrelevante fuere muy voluminosa.

Informes y consultas

Con frecuencia semestral, el Laboratorio de Informática Forense controlará en el Sistema Informático del Ministerio Público (SIMP) el estado procesal de las causas vinculadas con efectos recibidos y/o imágenes almacenadas en sus ordenadores. En los casos en que se hubiera adoptado una decisión definitiva o provisoria (sobreseimiento, condena, absolución, archivo, desestimación) o se hubiera declarado la incompetencia, remitirá una nota al Fiscal, solicitando directivas acerca de los efectos y los datos almacenados (Arts. 231, 522/525 del CPP).

Con frecuencia anual, el Laboratorio de Informática Forense remitirá al Secretario de la Fiscalía General un listado de las imágenes de disco que estén almacenadas, en el cual constará: número de proceso, Fiscalía interviniente, cantidad de espacio de almacenamiento ocupado, y fecha de finalización de la pericia (cf. art. 71 inc. 8° de la Ley 14.442 de Ministerio Público). También se elevará informe cuando se produzca, o sea inminente, la saturación de los medios de almacenamiento del Laboratorio y ello obstaculice el inicio de nuevas pericias.

Ejecución y documentación de medidas

En todos los casos en que el Fiscal o el Juez dispongan la eliminación total o parcial de copias forenses, la ejecución de la medida deberá documentarse mediante acta, conforme lo establecido en los arts. 117/120 del CPP.

IV. ANEXO I

EVIDENCIAS EN MEDIOS TECNOLÓGICOS

Se presenta en este documento un listado ejemplificativo de las evidencias pasibles de ser encontradas en diversos medios tecnológicos que almacenan información, así como su importancia para en el análisis forense. Se describen a continuación elementos que pueden encontrarse en Disco Rígido, Memoria, Red y otros dispositivos electrónicos.

A. Disco Rígido

En una copia forense de un disco rígido de un equipo, pueden encontrarse los siguientes elementos:

- ✓ Archivos:
  - De usuarios.
  - De sistema.
  - Ocultos.
  - Eliminados, recuperables con extracción lógica.
  - Eliminados, recuperables con extracción física.
- ✓ Fragmentos de memoria presentes en memoria virtual.
- ✓ Fragmentos de artefactos, de memoria o de red, almacenados temporalmente.

En general, puede considerarse que cualquier información almacenada en un disco es un archivo.

Además de los archivos, en el disco es posible encontrar metadatos de archivo, que permiten establecer fechas de acceso, creación, modificación, etc. Además, hay otra información de uso del equipo, los archivos y la actividad del usuario, presente en archivos de configuración, registros de sistema y aplicación (logs), registros de configuración (Registro de Windows, bases de datos de aplicación) y servicios del sistema operativo.

La descripción de los artefactos que pueden encontrarse en disco es vaga, porque puede haber miles de archivos de distintos tipos. La información que se puede recuperar depende de los archivos que se buscan y del interés para la investigación.

En el disco pueden encontrarse archivos que indiquen la existencia de programas, malware, virus, fotografías en distintos formatos de archivo (JPG, PNG, GIF, BMP, TIF), archivos de suite de oficina, de base de datos, entre otros.

Por otro lado, los archivos de sistema presentes en el disco brindan información sobre el uso de la computadora, archivos accedidos y acciones realizadas en el equipo por un usuario.

B. Memoria

En una imagen de memoria pueden encontrarse los siguientes elementos:

- ✓ Listado de procesos.
  - Con el término “procesos” se alude a programas en ejecución en un sistema. Además del código en sí, un proceso mantiene un estado y datos en memoria.
  - Los procesos pueden estar en tres estados: activos, terminados y ocultos.

- Es importante para detectar casos de malware, botnets, virus, etc. Además de permitir conocer qué estaba ejecutándose en el equipo al momento de adquirir una imagen de la memoria activa de un proceso.

✓ Archivos abiertos por un proceso.

✓ Conexiones de red abiertas por un proceso.

✓ Credenciales de acceso a servicios (pares usuario/contraseña o credenciales más complejas).

✓ Claves en memoria.

- Claves de encriptación (TrueCrypt, BitLocker o de otro tipo), claves de servicios manejadas por programas, etc.

✓ Archivos cargados en memoria por procesos.

✓ Listado de usuarios conectados al equipo, local o remotamente.

✓ Listado de dispositivos conectados al equipo.

✓ Listado de redes a las que tiene acceso el equipo.

✓ Librerías, DLLs y drivers cargados en el sistema.

El volcado de memoria es importante porque se vincula con la información presente en la computadora en un momento determinado y que se hace explícita durante el uso del equipo. El análisis de la memoria puede ayudar a inferir el uso que se le da al equipo, o detectar indicios que soporten una hipótesis particular.

Un ejemplo clásico de necesidad de realizar la adquisición de la memoria de un equipo encendido al momento de un allanamiento, es para descartar la presencia de un *malware*, el cual puede ocasionar que cierta acción parezca realizada por un usuario de un equipo, cuando en realidad es realizada por otro mediante el uso indebido de su equipo a distancia. Si bien un malware puede detectarse mediante el hallazgo en el disco rígido del equipo de los archivos que lo componen, es mucho más fácil identificarlo a través del proceso y las conexiones que establece.

Por otro lado, las claves cargadas en memoria dependen directamente de la actividad del usuario, y es muy probable que no se encuentren en las copias forenses del disco del equipo analizado.

C. Dispositivos de Almacenamiento extraíbles

Los dispositivos de almacenamiento extraíbles (CD, DVD, pen drive, disco externo, etc.) pueden considerarse como fuentes de evidencia tan valiosas como un disco principal, y por lo tanto tienen la misma importancia.

Debe destacarse que, por las características técnicas de los puertos USB, cualquier dispositivo USB debería evaluarse para determinar si tiene capacidad de almacenamiento de datos. Por ejemplo, hay formas técnicas de incorporar dentro de un mouse USB la electrónica de un pen drive, y tener así un dispositivo de almacenamiento oculto para los investigadores.

D. Volcado de Red

El volcado de red contempla la actividad y comunicación que realiza el equipo a través de una red, ya sea local, de área o internet.

El volcado de red es análogo a una escucha telefónica, sujeto a la información que se transmite a través de una red. Es necesario realizarlo con anterioridad a un allanamiento para poder recuperar una cantidad de datos sufi-

ciente que permita el análisis forense posterior.

De un volcado de red se puede recuperar la siguiente información:

- ✓ Actividad del equipo en la red local:
  - Archivos compartidos.
  - Archivos accedidos en otro equipo.
  - Impresión de documentos.
- ✓ Actividad del equipo en Internet:
  - Archivos compartidos.
  - URLs y sitios accedidos.
  - DNSs utilizados.
  - Paquetes con datos.
  - Paquetes de aplicación.
  - Utilización de VPNs.
  - Accesos remotos a equipos.

El volcado de red permite conocer en profundidad todas las comunicaciones que establece el equipo con otros. La información que pasa a través de la red puede ser de mayor o menor importancia, y podría no estar presente la comunicación de interés. Estas circunstancias ocasionan que el volcado de red pueda resultar difícil de trabajar. Sin embargo, poder ubicar la transferencia de un archivo de interés en el volcado de red es de suma importancia, ya que además de los contenidos mismos del archivo nos proporciona información de fecha, hora e IP de destino/origen.

E. Sinergia entre los componentes

Finalmente, se debe mencionar que el volcado de memoria, la imagen de disco y el volcado de red, son en realidad tres aspectos distintos del equipo informático y su actividad, siendo complementarios entre sí.

Se plantea a continuación un ejemplo de caso en el que se verifica la necesidad de complementar el estudio con los tres componentes arriba mencionados.

Caso Ejemplo:

En el disco de una computadora secuestrada se hallan fotografías de pornografía infantil. Como se sospecha del equipo en cuestión, también hay disponible un volcado de red que tiene la actividad de los últimos tres días.

De cada una de las imágenes (copias forenses), se puede extraer la siguiente información:

- ✓ Disco: La presencia de archivos JPG que contienen pornografía infantil. Eventualmente podría haber metadatos del sistema operativo que brinden fecha y hora de creación, modificación y acceso, o metadatos EXIF con información adicional.
- ✓ Memoria: En la imagen de memoria puede detectarse con herramientas forenses (ej.: Volatility) la presencia de un proceso oculto que es cliente de una botnet y permite controlar la computadora remotamente para distribuir archivos por internet.
- ✓ Red: En el volcado de red pueden encontrarse paquetes TCP/IP desde y hacia distintas direcciones IP que transmiten algunos de los archivos JPG encontrados en el disco. De ésta forma, puede establecerse una parte

del camino de distribución de los mismos, y otras direcciones IP implicadas.

Es evidente que cada uno de estos componentes en forma aislada presenta información incompleta. Si se analiza únicamente el disco o el volcado de red, pueden aparecer indicios inculpando a una persona inocente por posesión o distribución de pornografía infantil. Analizando únicamente memoria y disco, se podría detectar la existencia de un botnet operando sobre la computadora, pero costaría identificar las IPs involucradas. Del análisis parcial, trabajar con el volcado de memoria y el volcado de red sería lo más provechoso, ya que podríamos identificar la botnet en memoria y las comunicaciones, pero solamente podríamos detectar los archivos que se transmitieron en el período que se realizó el volcado de red.

Trabajando con las tres imágenes, se pueden identificar todas aquellas que resulten ilícitas, reconocer que se trata de un caso de una botnet de distribución y generar un listado de IPs involucradas. El análisis individual de cada una de éstas podría resultar parcial e incompleto, y no servir como prueba fehaciente de la participación de un usuario determinado. Por lo tanto, se recomienda trabajar con las tres imágenes (de disco, de memoria y de red), siempre que sea posible, a fin de realizar un análisis forense completo.

F. Otros dispositivos

Así como los dispositivos de almacenamiento externo pueden considerarse como casos particulares de los discos de almacenamiento principal de una computadora, existen en la actualidad una gran cantidad de dispositivos que se pueden considerar como casos particulares de computadoras. Por ejemplo, los teléfonos inalámbricos, celulares, Smartphones, cámaras digitales, Tablets, GPS, beepers, faxes, cámaras de seguridad y DVRs, entre otros dispositivos. Todos estos casos son, en realidad, pequeñas computadoras, limitadas en su utilidad para cumplir una función específica.

Al igual que de un equipo de computación clásico, de estos aparatos es posible extraer información relacionada con sus funciones, por ejemplo:

- ✓ Listados de llamadas.
- ✓ Mensajes recibidos y enviados.
- ✓ Páginas de internet visitadas.
- ✓ Datos de localización geográfica.
- ✓ Aplicaciones instaladas.
- ✓ Redes WI-FI detectadas.

Además, debe considerarse que los dispositivos de almacenamiento propios del equipo usualmente presentan una interfaz coherente y estándar similar a las de otros sistemas informáticos; por ejemplo un sistema de archivos, en donde el usuario podría esconder información, cámaras de fotos con memoria interna que se pueden utilizar como pen drive, entre otros. Asimismo, una misma información puede hallarse en (o ser accesible desde) diversos dispositivos de un mismo usuario.

G. Particularidades de la investigación en la nube

Respecto de la búsqueda y obtención de evidencia en la nube, no existen en la actualidad procedimientos ni herramientas que gocen de una aceptación generalizada.

La complejidad de este entorno ofrece desafíos en los ámbitos técnico, legal e institucional. No obstante, puede ser útil formular algunas recomendaciones generales.

Para identificar y obtener evidencia relevante, suficiente, confiable y válida, es indispensable contar con diversa información:

- ✓ Particularidades del ámbito investigado, tales como:
  - Tipo de nube implicado (privada, comunitaria, pública, híbrida).
  - Modelo de servicios utilizado (IaaS, SaaS, Paas), con los consecuentes niveles de control de datos asignados al ISP y al usuario.
  - Arquitectura y topología física y lógica de la nube.
  - Posibles lugares de almacenamiento de la evidencia.
  - Tecnologías utilizadas por los ISP (herramientas de auditoría, formatos de metadatos, cifrados, etc.).
- ✓ Datos de índole legal e institucional:
  - Contratos con usuarios y políticas de privacidad de los ISP.
  - Relaciones entre ISP (subcontrataciones de servicios).
  - Nivel de capacitación del personal técnico de los ISPs, y fiabilidad de sus herramientas y procesos de obtención de evidencia.
  - Ubicación de la sede social de los ISP.
  - Ubicación geográfica de los datos (cuestión relevante no sólo para su identificación y obtención, sino también para el trazado de líneas de tiempo).

Es recomendable que el Ministerio Público Fiscal cuente con un nexo centralizado, que esté adecuadamente capacitado para obtener y actualizar toda esta información.

Los datos precedentes son sumamente útiles para planificar las medidas investigativas. Especialmente, posibilitan:

- ✓ Identificar el lugar donde se encuentra la información.
- ✓ Conocer y respetar el régimen jurídico aplicable.
- ✓ Definir a través quiénes se accederá a la información (requerimientos a usuarios y/o ISP, y/o acciones directas de la Fiscalía).
- ✓ Ponderar los tiempos de demora previsibles y sus posibles consecuencias, las dificultades técnicas a sortear, y el nivel de fiabilidad de la evidencia.
- ✓ Escoger el tipo de herramientas informáticas a emplear.

El especialista asesorará al director de la investigación acerca de la conveniencia y posibilidad técnica de adoptar distintas medidas de obtención de datos:

- ✓ Solicitudes de retención de datos de tráfico y/o contenidos.
- ✓ Intervención de comunicaciones y modalidad de ejecución de la misma (desde el Laboratorio de Informática Forense, desde entes estatales autorizados, desde los dispositivos de un usuario, mediante orden a un ISP).
- ✓ Empleo de herramientas de intrusión (sniffers, honeypots, etc.).
- ✓ Obtener contraseñas de acceso y/o descifrar datos encriptados.

Cabe destacar que la información relevante no siempre será evidencia digital, pudiendo procurarse también la obtención de prueba documental y de informes. A su vez, la comprobación del origen y/o autenticidad de determinada evidencia digital podrá ser efectuada o corroborada por medios ajenos a la informática forense (ej.:

partícipes en un intercambio de mails, reconocimientos de voz, etc.).

Previamente a acceder a datos almacenados en otras jurisdicciones, el especialista constatará que se dé alguna de estas tres circunstancias:

- ✓ Carácter público de los datos.
- ✓ Permiso del usuario o persona con derecho de acceso a los datos.
- ✓ Autorización legal o judicial.

En caso de duda, el especialista consultará al director de la investigación.

H. Herramientas de *Triage*

Triage es un procedimiento que se toma prestado de la medicina, mediante el cual se evalúa rápidamente el estado de varios pacientes para establecer la prioridad y orden en que deben ser atendidos. En el ámbito de la informática forense, el *triage* es un análisis rápido que se realiza sobre un equipo para determinar si contiene evidencia o indicios que puedan ser de utilidad para una investigación. De esta forma se puede examinar rápidamente un conjunto de equipos y determinar su importancia para la investigación en curso.

El valor del *triage* reside en identificar rápidamente sobre cuáles dispositivos comenzar a trabajar cuando se cuenta con múltiples equipos para analizar. De esta manera es posible optimizar el uso de recursos (tanto físicos como humanos), y operar con celeridad. Puede utilizarse durante la ejecución de procedimientos tales como una orden de allanamiento, para determinar qué equipos deben recolectarse y cuáles carecen de importancia. La búsqueda de evidencia en la nube es otra labor que puede exigir el empleo de estas técnicas. El *triage* es también aplicable para la realización de pericias informáticas sobre grandes volúmenes de datos.

El empleo de esta herramienta depende de variables tales como las características y trascendencia del hecho investigado, la mayor o menor urgencia para obtener evidencia, el grado de relevancia de la evidencia buscada, el riesgo de alteración o pérdida de datos, los criterios de asignación de recursos investigativos, etc.

Si bien el concepto está entendido y explicado en la bibliografía forense más moderna (Roussev et al.), es aún un desafío desarrollar herramientas de software libre disponibles que permitan realizar *triage* en forma fiable. Los paquetes de software de informática forense (Encase, FTK, etc.) cuentan con módulos para *triage*.

V. ANEXO II

A. ACTA DE LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL

ACTA DE LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL Nº: _____/20____

DATOS DE LA CAUSA

FECHA		HORA DE INICIO		HORA DE FINALIZACION	
CARATULA					
VICTIMA					
IMPUTADO					
AUTORIDAD JUDICIAL COMPETENTE					
DEPARTAMENTO JUDICIAL					
DEPENDENCIA		DEPENDENCIA SOLICITANTE			

Seguidamente y preguntado al/los testigo/s si posee/n algún tipo de interés en la presente y si tiene algún tipo de relación con las partes de las presentes actuaciones (art.235 CPP) manifiesta/n que ____ por lo que impuesto de las penas con la que la ley castiga el falso testimonio (art.275 CP) presta juramento en expedirse con veracidad en todo cuanto supiere y le fuere preguntado (art. 100 CPP) como así lo que viere en este acto.-

TESTIGO 1

APELLIDO Y NOMBRES									
DOMICILIO									
NACIONALIDAD		EDAD		LEE Y ESCRIBE	SI		NO		
DOCUMENTO DNI / CI.PFA / L.E. / L.C Nº				EXHIBE		RECUERDA			

TESTIGO 2

APELLIDO Y NOMBRES									
DOMICILIO									
NACIONALIDAD		EDAD		LEE Y ESCRIBE	SI		NO		
DOCUMENTO DNI / CI.PFA / L.E. / L.C Nº				EXHIBE		RECUERDA			

ESPECIALISTA EN RECOLECCION

INFORMATICO		TELEFONIA		OTROS	
APELLIDO Y NOMBRE					
OBSERVACIONES					

LUGAR DE LEVANTAMIENTO

DOMICILIO CALLE						ENTRE					
NRO		PISO		DEP.		LOCALIDAD					
COMERCIO		DEPOSITO		OFICINA		CASA		DEPARTAMENTO		PRECARIA	
OBSERVACIONES											

LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL

DISPOSITIVOS

CPU		LAPTOP		MARCA		MODELO		GENERICA			
Nº DE SERIE						ENCENDIDA		APAGADA			
DISPOSITIVOS CONECTADOS	COPIA RAM	SI		NO		FOTO PANTALLA	SI		NO		Nº
	PEN DRIVE			MAQUINA FOTOS			TELEFONO				
	TARJETA MEMORIA			BD/DVD/CD			HDD EXTERNO				
	OTRO										
	OBSERVACIONES										

LEVANLEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL																			
	CPU		LAPTOP		MARCA				MODELO				GENERICA						
	Nº DE SERIE								ENCENDIDA				APAGADA						
	DISPOSITIVOS CONECTADOS		COPIA RAM	SI		NO		FOTO PANTALLA	SI		NO		Nº						
			PEN DRIVE					MAQUINA FOTOS					TELEFONO						
			TARJETA MEMORIA					BD/DVD/CD					HDD EXTERNO						
			OTRO																
			OBSERVACIONES																

LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL																			
	CPU		LAPTOP		MARCA				MODELO				GENERICA						
	Nº DE SERIE								ENCENDIDA				APAGADA						
	DISPOSITIVOS CONECTADOS		COPIA RAM	SI		NO		FOTO PANTALLA	SI		NO		Nº						
			PEN DRIVE					MAQUINA FOTOS					TELEFONO						
			TARJETA MEMORIA					BD/DVD/CD					HDD EXTERNO						
			OTRO																
			OBSERVACIONES																

LED																			
	TABLET		MARCA				MODELO				NUMERO DE SERIE								
	TARJETA DE MEMORIA				TARJETA SIM				OBSERVACIONES										

LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL																			
	TELEFONO		MARCA				MODELO												
	Nº IMEI						TARJETA SIM				TARJETA DE MEMORIA								
	SISTEMA OPERTATIVO		ANDROID		IOS		WINDOWS PHONE				SYMBIAN		OTRO						
	EMAIL ASOCIADO										ACCESO		SI		NO				
	ACCESORIOS																		
	OBSERVACIONES																		

LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL																			
	TELEFONO		MARCA				MODELO												
	Nº IMEI						TARJETA SIM				TARJETA DE MEMORIA								
	SISTEMA OPERTATIVO		ANDROID		IOS		WINDOWS PHONE				SYMBIAN		OTRO						
	EMAIL ASOCIADO										ACCESO		SI		NO				
	ACCESORIOS																		
	OBSERVACIONES																		

LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL																				
	TELEFONO		MARCA					MODELO												
	Nº IMEI							TARJETA SIM		TARJETA DE MEMORIA										
	SISTEMA OPERTATIVO		ANDROID		IOS		WINDOWS PHONE			SYMBIAN		OTRO								
	EMAIL ASOCIADO								ACCESO	SI		NO								
	ACCESORIOS																			
	OBSERVACIONES																			

LEVANTAMIENTO DE SOPOORTE DE EVIDENCIA DIGITAL																				
	GPS		MARCA					MODELO												
	Nº DE SERIE							ACCESORIOS												
	TARJETA DE MEMORIA		OBSERVACIONES																	

LEVANTAMIENTO DE SOPOORTE DE EVIDENCIA DIGITAL																				
	DISPOSITIVO SMART		TIPO		MARCA			MODELO												
	Nº DE SERIE							ACCESORIOS												
	OBSERVACIONES																			

LEVANTAMIENTO DE SOPOORTE DE EVIDENCIA DIGITAL																				
	DVR		MARCA					MODELO												
	Nº DE SERIE							ACCESORIOS												
	OBSERVACIONES																			

LEVANTAMIENTO DE SOPOORTE DE EVIDENCIA DIGITAL																				
	OTROS DISPOSITIVOS		TIPO					MARCA												
	MODELO				Nº DE SERIE					ACCESORIOS										
	OBSERVACIONES																			

LEVANTAMIENTO DE SOPOORTE DE EVIDENCIA DIGITAL																				
	OTROS DISPOSITIVOS		TIPO					MARCA												
	MODELO				Nº DE SERIE					ACCESORIOS										
	OBSERVACIONES																			

ANEXO FOTOGRAFICO

OBSERVACIONES
No siendo para más, se da por finalizado el acto, a las ___________ horas, labrada la presente, es leída, ratificada en todo su contenido y firmada al pie por todos los actuantes.-

B. ACTA DE LEVANTAMIENTO DE EVIDENCIA DIGITAL

ACTA DE LEVANTAMIENTO DE EVIDENCIA DIGITAL Nº: _____/20____

DATOS DE LA CAUSA					
FECHA		HORA DE INICIO		HORA DE FINALIZACION	
CARATULA					
VICTIMA					
IMPUTADO					
AUTORIDAD JUDICIAL COMPETENTE					
DEPARTAMENTO JUDICIAL					
DEPENDENCIA		DEPENDENCIA SOLICITANTE			

Seguidamente y preguntado al/los testigo/s si posee/n algún tipo de interés en la presente y si tiene algún tipo de relación con las partes de las presentes actuaciones (art.235 CPP) manifiesta/n que ____ por lo que impuesto de las penas con la que la ley castiga el falso testimonio (art.275 CP) presta juramento en expedirse con veracidad en todo cuanto supiere y le fuere preguntado (art. 100 CPP) como así lo que viere en este acto.-

TESTIGO 1								
APELLIDO Y NOMBRES								
DOMICILIO								
NACIONALIDAD		EDAD		LEE Y ESCRIBE	SI		NO	
DOCUMENTO DNI / CI.PFA / L.E. / L.C Nº				EXHIBE		RECUERDA		

TESTIGO 2								
APELLIDO Y NOMBRES								
DOMICILIO								
NACIONALIDAD		EDAD		LEE Y ESCRIBE	SI		NO	
DOCUMENTO DNI / CI.PFA / L.E. / L.C Nº				EXHIBE		RECUERDA		

ESPECIALISTA EN RECOLECCION					
INFORMATICO		TELEFONIA		OTROS	
APELLIDO Y NOMBRE					
OBSERVACIONES					

LUGAR DE LEVANTAMIENTO										
DOMICILIO CALLE						ENTRE				
NRO		PISO		DEP.		LOCALIDAD				
COMERCIO		DEPOSITO		OFICINA		CASA		DEPARTAMENTO		PRECARIA
OBSERVACIONES										

LEVANTAMIENTO DE EVIDENCIA DIGITAL	
MEMORIA RAM	
MEMORIA DETECTADA	
CAPTURA DE MEMORIA RAM	
ARCHIVO	
HASH	

No siendo para más, se da por finalizado el acto, a las _____ horas, labrada la presente, es leída, ratificada en todo su contenido y firmada al pie por todos los actuantes.-

VI. ANEXO III

I. MODELO PURI

El Modelo PURI®(Proceso Unificado de Recuperación de la Información) establece una guía de labores a desempeñar desde el área técnico-informático forense, organizándolas en fases, actividades y tareas. Se incluye entre paréntesis el destinatario de cada fase, indicando, técnico y/o legal.

Se presenta a continuación un gráfico explicativo de las fases que intervienen en el Modelo PURI.

FASES INTERVINIENTES

1. Fase de relevamiento e identificación

La fase de relevamiento abarca la investigación que se realiza para conocer el caso a trabajar. En un entorno judicial se corresponde con las medidas de "exploración" del caso.

En este sentido, debe considerarse la volatilidad de los datos y priorizar los objetos de interés.

También es importante tener en cuenta el principio de suficiencia de la evidencia, y a su vez considerar que muchos objetos informáticos pueden ocultar información, o su función no ser evidente. Por lo tanto, se recomienda considerar todas las situaciones y decidir en función del caso hasta qué puntos y qué tipo de dispositivos puede abarcar la Identificación/Investigación.

Esta fase está integrada por las siguientes tareas:

1.1 Identificación de Documentación (Legal y Técnica)

Actividades incluidas:

- ✓ Relevamiento de documentos legales (Legal).

Técnica: Pedido de Oficio.

Técnica: Exploración en Internet.

- ✓ Relevamiento de documentos técnicos (Técnico).

Técnica: Pedido de Oficio.

Técnica: Exploración en Internet.

- ✓ Relevamiento de documentos administrativos (Legal).

Técnica: Pedido de Oficio.

Técnica: Exploración en Internet.

- ✓ Relevamiento de documentos de seguridad lógica y física (Técnico).

Técnica: Pedido de Oficio.

Técnica: Exploración en Internet.

1.2 Identificación de Infraestructura IT (Técnica)

Actividades incluidas:

- ✓ Identificación de Servidores Internos y Externos.

Técnica: Para Servidores Internos y Externos – Enumeración.

Herramienta Recomendada: nmap.

Técnica: Para Servidores Externos - Consulta de Nombres de Dominio.

Herramienta Recomendada: Comando Dig.

- ✓ Identificación de Usuarios.

Técnica: Sniffing Red Lan.

Herramienta Recomendada: WireShark.

Técnica: Búsqueda de Usuarios por Internet.

Herramienta Recomendada: Navegadores – Mantra.

- ✓ Identificación de Dispositivo de Usuario (Equipos y Dispositivos Móviles).

Técnica: Enumeración.

Herramienta Recomendada: nmap.

Técnica: Sniffing Red Lan.

Herramienta Recomendada: WireShark.

- ✓ Identificación de Servicios Internos y Externos.

Técnica: Escaneo de Puertos y Servicios.

Herramienta Recomendada: nmap.

2. <u>Fase recolección</u> (Legal y Técnica)

La fase de recolección implica el hecho de conseguir los equipos sobre los que se realizará el trabajo forense. En un caso judicial este hecho puede implicar un "secuestro" durante un allanamiento o en la escena del hecho o una "presentación" espontánea.
Consideraciones:

- ✓ En esta fase debe tenerse en cuenta el principio de suficiencia de la evidencia, y recolectar lo mínimo indispensable para cumplir con el plan de investigación.
- ✓ Aquí puede realizarse la adquisición de algunos elementos y la recolección de otros, dependiendo del entorno, la situación, los recursos disponibles y otros factores variables que el Especialista en Adquisición considere.
- ✓ Resultan de particular interés notaciones y documentación que se encuentre próxima al lugar de allanamiento que contenga información trascendente para el análisis de la evidencia digital.
- ✓ Debido a que se puede trabajar en una orden de presentación, una orden de allanamiento o una escena de crimen, las acciones del Especialista en Recolección o el Especialista en Adquisición deberán adaptarse a cada situación.
- ✓ De tratarse de una actuación judicial, luego de las tareas de recolección deberá prestarse especial atención al llenado de las actas de levantamiento de evidencia, a la correcta mantención de la cadena de custodia y a la preservación adecuada de los objetos.

Esta fase está integrada por las siguientes tareas:

2.1 Detección de Infraestructura IT (Técnica)

Actividades incluidas:

- ✓ Detección de Servidores Internos y Externos (Ej: Red Local, Cloud).

Técnica: Inspección ocular, seguimiento cableado de red.

Técnica: para Servidores Internos y Externos, Enumeración.

Herramienta Recomendada: nmap.

Técnica: para Servidores Externos, Consulta de Nombres de Dominio.

Herramienta Recomendada: Comando Dig.

- ✓ Detección de Dispositivos de Usuario (Ej: Equipos PC, USB, SD, SIM, CD, Dispositivos móviles, etc).

Técnica: Inspección ocular, seguimiento cableado de red.

Técnica: Enumeración.

Herramienta Recomendada: nmap.

Técnica: Sniffing Red Lan.

Herramienta Recomendada: WireShark.

2.2 Recolección de Objetos

Actividades incluidas:

- ✓ Secuestro.
- ✓ Embalaje.
- ✓ Transporte.

3. <u>Fase adquisición</u> (Técnica)

La fase de adquisición involucra las tareas en la que se obtiene el "contenido" a analizar.

Consideraciones:

- ✓ Si el proceso de adquisición altera el medio original, debe justificarse y documentarse debidamente.
- ✓ La etapa de transporte no supervisado es opcional, y contempla el caso en el que, por alguna razón, el Especialista en Recolección no puede o no está autorizado a realizar el traslado de las imágenes obtenidas.

Esta fase está integrada por las siguientes tareas:

3.1 Adquisición de Medios de Almacenamiento Persistente *(Por ej: Disco, Tarjeta SD, ROM interna del Dispositivo)*

Actividades que incluye:

- ✓ Bloqueo del medio de Almacenamiento.

Técnica: Bloqueo por hardware.

Herramienta Recomendada: Bridge USB.

Técnica: Bloqueo por software.

Herramienta Recomendada: comandos de sistema operativos para bloqueo de puertos.

- ✓ Búsqueda de Host Protected Areas (HPA).

Técnica: Comandos de interfaz Serial ATA.

- ✓ Captura y resguardo de la imagen.

Técnica: Copia bit a bit del medio de almacenamiento (por SW).

Herramienta Recomendada: comando dd/ ddrescue (GNU) .

Técnica: Copia bit a bit del medio de almacenamiento (por HW).

Herramienta Recomendada: Duplicador de discos, Imágen Física de Dispositivo(Ej: UFED, XRY, MobilEdit), JTag.

3.2 Adquisición de Datos Volátiles (Ej: RAM Equipo, RAM Dispositivos Móviles, Tablas de Ruteo)

Actividades que incluye:

- ✓ Captura y resguardo.

Técnica: CrashDump por Software (Sólo Memoria RAM).

Herramienta Recomendada: NotMyFault (Sysinternals).

Técnica: Dump completo por Software (Memoria RAM y Área de Paginación - Memoria virtual).

Herramienta Recomendada: kntdd, dd (FAU), FTK Imager, Mandiant Memoryze.

Técnica: Captura de memoria por Hardware.

Herramientas recomendadas: Tribble, Bus Firewire, PCI Express, USB.

Técnica: Comandos internos del router.

3.3 Adquisición de Tráfico de Red

Actividades que incluye:

- ✓ Captura y Filtrado de Paquetes.

Técnica: Sniffing.

Herramienta recomendada: TCPDump, WireShark.

3.4 Adquisición de Smartcards *(Ej: SIM, Tarjetas de Crédito, Pasaportes Inteligentes)*

Actividades que incluye:

- ✓ Lectura del medio (orientada a la norma).

Técnica: Hardware específico.

3.5 Validación y resguardo

Actividades que incluye:

- ✓ Compresión y división de la imagen.

Técnica: configuración en el comando de copia de la información.

Técnica: comandos independientes.

Herramientas recomendadas: GZip /bz2/ ZIP.

- ✓ Generación de hashes.

Técnica: Generación de un hash en Original y copia.

Herramientas recomendadas: MD5, SHA-1.

Técnica: Generación de múltiples hashes, cada N bytes* MD5.

Herramientas recomendadas: MD5, SHA-1.

- ✓ Validación de hashes contra original.

3.6 Transporte no supervisado

Actividades que incluye:

- ✓ Almacenamiento protegido.

Técnica: cifrado del medio de almacenamiento por hardware.

Herramientas recomendadas: discos que incorporan cifrado por dispositivo.

Técnica: cifrado del medio de almacenamiento por software.

Herramientas recomendadas: Tecnología de cifrado transparente, ej: TrueCrypt, o Software ZIP o RAR con protección por contraseña y cifrado.

4. Fase preparación (Técnica)

La fase de preparación involucra las tareas técnicas de preparación del ambiente de trabajo del informático forense, restauración de la imagen y selección del set de herramientas, a fin de dejar preparado el entorno para su posterior análisis.

Consideraciones:

- ✓ Siempre es conveniente contar con la mayor cantidad de herramientas posibles, y que las mismas se encuentren certificadas por alguna entidad que garantice la información recuperada.

- ✓ Las herramientas seleccionadas de código abierto permitirán justificar los resultados de su operación, y seguir su ejecución a nivel instrucciones de ser necesario.

Esta fase está integrada por las siguientes tareas:

4.1. Preparación Extracción

Actividades que incluye:

- ✓ Asegurar espacio libre suficiente.
- ✓ Ensamblado y descompresión de las divisiones de la imagen.
- ✓ Validación del original y copia.

Técnica: generación de hashes.

Herramienta recomendada: Para estas tareas se debe utilizar las mismas herramientas que se utilizaron para la división y generación de hashes.

- ✓ Mapeo de Imagen a dispositivo del Sistema Operativo.

Técnica: loopback device / Dispositivo Virtual.

- ✓ Generación de Máquina Virtual.

4.2. Identificación de Tecnología de la Información en el objeto

- ✓ Recomposición de Volumen RAID.

Técnica: Reconstrucción estadística de arreglos RAID desordenados[6].

- ✓ Identificar cantidad de discos, particiones y tipos de filesystem.

Técnica: Lectura de tabla de particiones.

Técnica: Búsqueda de particiones.

Herramienta recomendada: fdisk, parted, cfdisk,mmls y fsstat de The Sleuth Kit.

- ✓ Identificar y quebrar medios de cifrado.

Técnica: Análisis estadístico y de entropía de sectores de disco.

Técnica: Recuperación de claves de cifrado de imagen de memoria.

Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.

Herramientas recomendadas: volatility, Hashcat/oclHashcat.

- ✓ Identificar cantidad y tipo de Sistemas Operativos presentes.

Técnica: Análisis de tabla de particiones.

[6] Para mayor detalle ver el trabajo “Reconstrucción de Volumenes RAID” (Revista Argentina de Ingeniería, Año 5, Volumen I, Abril 2015) disponible en el sitio http://info-lab.org.ar/images/pdf/10.pdf

- ✓ Identificar Máquinas Virtuales presentes.

Técnica: Búsqueda de hypervisores.

- ✓ Identificar programas instalados en los Sistemas Operativos detectados.

Técnica: Búsqueda de información de aplicaciones en registro (Windows).

Herramientas Recomendadas: RegRipper, Registry Decoder.

Técnica: Búsqueda de información de paquetes (aptitude, RPM, etc).

4.3. Preparación del Ambiente

- ✓ Preparación del Ambiente de Examinación.

5. Fase de extracción y análisis

5.1. Extracción a nivel de aplicación (información semántica dependiendo de la aplicación relacionada: historial web/base de datos/ registros de un sistema / cloud)

Se recomienda realizar las siguientes actividades dependiendo las necesidades del caso:

- ✓ Búsqueda de archivos recientes o frecuentes.
- ✓ Análisis de aplicaciones recientemente utilizadas.
- ✓ Análisis archivos recientes vinculados a herramientas frecuentes.
- ✓ Revisión de historiales de navegación Web (en aplicaciones de uso frecuentes).
- ✓ Análisis de almacenamiento en Cloud.
- ✓ Búsqueda de máquinas virtuales.
- ✓ Búsqueda y extracción papelera de reciclaje.
- ✓ Búsqueda y extracción archivos recientes.
- ✓ Búsqueda y extracción de archivos comprimidos.
- ✓ Búsqueda y extracción navegadores web.
- ✓ Búsqueda y extracción redes sociales.
- ✓ Búsqueda y extracción mensajería instantánea.
- ✓ Búsqueda y extracción correo electrónico.
- ✓ Búsqueda y extracción aplicaciones de transferencia de archivos.
- ✓ Búsqueda y extracción almacenamiento cloud.

- ✓ Búsqueda y extracción aplicaciones multimedia.
- ✓ Búsqueda y extracción archivos temporales.
- ✓ Búsqueda y extracción ofimática.
- ✓ Búsqueda y extracción juegos.
- ✓ Búsqueda y extracción aplicaciones particulares.

Para evaluar cada aplicación enumerada, o aplicaciones que no se han contemplado en el listado anterior, se recomienda:

- ✓ Análisis de los archivos de configuración de la aplicación.
- ✓ Análisis de archivos de datos y bases de datos asociadas a la aplicación.
- ✓ Búsqueda del ejecutable y sus archivos asociados en una base de datos de aplicaciones.
    - Recurso: base de datos NSRL del NIST.
    - Recurso: servicio VirusTotal.
- ✓ Análisis del comportamiento de la aplicación en un entorno controlado.

Técnica: Análisis de memoria y código dentro de un emulador.

Herramientas Recomendadas: QEmu, Pandas.

- ✓ Desensamblado de la aplicación para análisis de comportamiento.

Técnica: Ingeniería inversa sobre código.

Herramientas Recomendadas: bokken, radare, distorm, IDA Pro.

5.2. Extracción a nivel plataforma

- ✓ Obtención de listado de aplicaciones más utilizadas.

Técnica: Análisis de sistema de precarga de aplicaciones.

Herramientas Recomendadas: Nirsoft WinPrefetchView.

- ✓ Recuperación de archivos eliminados.

Técnica: Recuperación en base al sistema de archivos.

Herramientas Recomendadas: Recuva.

- ✓ Extracción de Información a examinar por tipo de archivo.
- ✓ Extracción de metadatos del archivo en el filesystem.

Técnica: Acceso a información del filesystem.

Herramientas recomendadas: The Sleuth Kit, Autopsy.

- ✓ Extracción de archivos protegidos con contraseña.

Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.

Herramientas recomendadas: Hashcat/oclHashcat.

- ✓ Detección y extracción de archivos cifrados.

Técnica: Análisis estadístico y de entropía de los archivos.

Técnica: Recuperación de claves de cifrado de imagen de memoria.

Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.

Herramientas recomendadas: volatility, Hashcat/oclHashcat.

- ✓ Búsqueda de Información de Configuración.
- ✓ Búsqueda de Información de Procesos en Memoria.

Técnica: Análisis de memoria.

Herramientas recomendadas: volatility, Rekall, BIP-M.

5.3. Extracción a bajo nivel (bloques/bytes)

- ✓ Búsqueda de información en disco.
- ✓ Búsqueda de información en el área de paginado.
- ✓ Extracción de archivos en espacio no asignado.

Técnica: File Carving.

Herramientas Recomendadas: Scalpel, PhotoRec, Adroit Photo Forensics, CIRA.

- ✓ Búsqueda de Bases de Datos en particiones no formateadas.

5.4. Análisis de Contenidos

- ✓ Búsqueda de información en el contenido.
- ✓ Búsqueda de información ofuscada u oculta en el contenido.
- ✓ Extracción de metadatos propios del archivo.

5.5. Análisis de Correlaciones

- ✓ Evaluación de puntos de pericia.

- ✓ Identificar relaciones entre elementos.

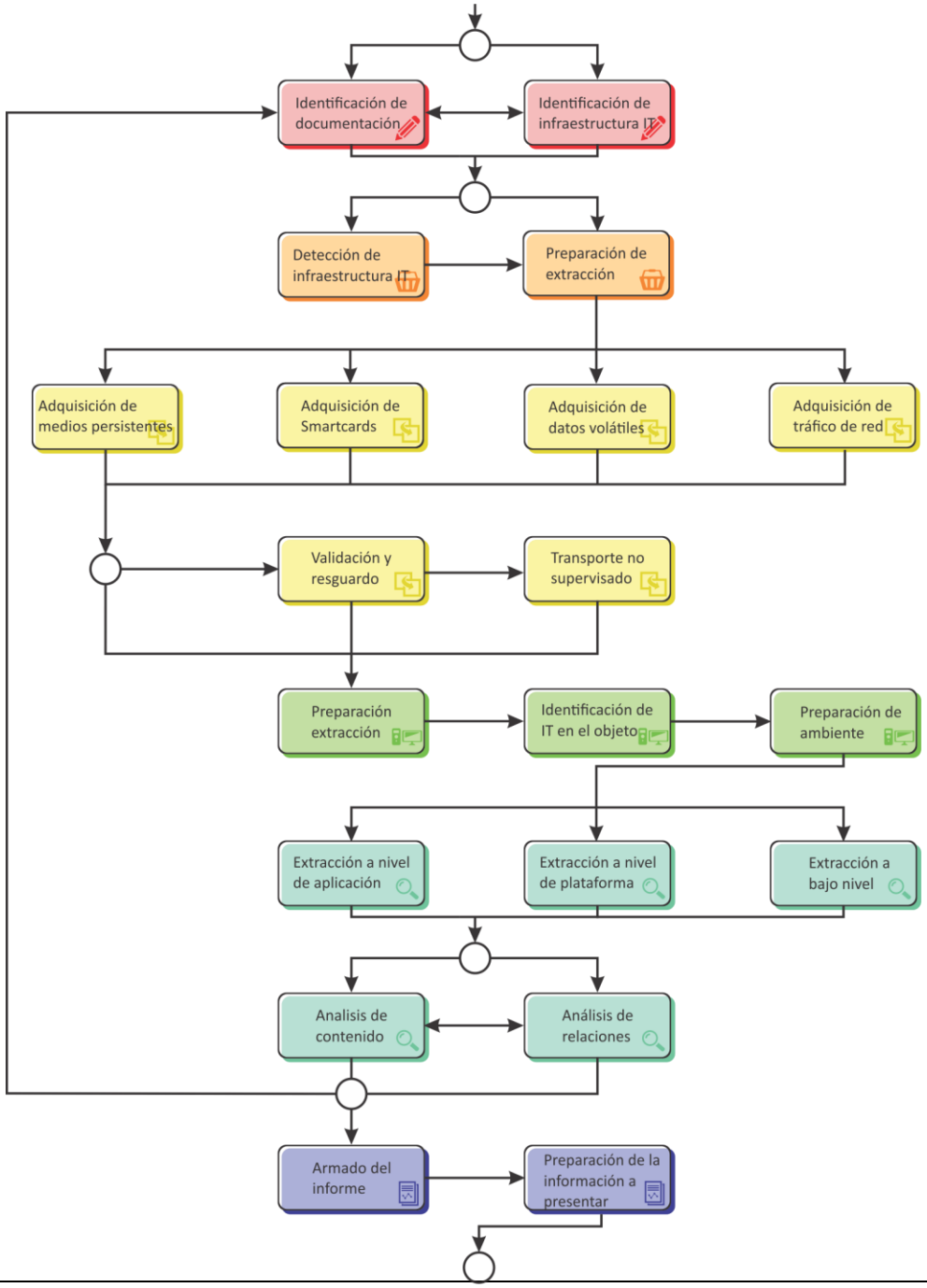
6 Fase presentación

6.1. Armado del Informe

6.2. Preparación de la información a presentar

6.3. Presentación del informe

MODELO PURI – DETALLE DE ACTIVIDADES POR FASE



II. TÉCNICAS Y HERRAMIENTAS DE INFORMÁTICA FORENSE

A. Técnicas y Herramientas – Fase de Adquisición

FASE ADQUISICIÓN

Nº	Herramienta	Tarea	Tecnica	Licencia	Sistema Operativo (host)	Sistema Operativo (dispositivo)	Link
1	dd	Adquisición imagen de disco	Imagen bit a bit	FOSS	Linux		
2	dd (FAU)	Adquisición imagen de disco	Imagen bit a bit	Comercial Free	Windows		http://gmgsystemsinc.com/fau/
3	GNU ddrescue	Adquisición imagen de disco	Imagen bit a bit (con errores).	FOSS	Linux		http://www.gnu.org/software/ddrescue/
4	dc3dd	Adquisición imagen de disco	Imagen bit a bit	FOSS	Linux		http://sourceforge.net/projects/dc3dd/
5	dcfldd	Adquisición imagen de disco	Imagen bit a bit	FOSS	Linux		http://dcfldd.sourceforge.net/
6	FTK Imager	Adquisición imagen de disco	Imagen bit a bit	Comercial Free	Windows		http://www.accessdata.com/support/product-downloads
7	TAFT	Detección HPA	Comandos ATA	Freeware			http://vidstrom.net/stools/taft/
8	HDAT2	Detección HPA	Comandos ATA	Freeware			http://www.hdat2.com/
9	dd (FAU)	Adquisición imagen de memoria	Volcado de memoria	Comercial Free	Windows	Windows	http://gmgsystemsinc.com/fau/
10	FTK Imager	Adquisición imagen de memoria	Volcado de memoria	Freeware	Windows	Windows	http://www.accessdata.com/support/product-downloads
11	LiME	Adquisición imagen de memoria	Volcado de memoria	FOSS	Linux	Linux, Android	https://github.com/504ensicsLabs/LiME
12	Mandiant Memoryze	Adquisición imagen de memoria	Volcado de memoria	Comercial Free	Windows	Windows	https://www.mandiant.com/resources/download/memoryze
13	MoonSols Dumpit	Adquisición imagen de memoria	Volcado de memoria	Comercial Free	Windows		http://www.moonsols.com/resources/
14	md5sum	Cálculo de hashes	Hash MD5	FOSS	Linux		
15	hashdeep	Cálculo de hashes	Hash MD5, SHA-1, SHA-256, SHA-512, piecewise hashing	FOSS	Linux, Windows		https://github.com/jessek/hashdeep/releases/tag/release-4-4
16	piecehash	Cálculo de hashes	Hash MD5, SHA-1, SHA-256, SHA-512, piecewise hashing	FOSS	Linux, Windows		https://github.com/bconstanzo/piecehash

B. Técnicas y Herramientas – Fase de Preparación

FASE PREPARACIÓN

Nº	Herramienta	Tarea	Tecnica	Licencia	Sistema Operativo (host)	Sistema Operativo (dispositivo)	Link
1	OSFMount	Montar imagen		Freeware	Windows		http://www.osforensics.com/tools/mount-disk-images.html
2	ImDisk	Montar imagen		Freeware	Windows		data.se/opencode.html/#ImDisk
3	FTKImager	Montar imagen		Freeware	Windows		http://www.accessdata.com/support/product-downloads
4	Prototipo RE-RAID FI-UFASTA	Reconstrucción RAID	Curti et al. 2014		Linux		
5	RAID Reconstructor	Reconstrucción RAID		Comercial	Windows		http://www.runtime.org/raid.htm
6	raw2vmdk	Traducir a disco virtual	Conversión raw a vmdk	FOSS	Linux, Windows		http://sourceforge.net/projects/raw2vmdk/
7	VBoxManage convertdd	Traducir a disco virtual	Conversión raw a vmkd, vdi	FOSS	Linux, Windows		https://blog.sleeplessbeastie.eu/2012/04/29/virtualbox-convert-raw-image-to-vdi-and-otherwise/
8	OpenLV	Generación de máquina virtual		FOSS	Linux, Windows		http://openlv.org/
9	LiveView	Generación de máquina virtual		FOSS	Linux, Windows		http://liveview.sourceforge.net/
10	VirtualBox	Utilización de máquina virtual		FOSS	Linux, Windows		https://www.virtualbox.org/
11	VMWare Workstation	Utilización de máquina virtual		Free/Comercial	Linxu, Windows		http://www.vmware.com/
13	md5sum	Cálculo de hashes	Hash MD5	FOSS	Linux		
14	hashdeep	Cálculo de hashes	Hash MD5, SHA-1, SHA-256, SHA-512, piecewise hashing	FOSS	Linux, Windows		https://github.com/jessek/hashdeep/releases/tag/release-4.4
15	piecehash	Cálculo de hashes	Hash MD5, SHA-1, SHA-256, SHA-512, piecewise hashing	FOSS	Linux, Windows		https://github.com/bconstanzo/piecehash

C. Técnicas y Herramientas – Fase de Análisis. Etapa Extracción Lógica

FASE ANÁLISIS - ETAPA EXTRACCIÓN LÓGICA

Nº	Herramienta	Tarea	Tecnica	Licencia	Sistema Operativo (host)	Sistema Operativo (dispositivo)	Link
1	hmft	Análisis de NTFS	Extracción MFT	Freeware			http://www.hexacorn.com/blog/2012/04/16/hmft-yet-another-mft-extractor/
2	analyzeMFT	Análisis de NTFS	Análisis de MFT	FOSS	Linux, Windows		https://github.com/dkovar/analyzeMFT
3	MFT Tools	Análisis de NTFS	Análisis de MFT	Freeware	Windows		https://github.com/jschicht
4	RegRipper	Análisis de Registro		FOSS	Windows		http://regripper.wordpress.com/
5	RegistryDecoder	Análisis de Registro		FOSS	Linux, Windows		http://www.digitalforensicssolutions.com/registrydecoder/
6		Análisis de Registro	Shellbags				
7	The Sleuth Kit	Análisis de discos		FOSS	Linux, Windows		http://www.sleuthkit.org/
8	Autopsy	Análisis de información del sistema		FOSS	Linux, Windows		http://www.sleuthkit.org/
9	undbx	Recuperación de emails		FOSS	Windows		https://code.google.com/p/undbx/

D. Técnicas y Herramientas – Fase de Análisis. Etapa de Extracción Física

FASE ANÁLISIS - ETAPA EXTRACCIÓN FÍSICA

Nº	Herramienta	Tarea	Tecnica	Licencia	Sistema Operativo (host)	Sistema Operativo (dispositivo)	Link
1	Adroit Photo Forensics	File carving	SmartCarving(TM)	Comercial	Windows		assembly.com/products/adroit-photo-forensics/
2	scalpel	File carving	Header/Footer carving	FOSS	Linux, Windows		https://github.com/sleuthkit/scalpel
3	PhotoRec	File carving	File Structure based carving	FOSS	Linux, Windows		http://www.cgsecurity.org/wiki/PhotoRec
4	CIRA	File carving	Multi algoritmo	FOSS	Linux, Windows		https://github.com/info-lab
5	CIRA FileValidators	Validación de archivos	Validadores rápidos por formato	FOSS	Linux, Windows		https://github.com/info-lab/FileValidators
6	Volatility	Análisis de memoria		FOSS	Linux, Windows		http://www.volatilityfoundation.org/
7	Mandiant Memoryze	Análisis de memoria		Freeware	Windows		https://www.mandiant.com/resources/downloads/
8	Mandiant RedLine	Análisis de memoria		Freeware	Windows		https://www.mandiant.com/resources/downloads/
9	BIP-M	Análisis de memoria		FOSS	Windows		

E. Técnicas y Herramientas – Fase de Interpretación (Análisis de Relaciones)

FASE ANÁLISIS - ETAPA ANÁLISIS DE RELACIONES

Nro	Herramienta	Tarea	Tecnica	Licencia	Sistema Operativo (host)	Sistema Operativo (dispositivo)	Link
1	antiword	Extracción y búsqueda de texto en documentos		FOSS			http://www.winfield.demon.nl/
2	pdfminer	Extracción y búsqueda de texto en documentos		FOSS			https://github.com/euske/pdfminer/
3	Pandoc	Extracción y búsqueda de texto en documentos		FOSS			http://pandoc.org/
4	exiftool	Extracción y búsqueda de metadatos		FOSS	Linux, Windows		http://www.sno.phy.queensu.ca/~phil/exiftool/
5	exiftoolGUI	Extracción y búsqueda de metadatos		FOSS	Windows		http://freeweb.siol.net/hrastni3/foto/exif/exiftoolgui.htm
6	Nirsoft MyLastSearch	Historial de búsquedas de Internet		Freeware	Windows		http://www.nirsoft.net/
7	Nirsoft CacheView	Análisis de cache de navegador		Freeware	Windows		http://www.nirsoft.net/
8	Nirsoft CokiesView	Análisis de cookies de navegador		Freeware	Windows		http://www.nirsoft.net/
9	Nirsoft HistoryView	Historial de navegación de Internet		Freeware	Windows		http://www.nirsoft.net/
10	Nirsoft IE PassView	Contraseñas almacenadas por Internet Explorer		Freeware	Windows		http://www.nirsoft.net/
11	Nirsoft PasswordFox	Contraseñas almacenadas por Firefox		Freeware	Windows		http://www.nirsoft.net/
12	Nirsoft WinPrefetchView	Análisis de pre-carga de aplicaciones		Freeware	Windows		http://www.nirsoft.net/

VII. ANEXO IV

ASPECTOS LEGALES Y ESTRATÉGICOS DEL EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL

Hacia una visión de conjunto

La pluralidad de intervinientes en las tareas relacionadas con la informática forense exige que todos posean una visión de conjunto:

- ✓ Para los fiscales es crucial familiarizarse con los aspectos técnicos de la actividad informático forense. Este conocimiento les ayuda a evaluar la pertinencia del empleo de la experticia informática en determinados casos o grupos de casos, teniendo en cuenta las exigencias legales. Todo ello contribuye a potenciar y facilitar la dirección de las investigaciones y la labor de litigación, conforme el abordaje estratégico de cada caso.
- ✓ Los peritos y especialistas en informática deben conocer no sólo los procedimientos y herramientas técnicas recomendadas vinculadas con su función. Es necesario que conozcan también las exigencias y límites legales de su desempeño, y que sepan cuál será el rol específico que desempeñarán en cada caso concreto, para poder integrar eficazmente su labor en la actividad estratégica del Ministerio Público Fiscal.
- ✓ La colaboración de los investigadores judiciales es clave en la planificación de las investigaciones penales, y su rol es irreemplazable en la ejecución de dichos planes. La creciente aparición de evidencias digitales en los procesos penales les exige fortalecer sus conocimientos en esta área e integrarlos con el saber proveniente de otras especialidades criminalísticas.

A. CONCEPTOS GENERALES

1. Nuevas tecnologías, delito y proceso penal

La constante evolución tecnológica y los nuevos hábitos culturales vienen impulsando el desarrollo de la informática de manera constante, involucrando, con mayor o menor intensidad, a todas las sociedades del mundo. Las nuevas tecnologías de la información y la comunicación (NTICS) se fueron incorporando efectivamente en millones de hogares en las más diversas latitudes y longitudes. Las redes han llegado no sólo a los centros de investigación, universidades, centros comerciales, banca financiera y área de negocios, sino que actualmente permiten relaciones al por menor dentro y fuera de la casa. Las relaciones humanas se amplían y los idiomas se simplifican, permitiendo novedosas formas de interacción.

Sin embargo, el surgimiento de Internet, y las consecuentes oportunidades tecnológicas que ofrece, han traído como corolario nuevos peligros y amenazas para la vida social y personal. No podemos perder de vista que el ciberespacio ha brindado nuevas oportunidades para la comisión de delitos, trayendo también como consecuencia la aparición de nuevas maniobras que se originan y tienen existencia únicamente a partir del uso de sistemas informáticos.

Paralelamente, las NTICS aportan herramientas de gran potencial para la investigación y persecución de las nuevas formas delictivas, y de muchos delitos tradicionales. Pero la utilización de estas herramientas encuentra tres desafíos: a) el respeto de los derechos de las personas y del orden jurídico; b) el empleo de metodologías de trabajo adecuadas; y c) la integración de la labor técnico-informática en el conjunto de la actividad investigativa y probatoria. Es en este contexto, que se visualiza como imprescindible contar con un protocolo de actuación judicial en informática forense.

2. La Informática Forense

La Informática Forense es la ciencia de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente en un medio computacional.

Existen distintas fases y modalidades de actuación relacionadas con la informática forense que, a lo largo de un proceso penal, llevan a cabo expertos, investigadores y profesionales del derecho. Por ejemplo, la planificación previa, la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

Una de las principales finalidades de la informática forense es el hallazgo de evidencias digitales, entendidas como información de valor almacenada o transmitida en una forma binaria. El cometido del experto o técnico informático será, entonces, la correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio, aplicando las técnicas y herramientas disponibles o creándolas, y garantizando un proceso reproducible de adquisición, examen, análisis, cotejo, preservación y presentación de la evidencia, que fortalezca su valor probatorio ante los órganos jurisdiccionales.

3. Necesidad de contar con una Guía Integral

Los cambios en las tecnologías, plataformas, medios de almacenamiento, legislaciones y aplicaciones de software, hacen cada vez más necesario el uso de procesos, métodos, estándares y buenas prácticas, que brinden algún tipo de garantías en la recuperación de información almacenada digitalmente y, sobre todo, que permitan asegurar que se realizaron todas las tareas posibles con los mecanismos adecuados.

La tarea de recuperación de la información tiene un aspecto forense cuando se la utiliza en procesos judiciales para obtener evidencia o corroborar la ya obtenida. Si bien existen guías o recomendaciones sobre cómo realizar procesos de recuperación de información en ámbitos forenses, las mismas no constituyen estándares adoptados por los organismos de justicia de nuestro país y de nuestra provincia.

Por todo ello, aparece como necesario elaborar, difundir y aplicar un Protocolo común y homogeneizar la realización de tareas de investigación y peritajes informáticos vinculados a la informática forense. Desde hace unos años, diferentes autores y organizaciones han estado trabajando en guías de buenas prácticas en informática forense. Al analizar estas guías se detectó que, si bien constituyen un excelente aporte procedimental, muchas abarcan sólo una parte del proceso, otras son muy generales, y otras focalizan únicamente en problemáticas delictivas específicas.

Por otro lado, para facilitar y tornar provechoso el empleo de la informática forense, parece imprescindible integrar la dimensión técnica en sus contextos jurídico, estratégico y organizacional. En otros términos, las labores informático forenses deben llevarse a cabo de un modo acorde con nuestra normativa y alineadas con las estrategias de actuación del Ministerio Público Fiscal.

- ✓ Desde el aspecto técnico, se ha elaborado un protocolo basado en el Proceso “PURI” - Proceso Unificado de Recuperación de Información, en la incorporación de variadas experiencias en la realización de pericias informáticas y en la consulta de normas y guías nacionales e internacionales referentes al tema. Se recomienda complementar este Protocolo con guías de recomendaciones o buenas prácticas y/o artículos científicos cuando haya dudas o situaciones no contempladas.
- ✓ En cuanto al marco jurídico, se ha de procurar preservar la validez legal de las actividades investigativas y periciales, minimizando a su vez los perjuicios o afectaciones de derechos de las partes y de terceros. Son muchos los derechos y garantías que pueden verse afectados mediante la labor informático foren-

se. La excelencia técnica no debe transitar por carriles apartados de la ley.

- ✓ La validez legal y la calidad técnica son condiciones necesarias, pero no suficientes, para lograr las metas buscadas. La dimensión estratégica hace a la razón de ser del Ministerio Público Fiscal. Para defender adecuadamente los intereses sociales y la vigencia equilibrada de los valores jurídicos fundamentales (art. 1° de la ley 14.442), se requiere articular un sinnúmero de actividades en las que suelen intervenir diversos actores: la priorización de determinados tipos de problemáticas político criminales (que se traduce en la asignación diferencial de recursos), la elección de la modalidad de abordaje más adecuada a cada caso, la planificación y ejecución eficaz de las variadas labores de investigación y litigación, etc. Aquí es donde debe integrarse la actividad informático forense.

Existen además otras utilidades adicionales. Hablar de sistemas de abordaje de casos, sistemas de investigación y sistemas de litigación nos lleva a las áreas de dirección estratégica, gestión, capacitación y aprendizaje organizacional. La presente Guía Integral de Empleo de la Informática Forense en el Proceso Penal podrá incorporarse en dichas áreas, y constituirse en material de consulta y discusión para los procesos de mejora continua de los servicios que brinda el Ministerio Público a la sociedad.

B. LA INFORMÁTICA FORENSE EN EL PROCESO PENAL

1. Plan de investigación penal. Teoría del Caso y Litigación

La informática forense no es una disciplina teórica, sino una ciencia aplicada que acude en auxilio de finalidades determinadas. Como tal, está regida por criterios de utilidad y pertinencia. Los expertos en informática forense no actúan en un vacío institucional y social. Para poder potenciar su aporte, es necesario conocer mínimamente el sistema en el cual se integran.

Frente a la noticia de un delito de acción pública, el Ministerio Público Fiscal interviene asumiendo la defensa de los intereses sociales y de la vigencia equilibrada de los valores constitucionales y legales involucrados (art. 1º de la ley 14.442). Esta intervención tiene varias posibles facetas: la averiguación del hecho, la persecución de los sospechosos, la acusación, etc. Desde una perspectiva más amplia, el Ministerio Público Fiscal también tiene a cargo la priorización de casos, el establecimiento de modalidades de abordaje para cada tipo de fenómenos criminales, la promoción de mecanismos de justicia restaurativa, etc.

La noticia de un delito o de un conjunto distinguible de delitos debe ser investigada.

En nuestro Código Procesal Penal, la investigación preliminar es responsabilidad del Ministerio Público Fiscal (arts., 56. 59 y 267 del CPPBA). En este punto, surgen algunas preguntas: ¿qué investigar?, ¿para qué?, ¿cómo hacerlo? Estas cuestiones son de gran utilidad para ordenar la actividad investigativa.

- ✓ Qué investigar: Existe una enorme variedad de delitos y de noticias de delito. Hay casos más o menos graves, aislados o inscriptos en un entramado delictivo (conflictos crónicos, criminalidad organizada), con mayor o menor cantidad de sospechosos o víctimas, con diversos grados de complejidad investigativa y probatoria, con daños irreversibles o reparables, hechos pasados o en curso, etc. Definir el objeto de la intervención será fundamental para los dos pasos siguientes.
- ✓ Para qué investigar: La investigación penal no es una investigación teórica. Se investiga para adoptar decisiones, Por ello, el Fiscal debe ir delineando desde el primer momento una estrategia de intervención. Tal estrategia ha de estar alineada con los criterios normativos e institucionales de política de abordaje penal que sean de aplicación al caso. Además, debe ser adecuada a las particularidades del caso concre-

to y adaptable a las cambiantes circunstancias que se vayan presentando (resultado de las medidas adoptadas, dinámica de los intereses sociales y valores jurídicos en juego, comportamiento de los demás actores procesales, etc.).

- ✓ Cómo investigar: El concreto objeto de investigación y los fines trazados ayudarán a definir los diversos aspectos de la actividad a desplegar (asignación de recursos, posibilidades de estandarización y/o secuencialidad, pedidos de colaboración, manejo de tiempos, unión o separación de casos, cantidad y tipo de medidas, nivel de formalización de cada diligencia, inclusión o no de medidas pasibles de afectar derechos, etc.).

Como puede verse, aun en los casos más simples, toda investigación requiere algún nivel de planificación, y debe integrarse armónicamente en el conjunto de investigaciones y estrategias del Ministerio Público Fiscal (sistemas investigativos y sistemas de abordaje de problemáticas político criminales). Este es, a grandes rasgos, un marco de referencia insoslayable para planificar y llevar a cabo las tareas de informática forense. El plan de investigación (que debe enmarcarse en la estrategia de intervención), da sentido y orienta a cada labor investigativa, siendo además un instrumento para controlar sus resultados. En la formulación (y eventuales reformulaciones) de este plan deben participar, con responsabilidades diferenciadas, el fiscal y el equipo de investigadores.

Aunque en la práctica no suele haber secuencias rígidas, podemos distinguir tres funciones de la actividad investigativa:

- ✓ Función exploratoria. Está dirigida a esclarecer ciertas cuestiones, que pueden presentarse en forma conjunta o separada: comprobar si existe un hecho delictuoso, precisando sus características concretas; determinar las circunstancias que permitan calificarlo legalmente; individualizar a sus autores y partícipes; detectar casos conexos; etc. (v. arts. 267 y 32 del CPPBA). La información que proporciona la función exploratoria de la investigación es un insumo necesario para la adopción de decisiones con relevancia procesal (desestimación, archivo, propuestas conciliatorias, imputación, pedido de medidas de coerción, etc.).
- ✓ Función persecutoria. Esta función de la investigación ofrece apoyo a las acciones procesales estratégicas (imputación, peticiones, negociaciones con las partes, preparación del juicio oral). Por ejemplo: dar sustento a la formulación de imputación y al requerimiento de citación a juicio; justificar la solicitud de medidas de coerción; otorgar bases sólidas para proponer acuerdos alternativos al juicio (suspensión a prueba, juicio abreviado, etc.); obtener y preservar pruebas para el juicio oral; etc.
- ✓ Función de resguardo de la defensa en juicio. Se trata de un deber del Ministerio Público Fiscal, ajeno a su plan de investigación. Cabe incluir aquí a la evacuación de las citas vertidas por las personas imputadas, y a las medidas investigativas propuestas por las partes. Esta función, primordialmente al servicio de las partes, puede servir además para que el fiscal chequee la fortaleza de su teoría del caso.

La denominada teoría del caso es una herramienta metodológica para la litigación, que reviste utilidad en todas las fases del proceso. A medida que la función exploratoria de la investigación va ofreciendo un panorama más claro acerca de los sucesos, de su calificación legal y de la participación de los sospechosos, el Fiscal va formando una hipótesis de los hechos. Para poder transitar hacia la faz persecutoria, la hipótesis debe sustentarse sobre dos bases. Por un lado, esos hechos hipotéticos deben ser encuadrables en normas penales que establezcan una consecuencia legal.

Por otro lado, los hechos deben ser mostrados como verosímiles y probables ante el juez de garantías. Asimismo, es necesario ir identificando, obteniendo y preservando los elementos probatorios que serán necesarios en la

etapa de juicio.

Ya en el ejercicio de su rol acusatorio (en el debate oral o al acordar un juicio abreviado), el Fiscal debe probar esos hechos ante el tribunal, para poder generar las consecuencias legales. El tránsito de la investigación exploratoria hacia la investigación persecutoria y de ésta hacia la función acusatoria debe ser armónico. De nada sirve hablar de un "caso resuelto" o esclarecido, si se olvida que todavía hay que probar los hechos ante un juez.

Los hechos a probar se presentan, en primer lugar, como un conjunto de afirmaciones fácticas que responden a preguntas básicas: qué, quién (o quiénes), dónde, cuándo, a quién, cómo, con qué, para qué o por qué. Existe un segundo orden de hechos necesitados de prueba, que es el de los indicios (hechos que no forman parte del relato acusatorio, pero que confluyen a probar algunos de sus extremos).

Cada una de las afirmaciones sostenidas ante el tribunal debe ser probada, y no existe una prueba única, apta para cubrir todos y cada uno de los puntos del relato acusatorio. Para cada afirmación se requiere prueba relevante, suficiente, confiable y legalmente válida. Es necesario, entonces, prever y precisar cuáles son los límites y aportes específicos de cada elemento probatorio respecto de cada una de las afirmaciones sostenidas en la persecución y en la acusación. Esta aclaración es especialmente válida para la prueba pericial informática, dada su complejidad, sus costos, y los condicionamientos legales existentes para su admisibilidad.

2. Consideraciones sobre la Evidencia Digital

El vocablo evidencia proviene del latín *evidentĭa* y significa "certeza clara y manifiesta de la que no se puede dudar". La búsqueda e identificación de posibles evidencias es una de las tareas vinculadas a la formulación y ejecución del plan de investigación. Desde el punto de procesal, las evidencias pueden cumplir esencialmente dos funciones:

- ✓ Función orientadora: la evidencia proporciona una pista o hilo conductor que permite avanzar en una investigación. La pista por sí misma no necesariamente acredita un extremo del hecho investigado. Un ejemplo de ello es la obtención de una dirección IP que conduzca luego a un domicilio físico.
- ✓ Función probatoria: la evidencia puede ser invocada como prueba de los hechos que afirma una de las partes del proceso. Por ejemplo: un archivo de video que aparece captando una colisión vehicular o un intento de cohecho.

Una evidencia puede cumplir sucesivamente ambas funciones. Es relevante recordar que cuando se pretende emplear evidencia en función probatoria, deben haberse cumplido los requisitos de relevancia, suficiencia, confiabilidad y validez de esa prueba.

La incorporación de las tecnologías de información a la vida cotidiana ha marcado la necesidad de incluir a los medios informáticos como elementos de carácter probatorio.

Con el desarrollo de la disciplina denominada "Informática Forense", se ha trabajado sobre su principal objeto de estudio: la evidencia digital. El término evidencia ha sido en principio relacionado al de "física" dando como resultado el concepto de "evidencia física". Ello pareciera ser contrastante con el término "evidencia digital", por cuanto, todo aquello relacionado con el término "digital" se ha asimilado al término "virtual", es decir, como no real. Es de importancia destacar que los datos o evidencia digital siempre están almacenados en un soporte real, siendo este último de tipo físico, por lo que este tipo de evidencia podría considerarse igualmente física.

De acuerdo con la Guidelines for the Managment of IT Evidence, la evidencia digital puede dividirse en tres categorías:

- ✓ Registros almacenados en el equipo de tecnología informática (por ejemplo, correos electrónicos, archi-

vos de aplicaciones, imágenes, etc.).

- ✓ Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
- ✓ Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos vistas parciales de datos, etc.).

Existe un principio de las ciencias forenses que relaciona la escena del hecho con la víctima y el victimario a través de la evidencia. Se trata del Principio de Intercambio de Locard, por el cual se explica que siempre que estén en contacto dos objetos, éstos transfieren material de cada uno en el otro. Esto implica que en el lugar del hecho se puede encontrar algún elemento que ayude a esclarecer lo sucedido, indicios y rastros que describen lo ocurrido. Para que un caso se resuelva, todos los elementos deben estar relacionados mediante las evidencias. Entonces, el objetivo es establecer el vínculo entre los tres elementos (escena, victima, victimario) ya que el victimario se llevará material del lugar y de la víctima, la víctima tendrá material del victimario y la escena del hecho tendrá de ambos. En lo que hace a la informática forense, el principio de intercambio opera bajo modalidades sumamente variadas. La "escena del hecho" puede llegar a estar diseminada en diferentes lugares físicos (escena virtual).

Por su parte, los diversos rastros digitales que deja el contacto entre escena, víctima y victimario requieren de un análisis complejo para poder reconstruir esta vinculación. La ciencia informático forense proporciona los principios y técnicas aplicables para identificar, obtener, analizar y contribuir a interpretar la evidencia digital durante una investigación criminal.

3. El hardware, el software y los datos como Evidencia

A la hora de investigar un hecho y/o suceso determinado, debe tenerse en consideración las distintas fuentes de evidencia. De este modo, el hardware y/o el software y/o los datos pueden ser:

- ✓ Mercancía ilegal o fruto del delito. En tal caso, su posesión o tráfico no están autorizadas por la ley.
  - Un ejemplo de hardware ilegal son los decodificadores de la señal de televisión por cable comercializados a espaldas de la empresa proveedora del servicio. El hardware es fruto del delito cuando es obtenido mediante robo, hurto, fraude u otra clase de infracción.
  - El software que viola la legislación de propiedad intelectual, poseído y utilizado por el sospechoso, es mercancía ilegal.
  - Ejemplo de datos: un archivo de datos personales ilegalmente obtenido puede ser una mercancía ilegal.
- ✓ Instrumento para la comisión de un delito. La evidencia ha sido utilizada como herramienta para la perpetración del ilícito.
  - Un ejemplo de hardware sería un router, una pc funcionando como router y cualquier otro dispositivo especialmente diseñado para capturar el tráfico en la red o interceptar comunicaciones.
  - Software instrumento del delito es aquél que es desarrollado y/o utilizado para cometer el delito (ej.: un virus informático).
  - La información falsa subida a una página web de compraventas puede ser uno de los instrumentos del ardid desplegado para cometer un fraude.
- ✓ Evidencia. En este caso, el hardware, el software y los datos no son una mercancía ilegal, fruto del delito

ni un instrumento de su comisión. Son elementos físicos que revisten utilidad como prueba de la comisión de un delito.

- La impresora en la cual un consumidor de pornografía infantil imprimió una imagen enviada por el sospechoso, resulta ser hardware de evidencia.
- Como ejemplo de software evidencia de un delito, podemos mencionar a un programa utilizado por el autor del ilícito, luego de cometido éste, para eliminar o disimular evidencia incriminatoria.
- Un archivo de cámara de video filmación digital puede ser evidencia relativa a un delito vinculado con el tránsito vehicular.

Los dispositivos de hardware, si bien no son evidencia digital, pueden revestir utilidad investigativo probatoria y/o estar sujetos a decomiso, destrucción o restitución.

Su recolección y examen puede estar abarcado por las competencias de los especialistas informáticos.

C. CUESTIONES DE JURISDICCIÓN Y COMPETENCIA. COOPERACIÓN INTERNACIONAL

En muchos casos en que los dispositivos, software y datos informáticos pueden ser objeto o instrumento del delito, o prueba de éste), emerge la necesidad de considerar las cuestiones de jurisdicción legal y competencia judicial.

Las reglas de competencia tienen como objetivo determinar cuál va a ser el tribunal que va a intervenir, con preferencia o exclusión de los demás, en una controversia que ha puesto en movimiento la actividad jurisdiccional. Dentro de las diferentes clases de competencia existentes (por cuantía, por materia, por grado y por territorio) en esta temática se tendrá especialmente en cuenta la competencia en razón del territorio.

Determinados delitos (delitos a distancia) pueden haber sido ejecutados desde distintos lugares, y tener efectos en otros tantos. La cuestión se torna más compleja aun cuando varias personas contribuyen a una acción delictiva, y/o cuando hay víctimas situadas en distintos puntos geográficos. Incluso las pruebas de la comisión de algunos ilícitos pueden estar diseminadas en distintos territorios.

Nuestro país tiene una estructura federal. Ante la presunta comisión de la mayoría de los delitos, interviene la justicia penal ordinaria de la provincia de que se trate. Ante ciertos casos de excepción legalmente establecidos, es competente la justicia nacional o federal (ver ley 48).

Las controversias acerca de la ley aplicable y la determinación del juez competente (ya sea para decidir en un caso o sólo para obtener una prueba) son más problemáticas cuando involucran a diferentes países. A ello se suma la particular configuración de la nube, que es administrada por entidades privadas y sólo parcialmente regulada por los Estados.

Según el art. 1° del Código Penal de la Nación, éste es la ley aplicable ante delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción, y ante delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo. De modo coincidente, para establecer el “lugar de comisión del delito” y, consecuentemente, la competencia judicial, nuestra Corte Suprema de Justicia de la Nación ha adoptado este criterio de ubicuidad (CSJN, "Ruiz Mira". Fallos: 271:396; íd., Competencia N° 63. XXXVI, Tatarsky, Héctor Eduardo s/ denuncia, 29/08/2000, Fallos: 323:2335). El hecho se considera cometido tanto en el lugar donde se produjo la exteriorización de voluntad del autor como donde se concretó el resultado. Para decidir si es competente el tribunal del lugar de exteriorización de la voluntad o el de producción del resultado, se aplican criterios centrados en la mejor y más pronta administración en justicia (defensa en juicio de las partes, celeridad y economía procesal).

En cuanto a la ley aplicable, el principio de territorialidad se complementa con el principio real, de defensa o de protección de intereses, por cuanto el principio territorial es insuficiente para cubrir un buen número de casos. El principio real constituye un criterio de aplicación de la ley penal que posibilita la sujeción a ésta de las infracciones contra ciertos bienes o intereses estatales cometidos fuera del territorio del país emisor de la norma jurídica penal; es decir, atiende primordialmente a la naturaleza e importancia del bien jurídico protegido agredido por el delito, sin que importe el lugar donde fue ejecutado el hecho ni la nacionalidad de sus autores (por ejemplo, un grupo de extranjeros, en un país distinto, fabrican moneda argentina falsa). Con carácter excepcional y subsidiario, se aplican los principios de la nacionalidad o de la personalidad (cuando el autor o la víctima son nacionales, en relación a un delito cometido en el extranjero, y funciona mediante tratados de extradición) y el principio universal o de justicia mundial (que se persiguen en cualquier país, porque lesionan bienes jurídicamente reconocidos por toda la comunidad internacional, como el caso de los delitos llamados de lesa humanidad).

No todos los países aplican las mismas reglas para determinar la ley aplicable y la competencia judicial. Para poder clarificar estas cuestiones, es necesario establecer cuál es la normativa de derecho internacional que rige la relación con cada Estado (convenios bilaterales y tratados, por ejemplo el Tratado de Derecho Penal Internacional de Montevideo).

En cuanto a las medidas de investigación y de prueba, también existen convenios bilaterales y tratados de asistencia recíproca. Hay asimismo normas de cooperación entre autoridades policiales, y a ello debe añadirse la relación que cada Estado establece con los distintos ISP. El nivel de afectación de derechos fundamentales que implique cada medida (ej.: privacidad), visto desde la perspectiva de cada Estado y/o ISP, determinará en general la vía a seguir para acceder a la prueba. Ello implica distintos niveles de demora, que deben ser contemplados teniendo en cuenta el grado de relevancia y urgencia que reviste la medida en el plan de investigación del Fiscal.

En determinados casos, es además necesario coordinar con autoridades extranjeras la realización de procedimientos simultáneos, para asegurar el éxito de las medidas. Aun superados estos escollos, resta prever el nivel de confiabilidad o valor convictivo que tendrá la prueba recibida de un Estado extranjero o de un ISP con sede en el exterior.

El instrumento internacional más abarcativo de estas cuestiones es la Convención de Cibercriminalidad de la Unión Europea (Budapest, 2001). Nuestro país ha manifestado su intención de adherir a la misma (cf. Resolución Conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos de la Nación) y ha ido adaptando su legislación de fondo al texto de ese Convenio. En cambio, no ha habido procesos de adecuación de las normas procesales. No obstante ello, la Convención de Budapest puede ser tomada como punto de referencia para adoptar criterio en diversas problemáticas procesales y para optimizar lo relativo a la gestión de diligencias investigativas y/o probatorias.

Particularmente importante es contar con un nexo permanente con organismos judiciales y policiales del país y del extranjero, y con proveedores de servicios de internet (ISP). Dicho nexo debería contar con información legal actualizada, manejo de los mecanismos de cooperación con organismos públicos y empresas privadas.

Además, podría centralizar el conocimiento de las particularidades de cada servicio de internet: tipo de servicio, tecnologías utilizadas, subcontratos con otras empresas, convenios con clientes, grado de capacitación del personal técnico asignado a las cuestiones forenses, contratos tipo con los usuarios, sede legal de las empresas, ubicación física de la información almacenada en la nube, etc. Operando internamente como mesa de atención para los investigadores judiciales, permitiría agilizar la identificación de evidencia potencialmente útil, la evaluación de su relevancia y confiabilidad, prever los tiempos de demora y los riesgos de pérdida de datos (adoptando los recaudos pertinentes), y establecer los mecanismos lícitos más rápidos y seguros para la obtención de pruebas.

D. INTERVENCIONES EN LA ESCENA DEL HECHO

A partir de la naturaleza de estos procedimientos y de la relevancia de la evidencia buscada, se debe tener especial cuidado en evitar cuestionamientos respecto del levantamiento y la custodia de los elementos que se presentan ante la autoridad jurisdiccional, aventando cualquier sospecha sobre su validez legal y dejando en claro de manera indubitada que los efectos se corresponden con los efectivamente secuestrados en la escena del crimen o durante un allanamiento.

Las intervenciones urgentes en la escena del crimen reducen el margen de planificación y control del Ministerio Público Fiscal. Generalmente, la toma de contacto inicial con la evidencia que será recolectada es realizada por la policía de seguridad, que recibe la noticia del hecho criminal y debe proceder a ejecutar las medidas impostergables, con comunicación inmediata al Ministerio Fiscal (arts. 294, 296 y 297 del CPP; art. 11 de la ley 13.482). La inmediatez con que el funcionario policial se constituya en el lugar del hecho es trascendental; así como la toma de control efectiva del territorio y la delimitación y custodia del perímetro de la escena del presunto delito.

Esto abre una ventana de riesgo en cuanto a las cuestiones de preservación de la evidencia, que debe tratar de minimizarse con la capacitación de los efectivos policiales en cuestiones del manejo temprano de la escena del crimen; situación que es totalmente diferente en los casos en que se procede en allanamientos, donde el personal interviniente debiera ser idóneo para tal fin y estar en funciones específicas sabiendo lo que busca y cómo manejarlo.

Teniendo en cuenta estos riesgos, es altamente recomendable contar con una guía de actuación para personal policial interviniente en casos flagrantes y en diligencias urgentes. Un instrumento de este tipo permitiría no sólo instruir a los efectivos policiales sino también efectuar el debido control de la actuación de éstos, por parte del Ministerio Público Fiscal.

La reconstrucción del escenario de los hechos suele requerir correlacionar distintas clases de evidencia, cuyo análisis corresponde a variadas disciplinas. Debe recordarse asimismo que, en delitos cometidos a través de medios informáticos, la escena puede estar distribuida en diferentes sistemas, lugares y momentos. Ello puede involucrar a múltiples jurisdicciones y requerir una actuación coordinada.

E. LA IDENTIFICACIÓN DE EVIDENCIA

A la luz de los principios de relevancia y de suficiencia, la identificación de los artefactos y/o datos buscados está sujeta a diversos criterios de ponderación, que mutan a lo largo del tiempo.

Frecuentemente, el grado de avance de la investigación determinará el nivel de precisión de la búsqueda. En los momentos iniciales, parece prudente no dejar de lado ninguna evidencia con potencial valor investigativo y/o probatorio. En cambio, cuando la hipótesis del caso y el plan de investigación están afianzados, ya se debería prever la concreta utilidad que se espera obtener de las evidencias buscadas, lo cual permite acotar el material a recolectar o adquirir.

Igualmente, la identificación de la evidencia potencial debe pasar por distintas variables de análisis. Se ha de definir cuál es la clase de evidencias y/o datos relevantes. Se debe asimismo establecer dónde podría encontrarse la evidencia. Si la misma está replicada en más de una ubicación física, corresponde determinar cuál vía de acceso es la más conveniente, en función de los niveles de demora, riesgos de pérdida o modificación de datos, costos para las partes y/o terceros, grado de fiabilidad que ofrece el procedimiento de obtención en cada lugar, limitaciones legales, etc.

Existen además diversos factores que deben ser tenidos en cuenta en este test de relevancia: la gravedad del ca-

so, la premura en la obtención de la prueba, los niveles de demora esperables ante la eventual realización de una pericia, la posibilidad de obtener material probatorio alternativo respecto del punto que se intenta esclarecer o probar, la existencia de derechos de terceras personas vinculados con equipos y/o datos, etc.

En los casos que requieren el aporte informático forense, la prueba sobreabundante o superflua es realmente un obstáculo. La multiplicación de dispositivos, de la capacidad de almacenamiento de cada uno de ellos y de los vínculos en la red genera un crecimiento exponencial de información. Mientras tanto, los laboratorios periciales carecen de elasticidad en cuanto a dotación de personal especializado, capacidad de almacenamiento y herramientas de análisis. Por tal razón, los procesos de selección de evidencia deben ser actualizados en otras fases de la investigación y/o investigación, más allá de la fase de relevamiento e identificación previa a un procedimiento o acta de recepción de evidencia. Esta necesidad de selección o filtrado puede presentarse en el transcurso del mismo procedimiento judicial (ej.: allanamiento), al definir y/o redefinir los puntos de una pericia informática, al presentar la evidencia en el juicio oral, etc.

Cuando se prevea que en un procedimiento podrá ser menester adquirir datos volátiles, efectuar un procedimiento de triage y/o realizar la adquisición total o parcial de medios de almacenamiento persistentes, debe incluirse tal eventualidad en la solicitud de orden judicial. Iguales recaudos deben adoptarse cuando estima que podría ser necesario llevar a cabo injerencias en datos o contenidos abarcados por el derecho a la intimidad o al secreto de las comunicaciones.

F. CADENA DE CUSTODIA

En el proceso de cadena de custodia intervienen todos aquellos empleados y/o funcionarios que participen durante las diferentes etapas del proceso judicial. La cadena de custodia inicia desde la obtención de la evidencia y finaliza cuando se dispone judicialmente sobre la misma (restitución, destrucción, etc.).

Las exigencias vinculadas con la cadena de custodia alcanzan también al personal policial interviniente en un procedimiento urgente. Ello debería ser objeto de regulación mediante un instructivo general y un adecuado control de su observancia.

Al momento de revisar la integridad de la cadena de custodia, tanto formal como material, el equipo de investigación debe considerarla desde tres puntos de vista complementarios:

a) Validez técnico-informática, que implica el control, revisión y auditoría de todas las operaciones técnicas informáticas, realizadas desde la identificación de la evidencia digital recolectada hasta el análisis.

b) Validación técnico-criminalística, que es el control, revisión y auditoría de todas las operaciones técnicas criminalísticas, realizadas desde la toma de contacto, de los actores participantes en la tarea analizada, es decir desde que se involucran con la problemática pericial propuesta.

c) Validación técnico-legal, que es la resultante del análisis en subsidio, a partir de las dos validaciones anteriores. Se trata del análisis integrador de la prueba indiciaria informática recolectada y disponible, a efectos de determinar su confiabilidad probatoria legal.

Los procedimientos de cadena de custodia deben abarcar no sólo a los dispositivos, sino también a los datos contenidos en ellos. La exposición de los datos a pulsos electromagnéticos accidentales o a manipulaciones remotas requiere adoptar recaudos especiales.

Por otra parte, si hubiere copias forenses, éstas deben seguir el mismo curso que el original en cuanto a su conservación y preservación, siendo igual de relevante la realización de la cadena de custodia. El punto cobra mayor relevancia en los casos en que solamente se resguardarán copias forenses por imposibilidad material o técnica

de custodiar el original (resultados de análisis de triage, resultados de volcados de memoria, extracción de información de dispositivos que se restituyen antes de la realización del juicio oral y/o dictado de sentencia definitiva).

G. COORDINACIÓN DE EXPERTOS, INVESTIGADORES Y FISCALES

Los procesos de investigación y litigación son complejos, debido a la variedad de procedimientos de trabajo implicados, los aportes de disciplinas diversas y la pluralidad de funcionarios intervinientes. La cooperación, el conocimiento compartido y la articulación de las tareas en pos de las metas buscadas no se producen de forma espontánea, sino que deben ser objeto de especial atención.

Fiscales, investigadores y peritos deben compartir su conocimiento de los problemas técnicos, legales y estratégicos, y discutir los posibles escenarios y cursos de acción.

Esta comunicación es necesaria, respetando el rol de cada funcionario, en distintos momentos y bajo diferentes modalidades:

- ✓ Al delinear un plan de investigación acorde con la estrategia de intervención que haya fijado el Fiscal, especialmente en casos de cierta complejidad.
- ✓ En el proceso de identificación de la evidencia potencialmente relevante para cada punto del plan de investigación y/o para la labor de litigación. Se ponderarán factores tales como la gravedad del caso, los límites temporales y legales, los costos, el grado de complejidad técnica de las posibles diligencias, el nivel de confiabilidad esperado para cada elemento probatorio, las fuentes alternativas de prueba, etc.
- ✓ Durante la ejecución de procedimientos, cuando las circunstancias exigen adoptar decisiones no previstas.
- ✓ Al hacer el seguimiento periódico de las medidas investigativas y/o probatorias ordenadas, al evaluar sus resultados y, eventualmente, reajustar el plan de investigación.
- ✓ En el momento de decidir si es o no pertinente realizar una pericia informática y, en su caso, en la ocasión de definir los puntos de pericia. A tales fines, es importante tener en cuenta lo siguiente:
    - De acuerdo con las particularidades de cada caso, se podrá evaluar la conveniencia de convocar a las otras partes y/o de sus peritos para establecer los puntos periciales, consensuar la modalidad de realización de las tareas de los expertos, determinar el destino de los dispositivos originales, etc. En tal caso, se recomienda formalizar las decisiones en un acta labrada en legal forma.
    - Hay labores administrativas o técnicas que no son propias de la informática forense (transcripción de textos, cruzamiento de datos, tareas de impresión, escuchas o filmaciones, elaboración de backups, etc.).
    - La precisión de los puntos de pericia es clave para proceder de modo eficiente, ya que minimiza las confusiones, demoras y costos innecesarios.
    - No obstante esto último, se recomienda dejar un punto pericial abierto para que el perito pueda explayarse sobre cuestiones que estime relevantes para el objeto de la investigación y no hayan sido solicitadas por las partes.
- ✓ En el transcurso del examen pericial, cuando diversas circunstancias tornan atinado agilizar el aporte pericial (ej.: información muy voluminosa; necesidad de contar previamente con pruebas complementarias; pedido de un informe de avance o de un anticipo parcial o total de las conclusiones; hallazgo de evidencia

contundente que torna superabundante la continuación de la pericia; etc.).

- ✓ En la preparación del juicio oral, para familiarizar al perito con los puntos de controversia principales, orientarlo acerca del escenario previsible durante el interrogatorio, preparar la presentación de la evidencia ante el tribunal, conocer los puntos débiles de la evidencia material y/o del aporte pericial, y preparar el modo de declaración del perito en lo que hace al rigor técnico y a la claridad del lenguaje y/o del apoyo ilustrativo.

Específicamente en lo que hace a la labor pericial, el director de la investigación controlará que exista debida autorización judicial para el análisis de comunicaciones y archivos abarcados por la esfera de privacidad del sospechoso y/o de terceros.

También vigilará la observancia de las notificaciones de ley respecto de la realización de la pericia.

El Fiscal deberá tener nociones acerca de las técnicas y herramientas a utilizar durante la labor pericial. Tendrá presente que en genera se sugiere el uso de herramientas Open Source, es decir, de código abierto, dado que éstas permiten conocer y validar los resultados que brindan, así como realizar modificaciones en su funcionamiento de ser necesario. Las herramientas de código cerrado, por lo contrario, no cuentan con estas posibilidades, y ello puede ser explotado por la contraparte. Se efectúa una recomendación de herramientas en el Anexo "Técnicas y Herramientas de Informática Forense".

Es recomendable que el Fiscal, al momento de realizar el ofrecimiento de prueba para el juicio, ofrezca tanto el dictamen pericial ya efectuado como la declaración en el juicio del perito, con expresa mención de los objetos que fueron peritados, sean estos los originales o las copias forenses.

H. DESTINO DE LAS EVIDENCIAS

Las cuestiones vinculadas con el destino de las evidencias son importantes desde varios puntos de vista. Se encuentran en juego los derechos de los propietarios de los efectos (sean víctimas, acusados o terceros), la privacidad y el secreto de las comunicaciones de los titulares y/o usuarios de los datos, el debido proceso legal, la economía procesal, la gestión de la capacidad de almacenamiento de los equipos informáticos periciales, y la aplicación de sanciones punitivas respecto de los bienes del condenado.

Según nuestro CPP provincial, los objetos secuestrados que no estén sometidos a decomiso, restitución o embargo, serán devueltos, tan pronto como no sean necesarios, a la persona de cuyo poder se obtuvieron. La devolución puede ordenarse provisoriamente en calidad de depósito e imponerse al depositario la obligación de exhibirlos cada vez que le sea requerido. Los efectos sustraídos serán devueltos al damnificado, salvo que se oponga el poseedor de buena fe. Las cosas secuestradas de propiedad del condenado podrán ser retenidas en garantía de los gastos y costas del proceso y de las responsabilidades pecuniarias impuestas (arts. 83 inc. 7°, 231 y

523). Si después de un año de concluido el proceso, nadie reclama o acredita tener derecho a la restitución de cosas que no se secuestraron a determinada persona, se dispondrá su decomiso (art. 525).

Como pauta general, la evidencia sujeta a examen pericial debería ser conservada, de modo que la pericia pueda repetirse. Si fuere necesario destruir o alterar los objetos analizados o hubiere discrepancia sobre el modo de operar, los peritos deberán informar al Agente Fiscal antes de proceder (art. 248 del CPP). Ahora bien, conforme el art. 226 del CPP, se podrá ordenar la obtención de copias o reproducciones de las cosas secuestradas, cuando puedan desaparecer, alterarse, sean de difícil custodia o así convenga a la investigación. Esta normativa es relevante para la labor vinculada con la informática forense. Cuando los soportes de evidencia digital deben ser restituidos y no constituyen un elemento de prueba, pueden ser devueltos, siempre que se garantice que el proceso

de replicación de los datos a otro soporte permite comprobar su origen, autenticidad e integridad. En tal caso, el procedimiento de cadena de custodia continuará solamente con la imagen o copia.

En virtud de estipulaciones probatorias (art. 338 inc. 6° del CPP), las partes pueden formalizar su decisión de otorgar valor a impresiones, copias ordinarias en soporte digital, o a datos filtrados (restando relevancia al resto de los datos). También pueden decidir no cuestionar la evidencia sobre la cual se basó una pericia informática. Una vez autorizadas, por el juez dichas convenciones, podrá prescindirse de la evidencia original.

Las copias forenses no son efectos secuestrados. Sin embargo, la información allí contenida puede estar sujeta a las disposiciones de leyes nacionales que tutelan los datos personales, el secreto de las comunicaciones y la privacidad (ver art. 4° inc. 5 y 7 de la Ley 25.326 de Protección de Datos Personales, art. 18 de la Ley 19.798 de Telecomunicaciones, art. 5° de la Ley 27.078 de Tecnologías de la Información y las Comunicaciones). En función de ello, es conveniente que, cuando ya hayan cumplido su función procesal, se disponga su eliminación de los sistemas de almacenamiento del Laboratorio pericial. Si se hubieren entregado copias a peritos de parte, también deberán ser eliminadas o destruidas. Para ello es necesario haber registrado previamente la entrega de dichas copias forenses.

Según el art. 23 de nuestro Código Penal, cuando recayese condena por un delito, la misma decidirá el decomiso de los instrumentos del ilícito y de las cosas o ganancias que son el producto o el provecho del delito, en favor del Estado nacional, de las provincias o de los municipios, salvo los derechos de restitución o indemnización del damnificado y de terceros. El decomiso afecta a los bienes de los mandantes y/o personas de existencia ideal representadas por el autor o los partícipes del delito, y a los que se han beneficiado gratuitamente con el producto o provecho del delito. Si el bien decomisado tuviere valor de uso o cultural para algún establecimiento oficial o de bien público, la autoridad competente podrá disponer su entrega a esas entidades. Si así no fuere y tuviera valor comercial, aquélla dispondrá su enajenación.

Si no tuviera valor lícito alguno, se lo destruirá.

VIII. ANEXO V

GLOSARIO

El presente glosario surge como necesidad de establecer un diccionario forense, de uso común para los destinatarios de esta Guía Integral, cumpliendo de esta forma con el compromiso asumido entre los intervinientes a las Jornadas de Debate en Ciencias Forenses, llevadas a cabo entre los días 18 y 19 de junio de 2014 en la ciudad de La Plata y organizadas por la Universidad del Este.

En dichas jornadas se planteó promover una instancia de discusión tendiente a reflexionar, analizar y debatir sobre el rol de los distintos intervinientes en la investigación criminal en torno a la construcción de informes periciales basados sobre argumentos sustentados en estructuras lógicas y claras. Se postuló el empleo de un lenguaje claro, común, con sentido y legitimado por los especialistas en la materia, para que el significado o definición del vocablo pueda ser comprendido e interiorizado por aquellos que no son doctos en ese área, y poder aplicarlos en un debate oral o sintetizarlos en una sentencia penal.

Conceptos básicos

- ✓ Evidencia digital: información o datos, almacenado o transmitido en un medio informático, que puede ser utilizado como evidencia.
- ✓ Copia de la evidencia digital: copia de una evidencia digital que se realiza para mantener la confiabilidad de la evidencia. Incluye tanto la evidencia digital como los medios de verificación. El método de verificación puede estar incluido en las herramientas utilizadas para la creación de la copia o ser independiente.
- ✓ Adquisición: es el proceso de generar una copia de datos de un conjunto definido.
- ✓ Identificación: es el proceso de buscar, reconocer y documentar potencial evidencia digital.
- ✓ Preservación: es el proceso de mantener y resguardar la integridad y/o condición original de la potencial evidencia digital.
- ✓ Recolección: es el proceso de reunir/juntar objetos físicos pasibles de contener evidencia digital.

Conceptos técnicos

Los conceptos presentados en esta sección se basan en el Glosario de términos de la siguiente bibliografía:

- ✓ Sistemas Operativos, 2da Edición, William Stallings, PRENTICE HALL
- ✓ Sistemas Operativos Modernos, 3ra Edición, Andrew S. Tanenbaum, PEARSON
- ✓ Comunicaciones y Redes de Computadores, 7ma Edición, William Stallings,

Debido a que es una bibliografía muy técnica, en algunos casos las definiciones no son una cita textual de los libros tomados como referencia, sino interpretaciones y adaptaciones para simplificar el entendimiento del tema por el público objetivo de este documento. De ser necesario, pueden ampliarse las definiciones consultando las fuentes.

Almacenamiento:

- ✓ HPA - Host Protected Area: es una zona de un dispositivo de almacenamiento donde puede almacenarse información, pero que en condiciones normales no se expone ni siquiera al sistema operativo. Su utilización

permite ocultar información a los usuarios, usualmente para almacenar un programa de restauración del equipo.

- ✓ RAID: del inglés, Redundant Array of Independent Disks, es un conjunto de técnicas que permiten utilizar varios dispositivos de almacenamiento – usualmente discos de igual tamaño y rendimiento - como si fueran un sólo dispositivo. Esto permite mejoras en la integridad de los datos y velocidad de acceso.
- ✓ Montar: es el proceso de asociar un dispositivo con un directorio o unidad del sistema informático. Éste proceso es el que permite el acceso a los datos en un dispositivo, tanto para lectura como para escritura.
- ✓ Partición: es una porción lógica de un dispositivo de almacenamiento que tiene asociado un sistema de archivos.
- ✓ Tabla de Particiones: es una estructura que describe las particiones de un disco, su tamaño y su sistema de archivos asociado.
- ✓ MBR: es un formato de tabla de particiones que se utilizaba anteriormente. Hasta la década del 2010 aproximadamente.
- ✓ GPT: es un nuevo formato de tabla de particiones que tiene ventajas técnicas con respecto a MBR. Hasta que se adopte masivamente, ambos formatos conviven.

General:

- ✓ Estructura de datos: las estructuras de datos son formas de representar información en la memoria de una computadora. Diferentes estructuras de datos facilitan el trabajo con distintos tipos de información. Algunas estructuras características de determinados sistemas operativos o programas resultan útiles para el análisis forense.
- ✓ Log: un archivo que guarda un registro de información, acceso, funcionamiento y errores de un sistema.
- ✓ Máquina Virtual: es una emulación de otro equipo que se ejecuta sobre una computadora.
- ✓ Hipervisor: es un programa que administra los recursos de un equipo real para poder ejectuar una (o más) máquinas virtuales.
- ✓ Almacenamiento distribuido: un sistema de almacenamiento de información compuesto por varios equipos físicos (discos o servidores) que podrían encontrarse en distintos lugares físicos, incluso en ciudades, regiones o países diferentes.
- ✓ Imagen: una imagen es una copia exacta de un dispositivo de almacenamiento.
- ✓ Volcado de memoria / imagen de memoria: es una copia de los contenidos de la memoria volátil (usualmente llamada RAM) de un sistema informático.
- ✓ ZIP: Algoritmo de compresión de datos de uso extendido.
- ✓ RAR: Algoritmo de compresión de datos de amplio uso, competidor de ZIP.
- ✓ GZip: Algoritmo de compresión de datos, similar a ZIP, muy utilizado en ambientes UNIX.
- ✓ bzip2 / bz2: Algoritmo de compresión de datos utilizado en ambientes UNIX. Tiene mejor rendimiento que GZip, aunque no está tan extendido.
- ✓ Almacenamiento volátil: es la región de almacenamiento de una computadora que tiene comunicación directa con el procesador. Usualmente se llama “memoria RAM”, aunque en algunos sistemas de computación el término “almacenamiento volátil” es más abarcador y comprende otras partes adicionales de la computado-

ra.

- ✓ Hash: es una función matemática que permite representar datos de longitud variable como un dato de longitud fija y donde pequeñas diferencias en los datos de entrada generan una gran diferencia en los datos de salida. Los valores resultados también se denominan hash (singular) o hashes y permiten identificar con gran nivel de precisión los datos originales, sin revelar el contenido real de los mismos.
- ✓ MD5: es un tipo particular de hash que genera claves de 16 bytes de longitud (128 bits). Por la facilidad para calcularla y sus características matemáticas, se utiliza ampliamente para verificar la integridad de archivos.
- ✓ SHA-1: es un tipo particular de hash que genera claves de 20 bytes de longitud (160 bits). Computacionalmente lleva más tiempo calcular que MD5, pero posee propiedades matemáticas que la hacen una mejor alternativa para usos criptográficos. En el ámbito forense suele usarse en conjunto con MD5 para complementar la validación que provee el otro algoritmo.
- ✓ Tablas Rainbow: son tablas de fragmentos de hashes pre calculadas que permiten acelerar el cálculo de hashes. Usualmente se utilizan para realizar ataques informáticos y adivinar contraseñas.
- ✓ Filtros bloom: es otro tipo de estructura de datos que permite calcular hashes en forma acelerada. Un filtro bloom además tiene asociado un componente probabilístico. Su uso es similar al de una Tabla Rainbow.
- ✓ Encriptación: técnica que permite convertir texto o datos en una representación ininteligible mediante el uso de un código de forma que, posteriormente, se pueda hacer la reconversión a la forma original.
- ✓ TrueCrypt: software que implementa algoritmos de encriptación, para archivos y dispositivos de almacenamiento, de forma transparente para el usuario.
- ✓ BitLocker: software incorporado con Windows (a partir de Windows Vista) para realizar la encriptación de dispositivos de almacenamiento.
- ✓ TPM (BitLocker): es un criptoprocesador (un procesador especializado para almacenar claves criptográficas) específico para guardar claves de BitLocker.
- ✓ FVEK (BitLocker): es la clave que permite desencriptar información encriptada con BitLocker.
- ✓ Bootkit: es un programa que altera el proceso de inicio de una computadora.
- ✓ Metadatos: son “datos sobre los datos”, información asociada a un archivo, que permite interpretar y organizar mejor los datos en una computadora (ej.: establecer fechas de acceso, creación, modificación, etc.).
- ✓ EXIF: es un protocolo que permite incorporar información de metadatos a distintos formatos de archivo. Es muy utilizado en archivos JPG.
- ✓ ID3: es un protocolo que permite incorporar información de metadatos a formatos de archivo. Se utiliza ampliamente en archivos de música, por ejemplo MP3.
- ✓ XMP: es un protocolo que permite incorporar información de metadatos a formatos de archivo. Se utiliza para algunos formatos de archivos de documentos, por ejemplo PDF.
- ✓ Cadenas (de texto): es una representación de textos en la memoria de la computadora. Una cadena de texto es una secuencia de números que representa texto. Los números hacen referencia a caracteres (letras) en una tabla de caracteres, y distintas tablas ayudan en la representación visual de la información contenida por la cadena. Por lo general, en los países con alfabetos Latinos se utiliza ASCII, y desde hace algunos años se utiliza Unicode, que tiene mejor soporte para alfabetos complejos.
- ✓ ASCII: un formato de codificación de textos, ampliamente utilizado en países angloparlantes y países con al-

fabetos latinos.

- ✓ Unicode: un formato de codificación de textos que permite representar caracteres de cualquier idioma. Tiene distintas implementaciones, las más comunes son UTF- 8 y UTF-16.
- ✓ Expresiones regulares: una expresión regular es un texto que describe la forma de un texto.
- ✓ Carving / file carving: se llama con este nombre a una familia de técnicas de recuperación de archivos e información que se basan en la estructura de los datos que interesa recuperar.
- ✓ File signature / firma de archivo: es una secuencia de caracteres característicos de un archivo o formato de archivo.
- ✓ Header / Footer: firmas de archivo usualmente asociadas con el encabezado y final de archivo típicos de un formato de archivo.
- ✓ Malware: software cuyo propósito es perjudicar a un usuario o sistema, en forma directa o indirecta.
- ✓ Virus: un tipo particular de malware, usualmente los virus están asociados con comportamiento dañino hacia la computadora en la que se ejecutan.
- ✓ Botnet: un conjunto de computadoras manejadas, directa o indirectamente, por un servidor de comandos. Las botnets usualmente se utilizan para realizar ataques de denegación de servicio masivos.
- ✓ Librería: es una especie de programa que se carga en la memoria principal de la computadora para proveer funcionalidad común a otros programas.
- ✓ DLL: del inglés, Dynamic Link Library, es un formato especial de librería utilizado en sistemas operativos Windows.

Móviles:

- ✓ Tarjeta SIM: es una tarjeta que contiene un chip de datos que almacena información relacionada con números de identificación, números de registro, claves, etc. para acceder a un sistema de telefonía celular.
- ✓ JTAG: es una arquitectura que define una interfaz y protocolo para analizar y verificar el estado interno de chips electrónicos. En la informática forense, provee un medio para acceder a la información de un chip independientemente del resto del sistema informático.
- ✓ Almacenamiento en móviles: los requerimientos particulares de los dispositivos móviles ocasionan que utilicen hardware muy especializado. En particular, el almacenamiento de información en dispositivos móviles usualmente se realiza con chips de memoria Flash. Además, también es común que un dispositivo móvil tenga 2 o más medios de almacenamiento.
- ✓ Memoria interna (de dispositivo móvil): es un medio de almacenamiento interno al dispositivo móvil, no removible. Usualmente la memoria interna almacena las aplicaciones y datos de usuario, aunque en dispositivos que no cuentan con memoria externa también almacena los archivos del usuario.
- ✓ Memoria externa (de dispositivo móvil): es un medio de almacenamiento removible, usualmente una tarjeta micro SD. En la memoria externa suelen encontrarse los archivos del usuario, y algunas ocasiones también datos de aplicación. En teoría es posible, aunque con muy baja probabilidad, encontrar también una partición swap.
- ✓ Memoria Flash: es una tecnología de almacenamiento que, por sus características, fomenta la fragmentación de los datos, a un nivel inferior que el sistema de archivos.

Redes:

- ✓ Red local: red de comunicación que proporciona interconexión entre varios dispositivos de comunicación en un área pequeña.
- ✓ Cloud computing: conocido también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos, (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de Internet. En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet, siendo un paradigma en el que la información se almacena de manera permanente en servidores de Internet.
- ✓ Dirección de red: un número que identifica unívocamente a un dispositivo en una red. Las direcciones de red no pueden repetirse en una red bien configurada. Si dos equipos comparten la misma dirección de red, uno de ellos no podrá comunicarse y estará efectivamente desconectado de la red.
- ✓ Dirección IP: dirección de 4 bytes (32 bits) que representa a un equipo en una red IP (Internet Protocol). Las direcciones IP no representan unívocamente equipos porque hay mecanismos que permiten conectar múltiples equipos con una misma dirección IP, sin afectar la conectividad de los mismos.
- ✓ Dirección MAC: dirección de 6 bytes (48 bits) que identifica a un equipo en el medio físico de una red local tipo IEEE 802. Las direcciones MAC son unívocas y, en teoría, no se repiten en todo el mundo, aunque hay métodos para cambiarlas y generar direcciones MAC repetidas.
- ✓ Dump de red / volcado de red: es una copia del tráfico de una red en un segmento de tiempo, que permite analizar a posteriori las comunicaciones de uno o varios dispositivos.

Sistemas Operativos:

- ✓ Sistema Operativo: software que controla la ejecución de programas y ofrece servicios tales como la asignación de recursos, la planificación, el control de entrada/salida y la gestión de los datos.
- ✓ Filesystem / Sistema de archivos: es un conjunto de reglas, estructuras y protocolos que definen cómo se almacena, organiza y distribuye la información en una partición. Además los sistemas de archivos definen metadatos que permiten conocer fechas de acceso, modificación, permisos de usuario y otra información relevante a los archivos que se guardan.
- ✓ FAT (filesystem): un sistema de archivos simple creado por Microsoft para el sistema operativo DOS, luego extendido y adaptado a entornos más modernos. En la actualidad algunos pen drives vienen formateados con una variante moderna, llamada exFAT.
- ✓ File Allocation Table (tabla de archivos): es una tabla de asignación de espacio de la partición a los archivos. Indica que un determinado sector de la partición (denominado “cluster”) pertenece a un archivo. También establece la secuencia ordenada de clusters que permite recuperar los datos de un archivo.
- ✓ NTFS: es un sistema de archivos creado por Microsoft para los sistemas operativos Windows basados en Windows NT. Presenta una serie de ventajas y mejoras con respecto a FAT, y actualmente tiene un uso extendido.
- ✓ MFT: es la tabla de archivos de NTFS, pero sustancialmente distinta a la File Allocation Table de FAT. Debido a los cambios y mejoras introducidos, la MFT es una tabla mucho más importante y una mayor fuente de información que la FAT.

- ✓ ext: es una familia de sistemas de archivos asociados con el sistema operativo GNU/Linux. Las versiones más comunes son ext2, ex3 y ext4. Operativamente trabajan con el concepto informático de i-nodos, lo que ocasiona que tengan, en promedio, mayor fragmentación de los archivos que NTFS o FAT (pero sin la consecuencia negativa al rendimiento).
- ✓ Fragmentación: es una consecuencia de algunos sistemas de archivos en la cual un archivo, en lugar de almacenarse en sectores contiguos de la partición, se almacena separado en bloques. En las cuestiones de informática forense, la fragmentación es importante porque dificulta la recuperación física de archivos por medio de técnicas como el file carving.
- ✓ Driver: es un programa que se ocupa de comunicar comandos específicos a una parte del hardware de la computadora (por ejemplo la impresora) para que realice acciones específicas.
- ✓ Proceso: programa en ejecución, controlado y planificado por el Sistema Operativo.
- ✓ Memoria virtual: es un espacio de almacenamiento que el sistema operativo considera como memoria principal, que se encuentra limitado por la capacidad de almacenamiento de la memoria secundaria (usualmente el disco) del equipo.
- ✓ Área de paginado: es la parte de la memoria secundaria que se destina a funcionar como memoria virtual en los esquemas de paginación. Es importante desde el punto de vista forense porque ofrece una parte de la memoria principal para ser analizada como parte de la memoria secundaria.
- ✓ pagefile / archivo de página: es un archivo que contiene el área de paginado de los sistemas operativos Windows.
- ✓ Partición swap: es una partición que se utiliza como área de paginado. Los sistemas operativos UNIX, GNU/Linux y otros derivados de UNIX utilizan una partición swap en lugar de un archivo de página.
- ✓ Registro de Windows: es un conjunto de archivos que concentran configuraciones de bajo nivel de un sistema operativo Windows. Desde el punto de vista de la informática forense, es importante porque se almacena mucha información relacionada con el uso del sistema y los usuarios.
- ✓ Archivos de Configuración Linux: en los sistemas operativos UNIX y GNU/Linux, la configuración usualmente se almacena en archivos. Hay distintos sistemas de organización que dependen de la distribución y versión del sistema operativo.

IX. ANEXO VI

FUENTES

FUENTES BIBLIOGRÁFICAS

- Acuerdo A/002//10 (Cadena de custodia- México). Recuperado a partir de http://dof.gob.mx/nota_detalle.php?codigo=5130194&fecha=03/02/2010
- Acurio del Pino, S. (2007). Introducción a la informática forense. Recuperado a partir de http://www.alfa-redi.org/sites/default/files/articles/files/Acurio.pdf
- Acurio del Pino, S. (2010) Manual de manejo de evidencias digitales y entornos informáticos, versión 2.0. AR: Revista de derecho informático. Recuperado a partir de http://www.oas.org/juridico/english/cyb_pan_manual.pdf
- Adams, R. B. (2012) The advanced data acquisition model (ADAM): a process model for digital forensic practice. Recuperado a partir de http://researchrepository.murdoch.edu.au/14422/
- Amador, V. El examen directo del perito. Recuperado a partir de http://www.tecnicasdelitigacion.com/Perito%3A_Directo_y_Contra.php
- Andrés Ibáñez, P. (2009) Prueba y convicción judicial en el proceso penal. Buenos Aires, editorial Hammurabi.
- Asociación Internacional de Derecho Penal (2014) Resoluciones dictadas en el XIX Congreso Internacional de Derecho Penal "Sociedad de la Información y Derecho Penal" (Rio de Janeiro, Brasil, 31 agosto al 6 de septiembre de 2014). Recuperado a partir de
- http://www.penal.org/es/resoluciones
- Association of Chief Police Officers (2012) ACPO Good Practice Guide for Digital Evidence, Version 5. Recuperado a partir de http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_For_Digital_Evidence_v5.pdf
- Avella Franco, P. O. (2007) Programa Metodológico en el Sistema Penal Acusatorio. Fiscalía General de la Nación. Bogotá, Colombia. Recuperado a partir de http://www.fiscalia.gov.co/en/wp- content/uploads/2012/01/ProgramaMetodologicoenelSistemaPenalAcusatorio.pdf
- Baytelman A., A. & Duce J., M. (2004) Litigación Penal. Juicio Oral y Prueba. Universidad Diego Portales, Santiago de Chile.
- Bernazza, C. Material sobre planificación estratégica. Universidad de Quilmes. Recuperado a partir de http://municipios.unq.edu.ar
- Boixo, I. (2003) Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos. Madrid. Recuperado a partir de http://peritoit.files.wordpress.com/2012/03/guia-buenas-practicas-para-la-recuperacion-de-ficheros-e-imagenes.pdf

- Bonilla, J. E. (2009) Principios de computación forense. Power point. Recuperado a partir de http://www.slideshare.net/joseber/computacin-forense
- Cano, J. J. - Pimentel Calderón, J. (2007) Consideraciones Sobre el Estado del Arte del Peritaje Informático y los estándares de manipulación de pruebas electrónicas en el mundo. Universidad de los Andes, Facultad de Derecho. Revista de Derecho Comunicaciones y Nuevas Tecnologías N° 3.
- Carrier, B. (2013) Open source digital forensics tools. The legal Argument. Recuperado a partir de http://www.digital-evidence.org/papers/opensrc_legal.pdf
- Case, A., Cristina, A., Marziale, L., Richard, G. & Roussev, V. (2008) FACE: Automated digital evidence discovery and correlation. Digital investigation. Recuperado a partir de http://www.dfrws.org/2008/proceedings/p65-case.pdf
- Cistoldi, P. A. (2013). Del perfil del instructor judicial a la participación en sistemas de investigación. Curso de instructores judiciales, Mar del Plata.
- Committee on the Judiciary House of Representatives (2014) Federal Rules of Evidence. Recuperado a partir de http://www.uscourts.gov/uscourts/rules/rules-evidence.pdf
- Conclusiones Jornadas de Debate en Cs. Forenses. (2014) La Plata, Buenos Aires. Recuperado a partir de http://www.ude.edu.ar/newsletter/Conclusiones_Cien_For_Jun_2014.pdf
- Cortez Díaz, A. & Chang Lascano, C. M. (2012) Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos. Tesis previa a la obtención del título de Ingeniero en Sistemas. Universidad Politécnica Salesiana, Guayaquil, Ecuador. Recuperado a partir de http://dspace.ups.edu.ec/bitstream/123456789/2812/1/UPS-GT000312.pdf
- D´Alessio, A. J. (2007) Código Penal. Comentado y anotado. Parte General. Buenos Aires. La Ley.
- Da Rocha, J. - de Luca. J. A. (2014) Informática y Delito. Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP). Grupo argentino, Facultad de Derecho, UBA, marzo de 2014. Ed. Ministerio de Justicia y Derechos Humanos de la Nación.
- Darahuge, M. E., & Arellano González, L. E. (2012) Manual de Informática Forense II. Buenos Aires. Editorial Errepar.
- De Bono, E. (1992) Seis pares de zapatos para la acción: Una solución para cada problema y un enfoque para cada solución. Paidós, Barcelona.
- Delgado Martín, J. (2013a). Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. Diario La Ley, (8202), 32.
- Delgado Martín, J. (2013b). La prueba electrónica en el proceso penal. Diario La Ley. XXXIV (8167), 1-29.
- Di Iorio, A., Sansevero, R., Castellote, M., Greco, F., Constanzo, B., Waimann, J. & Podestá, A. (2013) Determinación de aspectos carentes en un Proceso Unificado de Recuperacion de Informacion digital. (pp. 1-13). Presentado en 5to Workshop de seguridad informática. WSegI2013, Córdoba. Recuperado a partir de http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/430.
- Di Iorio, A. , Curti, H., Greco, F., Podestá, A., Castellote, M., Iturriaga, J., Trigo, S., Constanzo, B., Ruiz de Angeli, G., Lamperti, S. (2015) Construyendo una Guía Integral de Informática Forense. Congreso Nacional de Inge-

niería Informática / Sistemas de Información.

- Di Iorio, A., Mollo, R., Cistoldi, P., Lamperti, S., Giaccaglia, M.F., Malaret, P., Vega, P., Iturriaga, J., Constanzo, B. (2016) Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI) 2016, Santa Fe, Universidad Nacional del Litoral (inédito).
- Díaz Gómez, A. (2010) El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest. Especial consideración a España y Argentina. Recuperado a partir de http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf
- D´Onofrio, J. A. (2013) Creando el protocolo de procedimientos <cadena de custodia> y el anexo planilla de cadena de custodia. Recuperado a partir de http://www.senado-ba.gov.ar/secleg_busqueda_acypro_detalle.aspx?expe=93252
- Duce J., M. (2005) La prueba pericial y su admisibilidad a juicio oral en el nuevo proceso penal. Revista Procesal Penal nº 35, Lexis Nexis, Santiago de Chile.
- Dykstra, J. - Sherman, A (2012) Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Cyber Defense Lab, Department of CSEE, University of Maryland. Recuperado a partir de http://www.dfrws.org/2012/proceedings/DFRWS2012-10.pdf
- Fiscalía General de la República – Policía Nacional Civil de la República de El Salvador. (2009) Plan estratégico de investigación. Desarrollado con el apoyo de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Programa de Asistencia Legal para América Latina y el Caribe (LAPLAC), y de la Embajada Británica. Recuperado a partir de https://www.unodc.org/documents/colombia/2013/diciembre/PLAN_ESTRATEGICO_DE_INVESTIGACION_EL_Salvador.pdf
- Fiscalía General de la República de El Salvador. Manual Único de Investigación Interinstitucional. Recuperado a partir de http://escuela.fgr.gob.sv/wp-content/uploads/2012/03/MUI-Final.pdf
- Fondebrider, L & Mendonca, M. C. (2010) Protocolo modelo para la investigación forense de muertes sospechosas de haberse producido por violación de los derechos humanos. Recuperado a partir de http://www.pgjdf.gob.mx/temas/4-6-1/fuentes/11-A-8.pdf
- García, J. A. (2013) La cadena de custodia aplicada a la informática I. Recuperado a partir de http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i/
- Gómez, L. S. (2012, agosto 27). Protocolo de actuación para pericias informáticas. Acuerdo N° 4908. Poder Judicial de la Provincia de Neuquén.
- Gómez, L. S. (2008) Buenas Prácticas para el secuestro de evidencia digital. Power point. Recuperado a partir de http://es.slideshare.net/cxocommunity/buenas-prcticas-para-el-secuestro-de-evidencia-digital-sebastian-gomez
- Gómez, L. S. (2013) Pericias informáticas sobre telefonía celular. Recuperado a partir de http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf

- Granillo Fernández, H. M. & Herbel, G. A. (2009) Código de Procedimiento Penal de la Provincia de Buenos Aires. Buenos Aires. La Ley.
- Gudín Rodriguez - Magariños, A. E. (2014) Incorporación al proceso del material informático intervenido durante la investigación penal. Recuperado a partir de https://drive.google.com/drive/#folders/0B9HBExMI05SQd3Z6TWU0LWJDazg/0B9HBExMI05SQSjQxYzNfamgxSU0
- Gudín Rodríguez-Magariños, A. E. (2010) La búsqueda y conservación de los datos informáticos en el Derecho norteamericano E-discovery. Estudios de Deusto: revista de la Universidad de Deusto, Vol. 58, Nº. 2.
- Guzmán, C. A. (2010): Examen en el escenario del crimen: Método para la reconstrucción del pasado. B de F, Buenos Aires.
- Interpol (2008) Informe Forense de Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia. Recuperado a partir de http://www.interpol.int/es/Media/Files/News-Media-releases/2008/PR017ipPublicAbstract
- Leenes, R. (2010) ¿Quién controla la nube?. Universitat Oberta de Catalunya, Revista de Internet, Derecho y Política (IDP) N° 11. Recuperado a partir de http://journals.uoc.edu/index.php/idp/article/view/n11-leenes/n11-leenes-esp
- Lorenzo, L. (2012) Manual de litigación. Buenos Aires, Ed. Didot.
- Luzuriaga, J. M. (2004) Examen de evidencias en pericias informáticas judiciales. En X Congreso Argentino de Ciencias de la Computación. Recuperado a partir de: http://sedici.unlp.edu.ar/handle/10915/22317
- Marafioti, L. (2012) Prueba digital y proceso penal. Revista de Derecho Penal y Procesal Penal (dir.: Pedro J. Bertolino – Patricia Ziffer). Buenos Aires, Abeledo Perrot.
- Martell, R., Quates, C. & Roussev, V. (2013) Real-time digital forensics and triage. Digital investigation. Recuperado a partir de http://roussev.net/pubs/2013-DIIN—real-time--in-press.pdf
- Martinez Retenaga, A. (2014) Guía de toma de evidencias en entorno de windows. Recuperado a partir de
- https://drive.google.com/drive/#folders/0B9HBExMI05SQd3Z6TWU0LWJDazg/0B9HBExMI05S QSjQxYzNfamgxSU0
- Mauri, M. C. & Rossi, I. C.(2012) Análisis de la regulación de la prueba pericial durante la investigación penal preparatoria en tres Provincias argentinas que consagraron normativamente el sistema acusatorio. Problemas y desafíos. Revista de Derecho Procesal Penal (dir.: Edgardo Alberto Donna). Santa Fe, Rubinzal - Culzoni.
- Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires, Equipo Especializado en Delitos Informáticos (2013) Informe Final Cybercrime. Recuperado a partir de http://delitosinformaticos.fiscalias.gob.ar/wp-content/uploads/2014/02/CyberCrime-Informe- Final-2013-flip.pdf
- Ministerio Público de Paraguay - Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC): Manual del PEC. Recuperado a partir de http://www.ministeriopublico.gov.py/sitios/centro/publicaciones/pdf/pec/plan_estrategico.pdf

- Molina Quiroga, E. (2010) Prueba de una publicación en internet. Comentario al fallo de la Cámara Nacional de Apelaciones en lo Comercial, sala E, en "Frega, Enrique c/ Imbelloni, Marco Emilio s/ ordinario", 06-12-2010, elDial AA697B.
- Molina Quiroga, E. (2013) La prueba en medios digitales. Recuperado a partir de https://www.eldial.com/nuevo/lite-tcd-detalle.asp?id=5550&base=50&id_publicar=&fecha_publicar=13/04/2011&indice=comentarios&suple=DAT
- Molina Quiroga, E. (2014) Evidencia digital y prueba informática. Buenos Aires, editorial La Ley.
- National Institute of Justice, U.S. Department of Justice (2004) Forensic examination of digital evidence: a guide for law enforcement. Recuperado a partir de https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- National Institute of Justice, U.S. Department of Justice (2007) Investigations Involving the Internet and Computer Networks. Recuperado a partir de https://www.ncjrs.gov/pdffiles1/nij/210798.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce (2014) NIST Cloud Computing Forensic Science Challenges. Recuperado a partir de http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf
- Núñez Mori, O., Ramírez García, A. & Salas Ordinola, E. Propuesta de protocolo para la recolección de evidencias digitales relacionado con la legislación peruana. Recuperado a partir de https://drive.google.com/drive/#folders/0B9HBExMI05SQd3Z6TWU0LWJDazg/0B9HBExMI05S__QSjQxYzNfa-mgxSU0
- Oficina de las Naciones Unidas contra la Droga y el Delito (2009). La escena del delito y las pruebas materiales. Sensibilización del personal no forense sobre su importancia. Recuperado a partir de http://www.unodc.org/documents/scientific/Crime_scene_Ebook.Sp.pdf
- Oficina de las Naciones Unidas contra la Droga y el Delito en Colombia (UNODC). Programa de Asistencia Legal para América Latina y el Caribe (LAPLAC) (2008) Planeación de la investigación y programa metodológico. Bogotá, Colombia. Recuperado a partir de https://www.unodc.org/documents/colombia/2013/diciembre/Planeacion_de_la_InvestigacionColombia.pdf
- Orellana de Castro, J. F. (2011) Estrategias del perito en el acto del juicio oral (Institucional). Diario La Ley, Nº 7730, sección práctica forense, 7 de noviembre de 2011, Año XXXII, Editorial La Ley 17370/2011.
- Pérez Gil, J. (2005) Investigación penal y nuevas tecnologías: algunos de los retos pendientes. Revista Jurídica de Castilla y León. N.º 7. Recuperado a partir de http://www.jcyl.es/web/jcyl/binarios/690/55/RJ7-10-J.Perez.pdf?blobheader=application/pdf;charset=UTF-8
- Piccirilli, D. (2013). La forensia como herramienta en la pericia informática. Revista Latinoamericana de Ingeniería de Software, I(6):237-240.
- Presman, G. D. (2011) Investigación forense en redes sociales. Presentado en el XV Congreso Iberoamericano de Derecho e Informática, Buenos Aires. Recuperado a partir de http://carris.files.wordpress.com/2011/12/investigacion-forense-en-redes-sociales.pdf
- Presman, G. D. (2014) ISO/IEC 27037. Normalizando la práctica forense informática. Power point. Recuperado

a partir de
http://www.copitec.org.ar/comunicados/CAIF2014/CAIF-Presman.pdf

- Protocolo Federal de Preservación. Recuperado a partir de http://www.jus.gob.ar/media/183597/Protocolo%20Federal%20de%20Preservacion.pdf
- Righi, E. (2008) Derecho Penal. Parte General. Buenos Aires: Lexis Nexis.
- Salas Ordinola, E., Ramírez García, A. & Núñez Mori, O. (2011) Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana. Pontificia Universidad Católica del Perú. Publicado en alfa-redi, portal de Derecho y Nuevas Tecnologías. Recuperado a partir de http://www.alfa-redi.org/sites/default/files/articles/files/salas.pdf
- Scientific Working Group on Digital Evidence. Recuperado a partir de http://www.oas.org/juridico/spanish/cyb_best_pract.pdf
- Sindicatura General de la Nación de la Presidencia de la Nación. Instituto Superior de Control de la Gestión Pública. Paper "Evidencias digitales. Clase especial". Presentado en el Congreso Argentino de Informática Forense 2014, organizado por COPITEC, los días 4, 5 y 6 de junio de 2014.
- Taruffo, M. (2009) La Prueba. Artículos y Conferencias. Santiago de Chile, Ed. Metropolitana. Tortosa López, F. J. El informe pericial. Recuperado a partir de http://www.antud.org/El%20informe%20pericial.pdf
- Unión Internacional de Telecomunicaciones (2009) El ciberdelito: guía para los países en desarrollo. Recuperado a partir de http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
- Vaninetti, H. A. (2013) Preservación y valoración de la prueba informática e identificación de IP. Fallo Comentado: Cámara Nacional de Casación Penal, sala IV ~ 2013-03-22 ~ Gil, Juan José Luis s/rec. de casación. La Ley, 2013-C, 374.

FUENTES NORMATIVAS EXTRANJERAS Y LOCALES (NACIONALES Y PROVINCIALES)

- Convención de Cibercriminalidad (Budapest, 2001)
- Constitución de la Nación Argentina.
- Código Penal Argentino.
- Código Procesal Penal de la Provincia de Buenos Aires.
- Ley 14.442 del Ministerio Público Fiscal de la Provincia de Buenos Aires.
- Ley 13.634 (art. 55), Régimen Penal Juvenil.
- Ley 14.424 de creación del Cuerpo de Investigadores Judiciales de la Provincia de Buenos Aires.
- Ley 13.433 de Mediación Penal de la Provincia de Buenos Aires.
- Ley 13.016. Régimen del ejercicio de profesiones en Ciencias Informáticas de la Provincia de Buenos Aires.
- Ley 19.798 (y modificatorias). Régimen Nacional de las Telecomunicaciones.
- Ley 25.326. Régimen de Datos Personales. Habeas Data.
- Ley 25.506. Firma digital.

- Ley 25.690. Obligación de los ISP de ofrecer software de protección en el acceso a contenidos de sitios específicos.
- Ley 25.873. Responsabilidad de los prestadores del servicio de telecomunicaciones para su observación remota por parte del Poder Judicial o del Ministerio Público *(declarada inconstitucional, ver CSJN, c. "Halabi", 24-02-2009; Fallos: 332:111)*.
- Ley 25.891. Servicios de Comunicaciones Móviles.
- Ley 26.032. Búsqueda, recepción y difusión de ideas por Internet.
- Ley 26.522. Ley de Servicios de Comunicación Audiovisual.
- Ley 27.078. Argentina Digital. Tecnologías de la Información y las Comunicaciones.
- Resolución PGN Nº 756/16. Guía de obtención, preservación y tratamiento de evidencia digital.
- Resolución PG SCBA Nº 889/15. Protocolo de Cadena de Custodia.
- Resolución Conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos de la Nación.