UNIVERSIDAD NACIONAL
DE LA PLATA

POSTGRADO
FACULTAD DE INFORMÁTICA

Universidad Nacional de La Plata
Facultad de Informática

TESIS Doctoral en Ciencias Informáticas

"PROTOCOLOS A APLICAR EN LA FORENSIA INFORMÁTICA EN EL MARCO DE LAS NUEVAS TECNOLOGÍAS (PERICIA – FORENSIA y CIBERCRIMEN)"

Tesista: Mg.Lic. Darío A. Piccirilli

Directores: Lic. Javier Díaz - Dr. Luis Javier Villalba

La Plata – Prov. Buenos Aires, 2015

Dedicatoria

A mis esposa Mónica, única compañera en todo momento y por su apoyo permanente en todo el proceso de la tesis y en la vida

A mis hijas María Pía y María Eugenia, por su comprensión y ayuda permanente

A Javier Díaz, por guiarme con sus sabios consejos

A Luis Javier Villalba, por sus sugerencias y permanente apoyo

A Luis Marrone, por orientarme en momentos difíciles

A mis amigos por acompañarme y alentarme

Al Dr. Alejandro Catania, por sus consejos profesionales, orientadores en todo momento

A Ramón García Martínez, por sus consejos y sugerencias

A la memoria de David Airala, gran amigo y compañero en los temas de forensia e investigación informática.

Agradecimientos

A mi país, por la posibilidad de conocer, compartir y trabajar en la temática pericial

A la Justicia de mi país, que a través de los jueces, fiscales, secretarios de juzgado y colaboradores, me han permitido conocer los aspectos periciales asociados

A mis seres queridos por el apoyo y empuje en los momentos difíciles.

A los abogados amigos, que contribuyeron con el aporte de sus puntos de vista

A la Facultad de Informática de la Universidad Nacional de la Plata por permitirme acceso a un mayor conocimiento en mis estudios del doctorado, a través de los cursos, pudiendo compartir conocimientos con los docentes, y también, por permitirme dar cursos específicos de mis conocimientos, logrando compartir experiencias con los alumnos

Al personal de la secretaría de posgrado de la Facultad de Informática de la Universidad Nacional de la Plata por la permanente y sumamente útil asistencia

A las fuerzas de Seguridad como la Policía Federal Argentina, Gendarmería Nacional Argentina, Policía Metropolitana, Policía Judicial de C:A.B.A., policía Judicial de la Provincia de Buenos Aires e INTERPOL, por el constante apoyo y permitirme compartir experiencias profesionales

A mis directores de Tesis Javier Díaz y Javier Villalba, por dirigirme, orientarme y ayudarme en la realización de este trabajo.

RESUMEN

Esta Tesis intenta realizar una serie de aportes sobre la Forensia en Informática, contemplando las nuevas tecnologías que hoy día aplican en los procesos judiciales y que derivan en Pericias muy específicas y complicadas, tareas técnicas sobre las que no se puede generar ninguna duda en el tratamiento de la prueba. Es decir, el proceso de generación de la prueba, desde el secuestro de la misma hasta el análisis pericial, debe ser indubitable, de manera tal que quien deba impartir justicia pueda contar con elementos claros, contundentes y útiles. La informática puede considerarse que se encuentra relacionada en forma transversal con gran parte de la problemática judicial, aplicando en los distintos fueros de la Justicia Argentina, tanto en lo Laboral, Comercial, Civil, Contencioso Administrativo Federal, Penal Económico, Criminal y también para la Corte Suprema.

ABSTRACT

The process of generation of proof can consist of many stages, depending on the situation in which the computer expert can intervene. In other words, it is fundamental to understand the situation in which proof can or must be collected. During a search and seizure (the moment in which equipment is seized or information is “collected”, avoiding the seizure of critical equipment for the organization searched), information that has already been seized may have to be analysed, or it may have to be obtained on the basis of data seized from optical or magnetic storage media. These processes must follow best practices, applying work protocols accepted worldwide and employing trustworthy tools. Information obtained as digital evidence for the trial must be indubitable, so that the Court that must impart justice can count on elements that are clear, forceful and useful. Although this applies to Criminal law in Argentina, it is important to comprehend these practices and procedures in order to extrapolate the collection of digital evidence to other aspects of the Law, where, although there may be no procedure such as search and seize, a previous process, understood as a “pre proof” of digital evidence, may occur. This procedure may apply to Labour, Commercial and Civil law.

“Technology is a gift of God. After the gift of life it is perhaps the greatest of God´s gifts. It is the mother of civilizations, of arts and of sciences.”

Freeman Dyson (1961 – Proyecto Orion)

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

Bruce Schneier (2004)

"En 2031, los abogados serán componentes habituales de la mayoría de los equipos de desarrollo"

Grady Booch (6 de Abril de 2008)

"La imaginación es más importante que el conocimiento. El conocimiento es limitado, mientras que la imaginación no"

Albert Einstein

INDICE

CAPITULO 1. INTRODUCCIÓN

1.1. OBJETIVOS

1.1.1. OBJETIVO GENERAL

La presente tesis doctoral tiene como objetivo desarrollar una propuesta metodológica para definir protocolos de base a utilizar en el uso de la forensia aplicada al tratamiento de la evidencia digital, en el marco de las nuevas tecnologías informáticas.

Actualmente en Argentina en particular, y en el mundo en general, el concepto y la utilidad de la informática forense va adquiriendo una gran importancia dentro del área judicial. ***[ANTE 01] 2008 - OIPC-INTERPOL - 200 Quai Charles de Gaulle -69006 Lyon - (Francia)***

Ello se debe a que la informática es una disciplina transversal, y aplica en casi todos los órdenes en nuestras vidas. Ejemplo de ello lo tenemos en el ámbito **del trabajo** (para probar relaciones laborales, maltratos, entre otros aspectos), en el **comercial** (para las transacciones entre partes), en el ámbito **civil** (conversaciones a través de las redes sociales, operaciones bancarias), en el ámbito **penal** (para probar estafas, amenazas, problemas de propiedad intelectual), entre otros aspectos.

No es ajeno a nuestro conocimiento que la delincuencia ha encontrado en la cibernética una herramienta muy útil para la comisión de distintos tipos de delitos, pero también la justicia reconoce la utilidad de las pruebas digitales que pueden ser obtenidas a través de las herramientas informáticas. Por ello, una conversación virtual entre personas a través de las redes sociales, o un archivo de texto, o una imagen un una planilla de datos, o un correo electrónico, se han convertido en el objetivo de análisis para constituir una verdadera “prueba”. [**ANTE 02**] ***Fiscal Federal Argentina – Dr. Ricardo Sáenz T- ercer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática – M. del Plata - Mayo de 2014.***

A medida que avanza la tecnología, la informática evoluciona cada vez más rápido. Por ende, en un principio teníamos las computadoras, hoy tenemos teléfonos celulares, smartphones, smart TVs, tablets, GPS, máquinas fotográficas, tarjetas de crédito con chips, terminales de vigilancia, entre otras tecnologías.

Debemos considerar además los problemas derivados de depositar los datos en la nube. Lo que constituye un tema aparte y que conforma nuevas líneas de trabajo e investigación, que pueden ser tratadas como continuación de esta tesis, y en otra oportunidad.

Sobre la base de lo expuesto, es posible afirmar que la Justicia encuentra hoy día una base muy importante para la resolución de conflictos, teniendo en la informática forense una base decisiva en muchos casos para resolver etapas periciales y poder así fundamentar un fallo. Por ello, y para que realmente este proceso sea efectivo, deben aplicarse procedimientos estrictos y rigurosos, que deben respetar lo que se conoce hoy día como las mejores prácticas, aplicadas a la recolección, análisis y validación de todo tipo de pruebas digitales. El protocolo que se propone en esta tesis, se constituye en el aporte para poder solucionar la actual problemática sobre la validez de la evidencia digital en un fallo judicial.

1.1.2. OBJETIVOS ESPECÍFICOS

Teniendo en cuenta lo expresado en el punto anterior (Objetivos), es posible afirmar que hoy día la informática se ha convertido en una herramienta o vehículo para la comisión de un delito, y también esta ciencia es objeto de delitos.

Dicho de otra manera, hoy es posible aplicar la informática para realizar una estafa, enviar una amenaza (intentando quedar en el anonimato), para obtener claves secretas de cuentas bancarias y así conseguir ilegalmente fondos dinerarios de otras personas, para realizar robo de datos de una empresa con distintos fines, acceso indebido a la información de la cía., daños en las páginas WEB, violación de la confidencialidad y secretos de la cía., entre otros.

A esto debemos sumarle casos vinculados con delitos sociales como la pedofilia, grooming, o delitos federales como el Lavado de Activos, lucha contra el narcotráfico y otros delitos financieros.

Debemos considerar además la evolución del delito hacia el Cibercrimen y Ciberdelitos, apoyados en la ingeniería social y en las debilidades existentes en la seguridad informática de las empresas. Es de señalar que existen diversas actividades llevadas a cabo por los delincuentes, que son muy ingeniosas, y que tienden a ¨globalizarse¨, como por ejemplo la compra y venta de datos bancarios de ciudadanos de todo el mundo, con fines delictivos **[CIBER03]**

Lo expuesto genera la situación que cuando se tenga que realizar una pericia informática, se deban considerar distintos aspectos que involucran protocolos específicos según la etapa a encarar, los que integran **objetivos específicos** a saber:

- Evaluar el ambiente en el que se debe recolectar la evidencia digital
- Entender el objeto de la evidencia digital a obtener (considerar los puntos de pericia ordenados por el juez)
- Evaluar y seleccionar las herramientas a aplicar en el adecuado tratamiento de la prueba digital, para satisfacer el objetivo de la investigación
- Evaluar y seleccionar los recursos humanos adecuados a aplicar en el tratamiento de la evidencia digital

1.2. ALCANCE

Como alcance del presente trabajo, se establece que el protocolo a considerar en el desarrollo de la tesis, debe comprender desde el momento en que se ordena la obtención de una evidencia digital hasta la evaluación por parte del perito, para responder el cuestionario pericial ordenado por el juez.

Comprende además, la preservación de la prueba en todo momento, inclusive luego de la realización de la pericia, por una eventual repetición de la misma.

NO comprende las etapas posteriores al cierre de la investigación basada en la evidencia digital y la presentación del informe técnico pericial. Es decir, no integra parte de la presente tesis, la devolución o destrucción de la prueba involucrada en la investigación

1.3. FUNDAMENTOS DEL TRABAJO

Actualmente existen estándares y modelos de protocolos **([PROPER] [GUID001] [COFO001] [Casey04])**, que contienen actividades de Forensia a aplicar en etapas de obtención de evidencias, como el secuestro de drogas, de armamentos o de crímenes, tratamiento básico del Cibercrimen. Pero lo expuesto no alcanza a la obtención y preservación de la evidencia digital.

La adquisición y tratamiento de la evidencia digital (ED) son actividades estratégicamente importantes y decisorias, al momento de generar pruebas informáticas que permitirán dirimir situaciones dudosas y los respectivos autores o culpables.

Existen dificultades y fallas que normalmente se presentan el momento de encarar la obtención de la evidencia en cuestión. Para evitar estos inconvenientes, existen diversas técnicas de adquisición y preservación de la ED, siendo de gran importancia organizarlas en una metodología o marco para su correcto entendimiento, verificación y aplicación. **([PROPER]** Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana - Evelyn Salas Ordinola, Alan Ramírez García y Oscar Núñez Mori – Lima Perú – 15/04/2011) - **[FALLO1]** LA Cámara Federal Confirmó anulación de Peritaje sobre mails - Causa Nro. 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial" - Jdo. Fed. n° 7 - Sec. n° 14 Buenos Aires, 24 de mayo de 2012 (con intervención del Perito informático Darío A. Piccirilli) - **[PUB001]** La Forensia como Herramienta en la Pericia Informática - Mg. Darío A. Piccirilli - Perito en Informática - Capital Federal, Argentina - relais-v1-n6-237-240 - **[PUB002]** Consideraciones legales relativas a la privacidad en proyectos de Cloud Computing en el exterior del país – Mg. Darío Piccirilli – Ing. Juan Cruz González Allonca - relais-v2-n1-77-90)

Es muy importante considerar un marco teórico en los proyectos de investigación, ya que facilita y ordena la gestión, y constituye una herramienta para facilitar el proceso de conceptualización, entendimiento y aplicación, centrado en la orientación por objetivos, en la orientación hacia grupos beneficiarios (en nuestro caso, la Justicia Argentina), y el facilitar la participación y comunicación entre las partes interesadas (los jueces, los peritos y los abogados de las partes intervinientes en el pleito).

El Marco Teórico, es valioso para el diseño de un protocolo adecuado, que permita el tratamiento y presentación de la ED, a los efectos que se pueda cumplir con el objetivo de obtener una prueba válida y útil en un juicio

Como proceso de consolidación y desarrollo del protocolo planteado, se siguen los siguientes pasos lógicos como parte de la metodología:

La revisión bibliográfica aplicada, incluye artículos de publicaciones especializadas, de trabajos presentados en congresos e investigaciones llevadas a cabo por organismos internacionales, además de sitios web de autores, organizaciones e institutos de investigación vinculados con la temática.

Con base en el estudio de lo recopilado en el marco teórico, se consolida la fuente para el informe final del estado del arte de la problemática elegida.

1.4. ENFOQUE – METODOLOGIA EMPLEADA

La metodología aplicada para el desarrollo del trabajo de investigación se inicia con el estudio y análisis de la problemática pericial informática, las herramientas existentes en el mercado y las habilidades de los profesionales que intervienen en la solución de estos conflictos, en los que la evidencia digital cumple un rol fundamental.

Es de señalar expresamente que todo lo expuesto se desarrolla dentro de un marco “no formalizado” hasta el momento. Es decir, las actividades se llevan a cabo sobre la base de la experiencia del profesional que interviene, pero no sobre la base de un protocolo específico que permita realizar una tarea pericial eficiente, sin “huecos” o falencias de procedimiento, algo que permitiría obtener efectividad tecnológica necesaria para clarificar los delitos informáticos, con

resultados claros y concretos. Pues, esto puede traer aparejado distintos resultados frente a un mismo evento. Ello conforme a la experiencia y conocimiento del perito que interviene en el desarrollo de la tarea.

Por todo lo expuesto, se intenta aportar a través de esta tesis, una base de protocolo para mejorar las prácticas periciales en informática que hoy en día se vienen aplicando de manera no formalizada, presentando algunas falencias muy difícil de hacer valer en forma indubitable la prueba informática como evidencia digital.

Para el logro del objetivo propuesto, se plantean las siguientes seis (6) etapas, las que se describen en detalle en el Capítulo III.

A modo de resumen, se especifican las mismas:

La primera, se basa en el estudio y análisis del entorno, para identificar la evidencia digital a obtener

La segunda etapa se basa en el análisis de los puntos de pericia, que establecen el objetivo que debe cumplir la evidencia digital a obtener

La tercera etapa se basa en la adquisición de la evidencia digital

La cuarta etapa se basa en el análisis de la evidencia obtenida, conforme los lineamientos del cuestionario pericial ordenado.

La quinta etapa se basa en la forma de exponer la evidencia digital obtenida en la investigación realizada

La sexta etapa se basa en preservación de la evidencia digital tratada (para eventuales futuras etapas de investigación, cuya fuente sería la misma evidencia digital).

Una vez culminado lo anterior, se consolida y realiza el informe final de la presente tesis.

1.5. ESTRUCTURA DEL TRABAJO

El trabajo se estructura en cinco capítulos, sobre los que se brinda un pequeño detalle para cada uno:

Capítulo 1. Introducción. Contiene los objetivos generales y específicos del trabajo de tesis, el alcance, los fundamentos del trabajo, la metodología empleada, especificación y la estructura del trabajo.

Capítulo 2. Estado del arte. Describe en forma general las situaciones que ocurren hoy día en el tratamiento de la prueba informática, la generación de la evidencia digital, su tratamiento pericial y la posterior valoración por parte de las autoridades encargadas de impartir justicia. Incluye además los resguardos a considerar ante los ataques del cibercrimen, basados en la ingeniería social.

Es de señalar que hoy día, las fuentes utilizadas con éxito para realizara esta ingeniería social son:

- Por correo electrónico (47 %)
- Por sitios en redes sociales (39 %)
- Por dispositivos móviles (12 %)
- Otros (resto)

  Fuente: http://hackstory.net/Ingenieria_social

Capítulo 3. Desarrollo de la solución, basada en las seis (6) etapas señaladas en el punto 1.4. Estas etapas permitirán establecer una base y punto de partida para poder contar con un protocolo general, pudiendo aplicarse en todos los casos periciales, en los que intervengan elementos vinculados a la informática y a la telefonía celular, incursionada además en casos vinculados con el CyberCrimen y los Cyberdelitos.

Capítulo 4. Casos de estudio. Ejemplos de situaciones en las que se produjeron fallos en la justicia, con resultados negativos, que podrían haber cambiado el curso de las decisiones, de haber seguido en forma adecuada el protocolo y metodología propuesta.

Capítulo 5. Conclusiones y aportes de esta tesis. Contiene las conclusiones en cuanto a la valoración sobre la investigación, valoración del problema, valoración de la solución, valoración de los antecedentes explicitados como casos de estudio, respuesta de los planteos realizados en el Capítulo 2, y finalmente se definen futuras líneas de investigación.

Capítulo 6. Referencias - Bibliografía. Contiene las referencias bibliográficas utilizadas en el presente trabajo.

CAPÍTULO 2. ESTADO DEL ARTE

2.1. INTRODUCCIÓN

2.1.1.- CONTEXTO DE LA TESIS

En este capítulo se presenta en la sección 2.2., las propuestas que otros autores contextualizan sobre el concepto y utilidad de la cadena de custodia (CC) que debe respetarse para la prueba informática. Pues "*Cuando hay un eslabón roto en la continuidad de esta cadena, la prueba pierde validez, y el proceso queda nulo"* Dr. Crosby González Montiel – Dr. en Derecho - México – 2013 - http://temascrosbyglez.org/video_cadenacustodia.php

En la sección 2.3. se presenta la importancia que tiene la preservación de la prueba informática, concepto que a veces se confunde con la Cadena de Custodia (CC). Para ello, es de señalar el "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) **[GUID001]**, escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Documento que provee una guía que muestra las mejores prácticas para preservar las prueba informática de la alta volatilidad de los datos, en lo que a informática respecta.

Luego, en la sección 2.4. se menciona la utilidad de la forensia informática, cuya importancia y proceso válido se plantea en la guía del DOJ EEUU, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) **[GUI005]**, permitiendo definir dos aspectos importantes en el proceso forense informático, como es la adquisición de la evidencia, el análisis de la misma y la documentación técnico – legal del reporte obtenido.

Finalmente, en la sección 2.5. se establece la diferencia que existe entre la Forensia Informática y la pericia Informática. En este aspecto, considero que el presente trabajo genera un aporte a la problemática, evaluando los conceptos vertidos en dicho apartado. "… es de destacar que la forensia informática es un componente muy importante dentro de las Pericias Informáticas…." Darío

Piccirilli – 2013/2014 **[PUB01]**, y tratando de generar un aporte para una eventual reforma del Código penal Procesal de la república Argentina **[ANTE 01]**

En la sección 2.6 se realiza un resumen del capítulo, en el que se explican tres conceptos asociados, como ser: **cadena de custodia**, **pericia informática y forensia en informática**. En tal acápite, se señala el alcance de cada concepto y su vinculación dentro del marco de un análisis pericial o dentro del marco de pre constitución de la prueba.

Aquí nace el concepto de aplicar la forensia hacia **"afuera"** de la organización (como en el caso de un pleito judicial) o hacia **"adentro"** de la organización, para aplicar en una investigación interna y generar una prueba indubitable, en caso de ser aplicada en juicio *(Mg. Darío A. Piccirilli – M.I.S.I. – Depto. Posgrado – UTN FRBA).*

2.1.2.- PRODUCCIÓN CIENTÍFICA DERIVADA DE RESULTADOS PARCIALES DE LA TESIS

Durante el desarrollo de esta tesis se han comunicado resultados parciales a través de distintas publicaciones que a continuación se detallan:

Publicaciones

Piccirilli, D. (2013*. La Forensia como Herramienta Informática*. Revista Latinoamericana de Ingeniería de Software, 1(6): 237-240, ISSN 2314-2642.

Piccirilli, D., González Allonca, J.C. (2013)*. Consideraciones legales relativas a la privacidad en proyectos de Cloud Computing en el exterior del país*. Revista Latinoamericana de Ingeniería de Software, 1(1): 1-3, ISSN 2314-2642.

Congresos Internacionales

Piccirilli, D. (CACIC 2014). *La forensia como herramienta en la pericia de informática.* XX Congreso Argentino de Ciencias de la Computación. - 1a ed. - San Justo: Universidad Nacional de La Matanza. E-Book ISBN 978-987-3806-05-6.

Piccirilli, D., González Allonca, J. C. (43 JAIIO 2014). *Consideraciones legales relativas a la privacidad en proyectos de Cloud Computing en el exterior del país*, 14º Simposio Argentino de Informática y Derecho, ISSN: 1850-2814.

2.2. PLANTEO SOBRE LA CADENA DE CUSTODIA

Hoy día, en el Código Procesal Penal de la Nación, considera en el Art. 144, en forma específica la obtención de la prueba informática ante la necesidad de secuestrarla para realizar la posterior tarea pericial.

En dicho artículo de expresa: "… *ARTÍCULO 144.- Incautación de datos. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de 39Código Procesal Penal de la Nación LIBRO CUARTO - MEDIOS DE PRUEBA - TÍTULO II - Comprobaciones directas ARTS. 145 - 148 secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 129. Regirán las mismas limitaciones dispuestas para el secuestro de documentos. El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó. Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia. Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la*

destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos….¨

http://www.infojus.gob.ar/docs-f/codigo/Codigo_Procesal_Penal_de_la_Nacion.pdf

De esta manera, se genera la necesidad de contemplar la Cadena de Custodia de la prueba informática.

La cadena de custodia es un proceso controlado que a los efectos de poder cumplir con su objetivo, debe contener básicamente una serie de aspectos, que aseguran la trazabilidad de la prueba informática. Pues, para tener éxito en el proceso pericial informático, es vital que la prueba "no se contamine". Esto es, que no se modifique o borre. Debe conservarse en su estado "original" sin alteraciones. "*La contaminación de la cadena de custodia invalida las pruebas periciales informáticas*", así lo plantea Juan de Dios Meseguer González – Abogado y Perito Informático – El Derecho – Grupo Francés Lefebvre - http://www.elderecho.com/publicaciones/autores/Juan-Meseguer-Gonzalez_9_475545001.html

Por otra parte, existen fallos judiciales relacionados con la importancia de la preservación de la prueba informática, a los efectos de poder probar situaciones indubitables, al momento de definir una situación legal. **[FALLO2] Cámara Federal de Casación Penal - REGISTRO Nro: 337/13 - Causa Nro. 16339 -Sala IV– C.F.C.P. "GIL, Juan José Luis s/ rec. de casación"**

Es fundamental comprender que desde el momento en que se secuestra una prueba informática hasta que llega a las manos de un perito para su examen técnico, y luego la devolución de dicha prueba, conforma un ciclo de vida pericial que básicamente comprende las siguientes etapas:

a) Intervención en el lugar del hecho (puede estar presente o no el perito informático)

b) Detección e identificación de la prueba a secuestrar u obtener

c) Recolección

d) Registro de los detalles del equipamiento o prueba informática, identificada como de interés para el proceso. Esto puede complementarse con el acta policial.

e) Intervención o embalaje del elemento

f) Identificación o rotulado del elemento

g) Fajado de protección del elemento

h) Traslado de la prueba (al Juzgado o Fuerza de Seguridad interviniente)

i) Almacenamiento temporal de la prueba, hasta la realización de la pericia.

j) Traslado al perito (Perito ad hoc o Fuerza de Seguridad)

k) Realización de la pericia

l) Devolución de la prueba al Juzgado

m) Posibilidad de nuevas pericias

n) Devolución de la prueba pericial al propietario

En cada paso se debe registrar los intervinientes, indicando fecha – hora – lugar y estado del elemento. Esto asegura trazabilidad de la prueba informática. Ver figuras Figura 1 – Formulario de Custodia Informática – Mg. Darío A. Piccirilli (parte 1 y 2), en la que se exhibe un formulario ejemplo de Cadena de Custodia Informática (FCCI), cuyo diseño es un aporte de la presente tesis.

REGISTRO DE CADENA DE CUSTODIA PARA ELEMENTOS INFORMÁTICOS

En este formulario se debe registrar todos los movimientos que se realicen desde el momento del secuestro o aporte de la prueba informática hasta su devolución o destrucción del /os elemento/s

Identificación causa:

Nro:	
Carátula	
Juzgado	
Secretaria	

Identificación del origen del elemento:

	Domicilio		Fecha	Hora	Interviniente (Aclarar Dependencia – experto que interviene)
	Calle – Nro.	Localidad / Provincia			
1					
2					
3					

Identificación de los elementos obtenidos:

Nro. / Rótulo	Tipo de elemento (describir PC, GPS, memoria RAM, CD/DVD, pendrive, disco rigido, teléfono, máq. Fotográfica, etc.)	Tipo de embalaje (describir como se interviene el elemento: papel madera, bolsa nylon, caja, etc.) – Si se utiliza papel que sea sin uso previo → evitar uso de papel o cajas pre impresas, etc.)	Observaciones (complementario, para identificar el elemento: apariencia física – fotografía, etc.)

Figura 1.a - Formulario de Custodia Informática

Mg. Darío A. Piccirilli

CONTINUACIÓN REGISTRO DE CADENA DE CUSTODIA PARA ELEMENTOS INFORMÁTICOS

Identificación causa:

Nro:	
Carátula	
Juzgado	
Secretaria	

	Domicilio		Fecha	Hora	Interviniente: Firma / aclaración / función	Observaciones (Guarda / Pericia / Devolución / Destrucción)
	Domicilio – Dependencia (Sede)	Localidad / Provincia				
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						

Figura 1.b – Formulario de Custodia Informática

Mg. Darío A. Piccirilli

Por otra parte, en la Justicia Argentina comienza a ser considerada la fragilidad que adolece la prueba informática. Así lo expresa la Cámara Federal de Casación Penal el 22/03/2013 - REGISTRO Nro: 337/13 - Causa Nro. 16339 - Sala IV– C.F.C.P. "GIL, Juan José Luis s/ rec. de casación", cuando expresa: "… *En este orden de ideas, corresponde tener presente que la evidencia electrónica puede ser alterada, dañada o destruida si se la manipula o analiza incorrectamente, motivo por el cual es preciso adoptar precauciones especiales a la hora de recolectar, preservar y examinar esta clase de evidencia ……. El uso de la evidencia digital o electrónica en el proceso penal requiere, pues, la adopción de medidas tendientes a preservar su integridad, desde que en caso de que una parte de la prueba resulte contaminada, toda ella se torna sospechosa y puede ser invalidada*…" **[FALLO2]**

Luego, en el Código Procesal Penal de la Nación, se establecen aspectos básicos a considerar en la cadena de custodia de la prueba, definiendo en su articulado lo siguiente: ¨… *ARTÍCULO 150.- Cadena de custodia. Con el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes*…. "
http://www.infojus.gob.ar/docs-f/codigo/Codigo_Procesal_Penal_de_la_Nacion.pdf

Pues en realidad es de vital importancia llevar una especie de "***historia clínica***" de todos los pasos que se siguen con la evidencia, siendo este un elemento sumamente frágil y volátil.
.No debemos olvidar que muchas veces del momento que se accede a la prueba o evidencia digital hasta el momento que llega al perito informático, no sólo pasa un considerable tiempo, sino que también se pasa por distintas etapas y sectores (desde el allanamiento, a la comisaría, de allí al juzgado, de allí al

perito), generándose riesgos en cada traslado, que pueden generar situaciones de alteraciones o pérdidas.

El protocolo propuesto en el presente trabajo, tiende a perfeccionar el tratamiento que hoy día se le da a la prueba digital obtenida durante allanamientos y posterior secuestro.

2.3. LA PRESERVACION DE LA PRUEBA

Este concepto se relaciona en forma directa con el punto anterior. Pues la prueba informática debe ser conservada exactamente como en su estado original, a lo largo de todo el ciclo de vida pericial (CVP). Puede suceder que deba realizar algún cambio, y esto de manera inevitable. Pero aún así, ese cambio debe ser explicado. Así lo plantea Ajoy Ghosh - Australia, en su guía Guidelines for the management of IT evidence - Marzo 2004 **[COFO003]**.

Pues la prueba informática tiene una característica esencial, que la diferencia de otras pruebas, como un arma, droga o un cadáver. Esta diferencia se llama volatilidad.

Para poder realizar una correcta preservación del elemento que nos ocupa, es fundamental contar no sólo con el protocolo que se propone en este trabajo, sino además con ciertos elementos físicos como:

a) Papel para envoltorio (puede ser papel madera u otro similar, pero que no contenga inscripciones previas, ni dibujos, gráficos o leyendas
b) Cajas de cartón, para embalaje
c) Papel especial de protección contra golpes
d) Paneles de espuma antiestática
e) Cinta de embalaje
f) Pulsera antiestática para manipulación
g) Bolsas de plástico de buen grosor, para embalaje
h) Precintos de seguridad (numerados y de distinto color)

Es de señalar que al momento de un allanamiento, es probable que no se cuenten con estos elementos, no obstante, se debe procurar mantener aspectos

fundamentales como la protección de la prueba informática y asegurar su traslado y almacenamiento hasta la intervención del perito.

2.4. FORENSIA INFORMÁTICA

Una vez obtenida la prueba informática, y habiendo corroborado los puntos anteriores, es decir, hay una cadena de custodia y la prueba ha sido debidamente preservada, deben seguirse una serie de pasos que garantizan un adecuado procedimiento. Según la guía Guidelines for the Management of IT Evidence – 03/2004 **[COFO003]**, dicho proceso debe comprender básicamente los siguientes pasos:

a) Determinar el objetivo de búsqueda forense
b) Definir un plan de investigación
c) Realizar la adquisición
d) Mantener la preservación de la evidencia
e) Realizar el análisis forense sobre la información obtenida o adquirida
f) Realizar el informe correspondiente

Es fundamental considerar la potencia de cada herramienta de forensia, y en muchos casos, es necesario aplicar una combinación de las mismas. Así lo expreso en mi artículo "La Forensia como Herramienta en la Pericia Informática" - relais-v1-n6-237-240 **[PUB 01]**, cuando se menciona "…*Generalmente, y dependiendo del problema a analizar, se sugiere aplicar una combinación de herramientas, para asegurar la efectividad que se debe tener en estos casos donde la libertad de las personas puede estar comprometida, y ello podría depender del resultado de una pericia informática aplicando herramientas de forensia* "

2.5. PERICIA INFORMÁTICA

La pericia informática es una tarea ordenada por un juez, y que debe respetar ciertos parámetros de claridad procesal para que pueda cumplir su verdadero objetivo. **[PROPER]**

El punto de partida para una pericia informática, son los puntos de pericia, y los mismos pueden ser solicitados por el Juez o por alguna de las partes que intervienen en el conflicto legal. Estas partes se denominan Actora y Demandada.

Por ende, el cuestionario pericial se compone de puntos que tienden a despejar dudas pero con distintos intereses, dependiendo quien sea el solicitante de la pericia informática. Lo que resulta claro, es que dicha tarea siempre la solicita un abogado. Por ello, es fundamental la manera en que se pide la tarea, para que se pueda asegurar el éxito de la misma y no se corra el riesgo de "revertir la carga de la prueba".

Los abogados deben comprender la complejidad de una pericia informática y obrar en consecuencia. Para cumplir este fin, se vienen desarrollando distintos congresos, eventos interdisciplinarios y capacitaciones, que tienden a acompañar esta etapa previa a la pericia.

Por ello, por ejemplo la Dra. Luz Clara y la ingeniera Di Iorio, en el taller *"Prueba pericial informática. Importancia de los puntos de pericia*", llevado a cabo en Marzo 2014, organizado por el Colegio Público de Abogados de Mar del Plata, explican los puntos que deben tener en cuenta a la hora de solicitar una pericia informática, aclarando además "… qué es la informática forense…", y ".,. *qué elementos pueden ser considerados evidencia digital, quiénes pueden ser peritos, los pasos de un proceso pericial, y todo lo relacionado con el trabajo que se lleva a cabo para que los resultados de la investigación sean los que el abogado busca y sirvan al fin de la causa*".

Pues es fundamental además entender el **perfil del problema o del delito a peritar**, es necesario saber que nunca existe una pericia informática igual a otra, a pesar que se encuentren caracterizadas por el mismo tipo de delito.

Siempre varía:

- el escenario
- las pruebas y la modalidad en que han sido obtenidas
- las partes que intervienen en el pleito o en la investigación

- las herramientas que deben usarse
- el conocimiento que el perito debe aplicar, como así también su experiencia

Por ello, a veces es necesario integrar más de un perito a la tarea pericial. Pues a pesar que tengan todos la misma especificidad, es muy probable que no todos cuenten con la misma especialidad, experiencia y grado d conocimiento sobre la tarea a realizar. (Darío A. Piccirilli - Curso de Especialización de Posgrado en Pericias Informáticas – Depto. Posgrado Informática UNLP y Depto. Posgrado UTN – FRBA)

Por otra parte, el procedimiento científico a considerar es el protocolo que se debe aplicar al momento de realizar una pericia informática, y parte del mismo es la herramienta de forensia a utilizar. En el caso de existir peritos de parte, esta tarea debe ser consensuada entre todos los participantes, con el objetivo de obtener una prueba clara y útil para impartir justicia por la autoridad competente. **[FALLO2] Carlos Machado Schiaffino. "*El perito en la Legislación Argentina*". Rev. INTERPOL, 1986 - [FoEx04] US DEPARTMENT OF JUSTICE - [FoEx05] *Forensic Toolkit* - [FoEx06] *WinHex* - [GUI007] *Electronic Crime Scene Investigation: A Guide for First Responders* - [FoEx07] *System Forensics, Investigation, and Response* - [FoEx08] *Digital Forensics: Digital Evidence in Criminal Investigations***

2.6. RESUMEN

Sobre la base de lo expuesto, se contribuye a clarificar conceptos que comúnmente son confundidos y que son básicamente:

- La cadena de custodia incluye la preservación de la prueba, pues la misma debe ser debidamente preservada en el momento del allanamiento e incorporar las características de esta preservación en el formulario de cadena de custodia. Este formulario acompañará durante todo el circuito que siga la prueba informática. Es decir, desde el allanamiento hasta la intervención del perito, incluyendo la devolución al juzgado de los elementos peritados

- La pericia informática puede incluir, aunque no necesariamente, a la forensia informática. Esto es, es posible realizar una pericia informática sin incluir forensia, pero cuando hablamos de ella, estamos hablando generalmente dentro del marco de una pericia.

Sin embargo, y considerando los avances en la tecnología informática, el uso de herramientas de forensia en general, y en particular para mobile, comienzan a ser aceptadas en el campo privado para pre constituir una prueba, para luego ser aportada en juicio, con la mayor verosimilitud posible. Ello, es lo que se conoce como la aplicación de la forensia hacia "adentro" de una organización.

Estos conceptos son también enunciados en Informática forense: generalidades, aspectos técnicos y herramientas - Óscar López, Haver Amaya, Ricardo León. (2001) **[INCFOR02]**. Conceptos similares se aplican en el documento Forensic Investigation - Hunting Down The Source of Your Attack **[INCFOR01]**

CAPITULO 3. DESARROLLO DE LA SOLUCIÓN

3.1. Introducción

En este capítulo, se presenta una serie de etapas necesarias para contemplar y definir un verdadero protocolo pericial informático, que permita brindar una adecuada y efectiva respuesta en una pericia informática. Esto permitirá contar con una base y punto de partida para el desarrollo ordenado de una pericia informática, dentro de un marco de calidad, asegurando resultados efectivos y sustentables, al momento de elaborar un fallo judicial

Se describirán a continuación una serie de etapas, que permitirán entender las características, alcances y herramientas a aplicar en el protocolo a plantear en el presente trabajo.

La primera etapa se basa en el estudio y análisis del entorno, para identificar la evidencia digital a obtener.

La segunda etapa se basa en el análisis de los puntos de pericia, que establecen el objetivo que debe cumplir la evidencia digital a obtener

La tercera etapa se basa en la adquisición de la evidencia digital

La cuarta etapa se basa en el análisis de la evidencia obtenida, conforme los lineamientos del cuestionario pericial ordenado.

La quinta etapa se basa en la forma de exponer la evidencia digital obtenida en la investigación realizada

La sexta etapa se basa en preservación de la evidencia digital tratada, y entrega al Tribunal (para eventuales futuras etapas de investigación, cuya fuente sería la misma evidencia digital).

3.2. Etapa I – Análisis del entorno

Se realiza un análisis de entorno, tanto técnico como formal del procedimiento, para identificar la evidencia digital a obtener, debiéndose considerar distintos aspectos a saber:

- **El tipo de problema o del delito**, sobre el que se deben obtener las pruebas para luego poder peritar.
  Esto incluye un análisis básico sobre el fuero o jurisdicción en el cual se ubica el delito o problema.
  Pues de esta manera se logra direccionar y definir el tipo de protocolo a aplicar. No es lo mismo proceder a identificar y aplicar prueba informática en el fuero penal, que en el fuero laboral o civil.

- **En qué lugar se encuentra y cuál es la evidencia informática a obtener** (por ejemplo es una PC – estación de trabajo, un servidor de red, un teléfono celular, un Smartphone, un Smart Tv, un disco rígido externo, una memoria flash (por ejemplo USB).

  En tales circunstancias, existen buenas prácticas que deben aplicarse, y que consisten en pasos básicos a seguir con el objetivo de obtener la evidencia digital. Es de señalar que aquellas pruebas y evidencias que no se obtienen durante el allanamiento, es muy difícil que se puedan lograr en momentos posteriores a tal acción.

- **El procedimiento científico a aplicar**.
  Es decir, si se va analizar un correo electrónico, verificar el texto del mensaje, los adjuntos (si existen) y el encabezado el propio correo, de manera que permita obtener datos para su eventual seguimiento, como por ejemplo las direcciones de IP, servidores locales o instalados en el extranjero. Esto puede facilitar a los jueces la posibilidad de solicitar información adicional, en el marco de convenios de cooperación internacional, debiendo aplicar en muchos casos un pedido de exhorto para obtener la información. **[CONV01] CONVENIO SOBRE LA CIBERDELINCUENCIA Budapest, 23.XI.2001**

- **La presencia de peritos de parte o técnicos de parte**.
  Este es un punto de especial atención, pues debemos considerar que existen dos conceptos asociados: peritos de parte y consultores técnicos.

Para los primeros, es necesario realizar una citación fehaciente a los mismos, para asegurar su participación en la pericia. No se puede realizar la tarea si no se cuenta con la presencia de dichos profesionales de parte, en caso que se los haya designado.

Claro está, que puede existir la designación del perito de parte, pero ante circunstancias de fuerza mayor, con la debida autorización del juez, la pericia se puede llevar a cabo sin la participación de esta parte.

Es fundamental que el perito de oficio, que es el designado por el juez, asegure las comunicaciones a sus pares de parte.

- **El procedimiento protocolar a aplicar**, en relación a la situación procesal

  Sobre este punto, es conveniente tener en claro el fuero en el que se encuentra ordenada la pericia informática.

  Pues dependiendo de ello, se deben tener en cuenta ciertos pasos en un protocolo para el Fuero Penal, que no son los mismos para el Fuero Laboral, y tampoco para el Fuero Civil y Comercial, o para la Suprema Corte de Justicia de la nación.

- En relación al **perfil del problema o del delito a peritar**, es necesario saber que nunca existe una pericia informática igual a otra, a pesar que se encuentren caracterizadas por el mismo tipo de delito o por escenarios similares. Pues existen variaciones en los siguientes aspectos:

  - **el escenario**

    En relación a este concepto, es importante tener en claro que de qué tipo de escenario hablamos y quienes son los actores.

    Para ello, podemos considerar el siguiente gráfico:

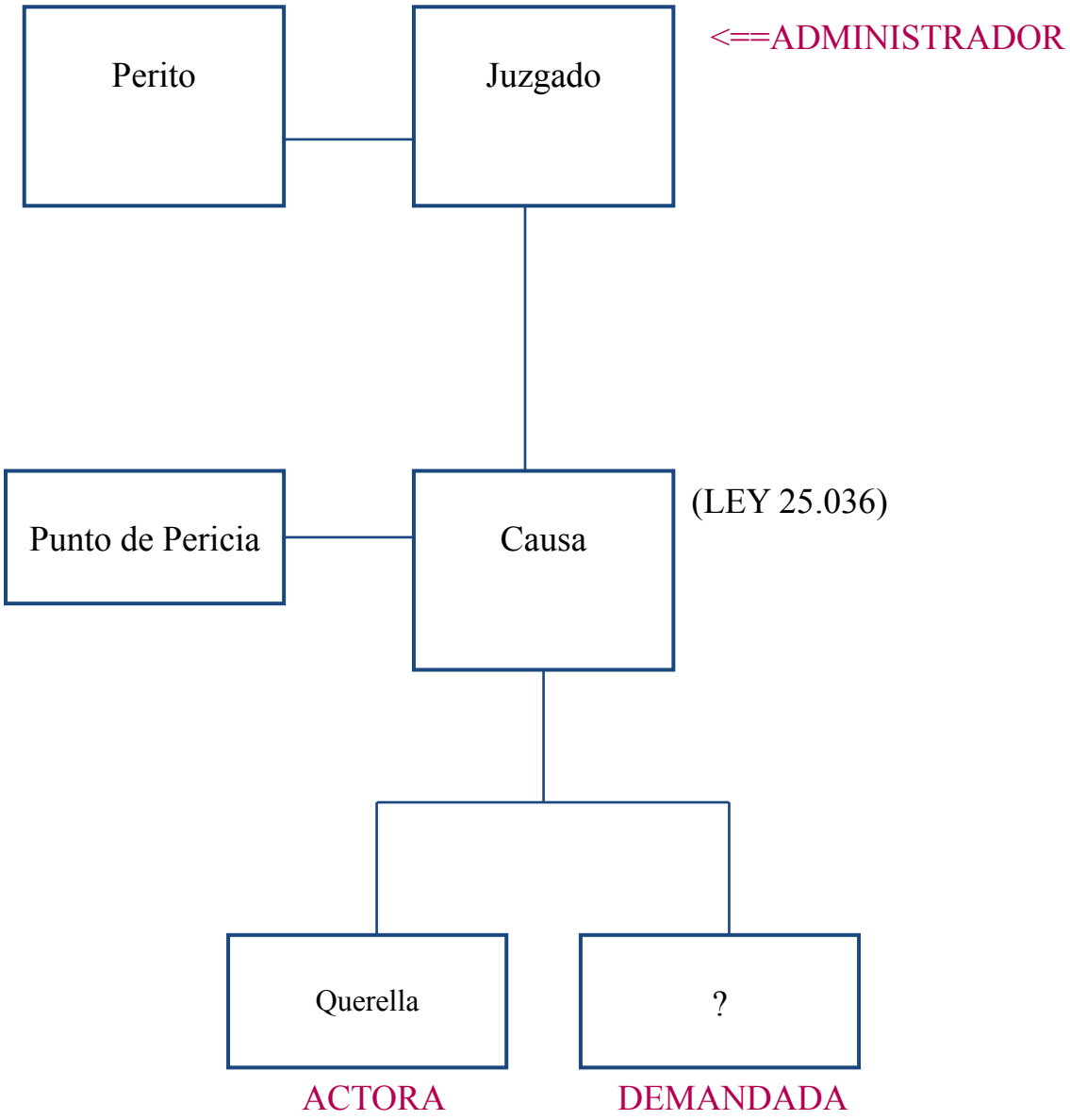

Figura 2 – Partes que Intervienen en un juicio
Mg. Darío Piccirilli – M.I.S.I. – Escuela de Posgrado – UTN FRBA

En dicho gráfico podemos apreciar:

- Juzgado: es la autoridad del Poder Judicial, encargada de administrar justicia sobre el problema planteado.

En general nos vamos a referir al Fuero Penal, Penal Económico o Penal Federal. No obstante, debe entenderse que alcanza a todos los fueron del Poder Judicial de la Nación. Es decir, al fuero Laboral, Civil, Comercial, Contencioso Administrativo Federal y a la propia Corte de Justicia de la Nación

- Perito: es el auxiliar de la justicia, que acompaña al Juzgado en el tema técnico, sobre el cual el juez no puede entender, porque no es su especificidad, es decir, no es su naturaleza.

  Hablamos en este caso del perito en informática.

  Es de señalar, que a pesar de ser auxiliar del juez, dicho experto puede ser procesado por cometer por ejemplo, falso testimonio o falsedad ideológica.
- Causa: es el motivo por el cual se inicia el litigio. Es el nombre por el cual se identifica el problema en el juzgado y para todos los intervinientes, durante lo que dure el juicio.
- Puntos de pericia: es el cuestionario técnico (lista de puntos específicos) que debe ser resuelto por el perito informático.

  Es importante que dicho cuestionario sea claro y preciso, para que el perito pueda expresarse en forma fáctica y con la objetividad que la materia exige, para poder dilucidar la cuestión.

  A veces, teniendo en cuenta la complejidad informática, es necesario que exista una intervención técnica del experto, como un paso previo a ordenar los puntos de pericia. Esto sin duda agiliza las cosas y permite lograr los objetivos previstos durante la investigación,
- Actora: es la parte que inicia la demanda o el juicio. Es quien presenta los motivos suficientes, para que el Juez entienda que corresponde dar lugar al comienzo del juicio para dilucidar el pleito.

  Está representada por un abogado que lleva adelante la tarea de impulsar el juicio

- Demandada: es la otra parte del juicio. Es contra quien se entabla la demanda. Puede ser una persona la demandada, una empresa, ambos, etc.
  También está representada por un abogado que lleva adelante la defensa de la parte que representa.

Sobre la base de lo descripto, es de señalar que nunca se van a repetir ninguna de los ítems mencionados, al menos uno de ellos va a variar en otro caso. Si no, estamos hablando de la misma pericia.

Es decir, podrán repetirse puntos de pericia, pero al menos va a variar el juzgado, o la parte actora o la parte demandada, o el perito. Algo debe variar, si no estamos repitiendo la pericia, y eso puede suceder en casos excepcionales, cuando la pericial inicial no sirvió por algún motivo y debe repetirse la misma.

b. Luego, deben considerarse las pruebas y la modalidad en que han sido obtenidas

En este punto es que se deben poner especial énfasis, pues las pruebas a peritar pueden se pueden haber generado de las siguientes formas:

- aportadas por la parte interesada.

  Puede ser un correo electrónico, una prueba informática previamente constituida por alguna de las partes (un correo electrónico, un disco rígido, una PC, un teléfono celular, un listado de computadora, una página web, un diálogo a través de una red social (Twitter, FaceBook, o similar), accesos a Internet, datos de un archivo en formato de texto (txt), un programa de computadora, un sistema específico, entre otros elementos.

- Obtenidas a través de un allanamiento

Pueden ser básicamente las mismas que las mencionadas en el punto anterior, nada más que las mismas han sido obtenidas por la sorpresa que implica el allanamiento, y por lo tanto a veces pueden adolecer de ciertas debilidades, como estar incompletas o no haber sido bien preservadas.

En estos casos, debe considerarse que existen varias alternativas a evaluar en el momento del secuestro. Es decir, es necesario considerar si se debe secuestrar sólo el gabinete de una PC, o su conjunto con teclado, impresoras, etc., debiéndose respetar una serie de pasos que hasta la fecha no se encuentran debidamente normalizados, y que a través del presente trabajo se intenta formalizar en los siguientes pasos:

a. Asegurar el área en la que se encuentra el equipamiento a analizar o secuestrar.
   - ✓ Esto significa que se debe aislar el equipo, por ejemplo:
     - alejar las personas ajenas al procedimiento (excluyendo los testigos exigibles en el protocolo procesal)
     - controlar las fuentes de energía, evitando manipular enchufes, ups, entre otros, con el objetivo de no destruir la prueba mediante manejos eléctricos
     - verificar conexiones a redes locales y remotas, con el objetivo de no evitar accesos no autorizados que intenten eliminar o alterar las evidencias útiles para el proceso de investigación
     - de ser posible analizar si existe el uso de la facilidad de **"cloud computer¨** (nuevo desafío tecnológico), es decir verificar si se utiliza la facilidad de acceso a la "nube¨ para almacenar datos. En caso afirmativo, se deberá tratar de obtener las características de acceso a tal información, a los efectos que la misma sea

"bajada¨ a un dispositivo como pendrive o disco rígido, para luego ser secuestrado y posteriormente analizado.

En estos casos es de fundamental importancia la colaboración del usuario técnico de la organización que está siendo allanada. Pues de no obtener información en ese momento, se perderá toda posibilidad futura de tener acceso a la misma.

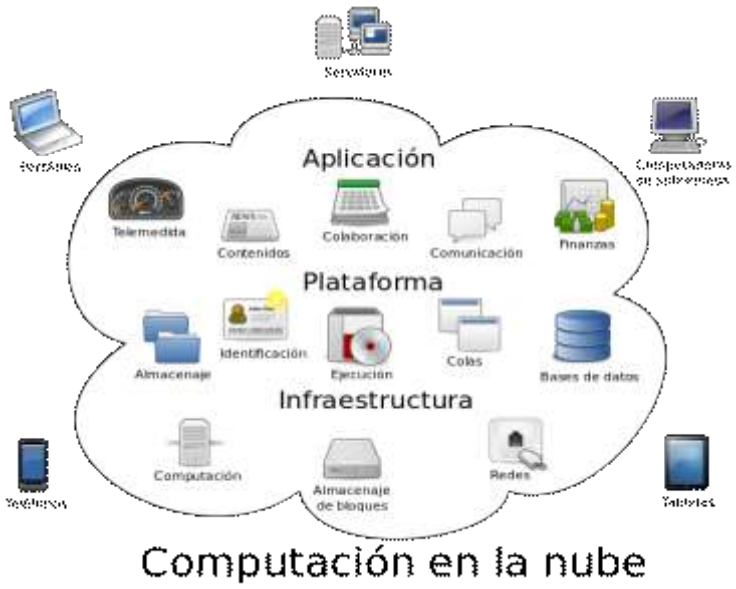

Figura 3 – Esquema básico del funcionamiento de Cloud Computing

- ✓ Luego se deben obtener imágenes fotográficas de la identificada "escena del crimen". También es posible realizar filmaciones y grabaciones de audio, a los efectos de ser aplicadas en posteriores pericias.
- ✓ También es conveniente realizar un gráfico o croquis ilustrativo de la ubicación de los elementos informáticos, especificando de ser posible posición de los dispositivos de

almacenamiento y también de comunicaciones y sus conexiones.

Es conveniente registrar en el gráfico, la distribución del cableado de datos instalado al momento del allanamiento.

- ✓ Si las computadoras están encendidas, ver la posibilidad de extraer los datos de la RAM, a través de herramientas de forensia específicas.
  Algunas de ellas, pueden ser:

  pd Proccess Dumper: Convierte datos de la RAM a un archivo del tipo TXT.
  FTK Imager: Permite adquirir datos de la memoria RAM, pudiendo copiarlas a un TXT.
  DumpIt: Realiza volcados de memoria a archivo del tipo TXT.
  Volatility: Analiza datos de procesos que puedan quedar en la RAM y extrae información para la investigación.
  RedLine: Captura la memoria a un TXT y permite analizarla. Dispone de entorno gráfico muy intuitivo para su manejo.
  Memorize: Captura la RAM, grabando un archivo del tipo TXT (disponible también en plataforma OSX).

  http://conexioninversa.blogspot.com.ar/2013/09/forensics-powertools-listado-de.html

b. Luego apagar la computadora. Verificar que la computadora se encuentre realmente encendida, analizando los indicadores de energía o de actividad de disco rígido.
   Considerar que existen protectores de pantalla que pueden confundir al perito que el computador esté apagado y en realidad no lo esté. Esto permite evitar una mala acción, que puede conducir a destruir involuntariamente la prueba.

También debe evaluarse si la computadora se encuentra en eventual estado de “ahorro de energía”. En este caso, también debe apagarse en la forma habitual.

c. Si el equipo se encuentra apagado, NO encenderlo

d. En caso de laptops, ultrabooks o netbooks, se debe tener especial cuidado si están cerradas. Pues al levantar la tapa, es posible que “se enciendan”, activando sistema operativo, actualizando la RAM y archivos en el disco rígido.

   Es conveniente quitar la batería del equipo y secuestrar los respectivos cargadores de la batería. Pues generalmente cuando el equipamiento llega a pericia, la batería se encuentra agotada y no siempre es posible obtener fuentes y conectores para realizar una efectiva conexión a energía eléctrica.

   Nunca se debe intentar explorar los contenidos que existen dentro de una computadora (es decir, explorar el contenido almacenado en el disco rígido), tampoco en cualquier otro dispositivo electrónico (por ejemplo en una cámara de fotos, teléfonos celulares, entre otros). Estos cuidados deben contemplarse en forma previa a la orden de la realización de una pericia informática, la que debe ser emanada por un Juez.

   En caso de equipos computadores, se debe verificar si el gabinete posee unidades lecto-grabadoras de CD/DVD´s. En caso positivo, verificar que no haya alguno de estos elementos inserto en dicha unidad. De ser así, se deberá extraer, identificar dicho disco CD/DVD y colocarlo en un sobre debidamente rotulado, con especificación de:

   - Equipo computador en el que fue hallado

- Características del elemento encontrado (marca, capacidad, si tiene alguna inscripción identificadora, transcribir dicha leyenda en forma textual, aclarando el color de la tinta de la notación verificada)
- Registrar estos detalles en la correspondiente acta de allanamiento

e. Luego desconectar de la red eléctrica el cable de “power” y todos los periféricos. Esto permite además de lo operativo, evitar posibilidades de accesos remotos.

f. Etiquetar los puertos y cables respectivos, con el objetivo de poder reconstruir el escenario durante la etapa pericial.

g. Verificar la posibilidad de obtener eventuales claves de acceso a las computadoras, con el objetivo de evitar demoras en el acceso a la información (pues puede derivarse en partes del proceso judicial, en las que se deberá librar oficios del juzgado para solicitar o requerir dichas claves a las partes intervinientes en el pleito).

   Durante el allanamiento, estos datos pueden obtenerse a través de papeles sobre los escritorios o pegados en los propios dispositivos. También es posible consultar a los usuarios.

g. Realizar el acta de allanamiento correspondiente, en donde se deberá especificar todo lo actuado, incluyendo formar en que fueron secuestrados los equipos, como fueron etiquetados y resguardados, si se obtuvieron passwords durante el procedimiento.

h. Como complemento a todo lo señalado en los puntos precedentes, se sugiere analizar la posibilidad de secuestrar

teclados, siendo estos elementos factibles de aportar datos adicionales, como ser huellas digitales que permitan identificar y asociar personas o usuarios.

Es de señalar que dicho aporte deberá ser analizado a través de otro tipo de pericia, pues no es de la especificidad informática.

También se deberá analizar si durante el secuestro se retiran cintas de backups, cartridges o similares, es conveniente llevar dispositivos periféricos que puedan leer dichos elementos al momento de la pericia.

De esta manera se evitan serios inconvenientes operativos que surgen al momento de realizar la tarea, y que nada tiene que ver con lo técnico específico de forensia o pericia informática.

- **Obtenidas por el perito durante la pericia informática**

  En este caso, las pruebas son generalmente muy precisas, porque el perito sabe bien lo que quiere para responder el punto de pericia, y va en la búsqueda exacta de la prueba. El problema que se puede presentar es que como el experto debe coordinar la reunión pericial para retirar la prueba, la misma puede ser incompleta o manipulada. El efecto negativo de estas situaciones, es que no se podría probar exactamente lo que el juez quiere y necesita.

- **Datos obtenidos a través de acciones de prevención para CyberDelitos**, generados a través de herramientas y acciones especiales, para ciberdetecciones y para prevenir situaciones no deseadas.

  Sobre el punto es posible señalar una serie de aspectos que se han previsto para prevenir ataques y comisiones de delitos informáticos a través de Internet. Pues hoy día, es más eficiente el “cyberpatrullaje” en la red, que el típico patrullaje por las calles.

En la siguiente figura, se especifican dichos aspectos, los que hoy día son contemplados en forma progresiva, por cada vez más organizaciones. Los mismos van intensificando su control, creciendo en márgenes significativos para el 2014 y 2015, específicamente en los ítems relacionados con:

i. Aplicación del standard ISO 27001
ii. Aplicación de herramientas de forensia para uso interno de la organización. Ello con fines de detectar autores de problemas y "medir" adecuadamente el impacto y profundidad de la penetración

Finding	2012	2013	change
Number of organisations that identified cyber security incidents on their networks	22%	56%	↑ of 34%
Number of organisations that increased expenditure on IT security	52%	27%	↓ of 25%
Number of organisations applying IT security standards & frameworks	64%	83%	↑ of 19%
Number of organisations using the standard ISO 27001	50%	83%	↑ of 33%
Number of organisations using the standard PCI DDS	20%	42%	↑ of 22%
Number of organisations using cryptographic controls	25%	60%	↑ of 35%
Number of organisations with a forensic plan in place	12%	25%	↑ of 13%
Number of IT security staff with vendor certifications	50%	60%	↑ of 10%
Number of IT security staff with at least five years' experience working in IT security	35%	79%	↑ of 44%
Percentage of respondents who identified the need for general staff to improve their IT security skills &/or practices	70%	95%	↑ of 25%
Percentage of respondents who identified the need for management to improve their IT security skills &/or practices	70%	91%	↑ of 21%
Percentage of respondents who identified the need for boards of directors to improve their IT security skills &/or practices	48%	62%	↑ of 14%
Number of organisations not reporting cyber security incidents to an outside agency	44%	57%	↑ of 13%

Figura 4 - Cyber Crime & Security Survey Report 2013 – Herramientas de Ciberdetección

- Existen diversas herramientas en el mercado desde 2004, y que permiten lo que hoy se denomina el **"Cyberpratullaje",** permitiendo obtener evidencias para aportar en una investigación.

  Dichas herramientas son generalmente de uso reservado para las organizaciones federales de investigación, entre las que podemos considerar:

  i. Herramientas de aplicación exitosa (Quantum Insert, Quantum Bot, Quatum DNS y Quantum Sky)
  ii. Herramientas en estudio (Quantum Cooper, Quantum MackDown, Quantum Phantom)
  iii. Herramientas reservadas (Quantum BisCuit)

  A continuación se exhibe en las siguientes figuras, el modelo de comportamiento de una de las herramientas mencionadas, como la QUANTUMINSERT y luego una lista de herramientas asociadas al producto QUANTUM, con especificación de sus objetivos y situación de mercado.

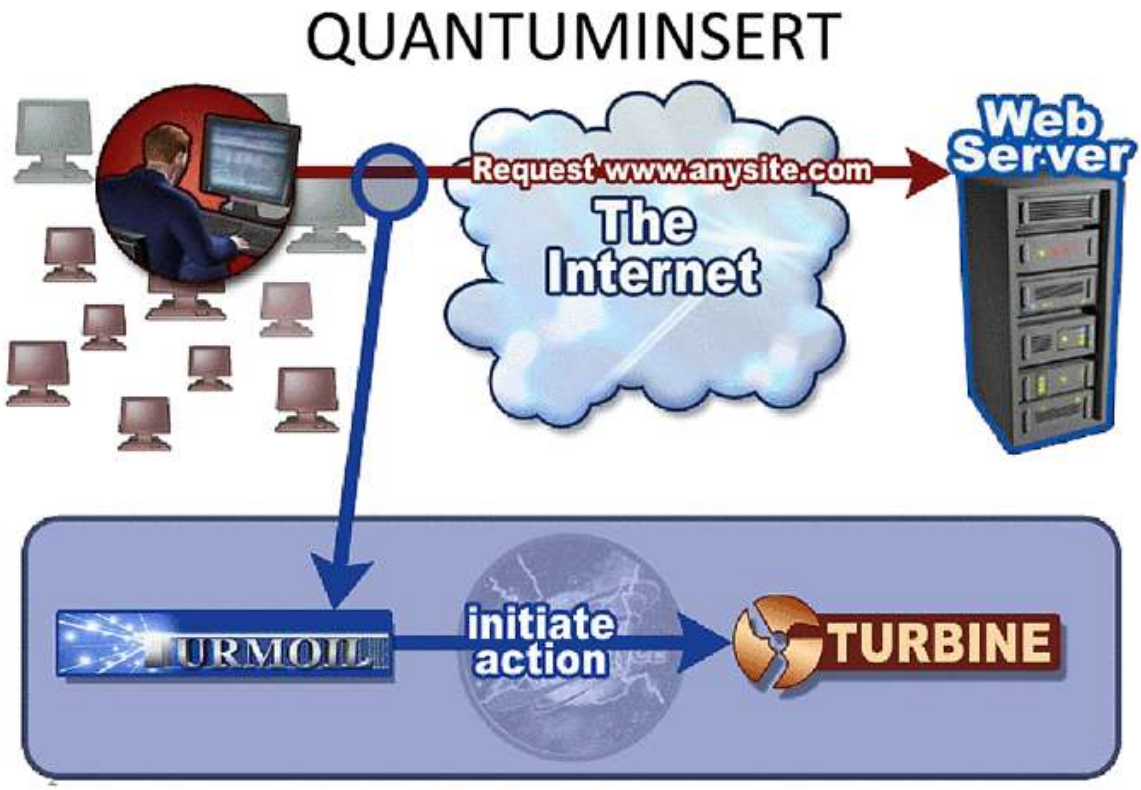

Figura 5.a. – Top Secret//Comint//Rel USA -QUANTUMINSERT

CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**

Figura 5.b. – Top Secret//Comint//Rel USA, Fvey

También existen alternativas de "rastreo digital¨, que permiten verificar la existencia de malware con distintos fines. Por ejemplo, hay aplicaciones que emplean un software específico denominado ¨mutex", que permite asegura la ejecución de una sola instancia, permitiendo así acceso y control no autorizado de un computador. **[CIBER01], [CIBER02].**

Las herramientas mencionadas, permiten realizar un seguimiento y análisis de la existencia de este tipo de malware.
Lo importante en estas situaciones, es tener un dominio de las mismas y explotar todo su potencial.

3.3. Etapa II - Análisis de los puntos de pericia

En esta etapa se realiza un exhaustivo análisis de los puntos que deben ser respondidos durante la pericia. Es deci50r, un profundo estudio sobre "qué

debe responderse", "cómo debe responderse" y "qué herramientas y métodos" deben aplicarse para resolver el cuestionario técnico.

Durante esta etapa es necesario conocer punto por punto lo que el Juez requiere, con el objetivo de dar acabada y precisa respuesta. Pues un perito no debe apartarse de lo que se pregunta, es decir no debe "irse" del punto de pericia, esto sería motivo de impugnación.

Por otra parte, debe tenerse bien en claro que un perito no puede emitir juicio de valor en la respuesta brindada en el informe.

Durante el análisis de los puntos, puede suceder lo siguiente:

a) Que exista un punto genérico, del estilo "*todo aquello que el perito pueda aportar para arrojar luz sobre la causa*". Es necesario ser cuidadoso con este apartado. Pues, no hay que exponerse frente a la posibilidad de cometer errores como los citados precedentemente, especialmente en un juicio de valor sobre lo requerido por el Tribunal. Es seguro que va a existir una impugnación.
b) Que existan puntos de pericia que si bien son requeridos por el juez, no son de la especificidad del perito informático. Por ejemplo, no es lo mismo solicitar "… *que el perito explique si en el medio óptico aportado por la parte, contiene registros de llamadas telefónicas*", a "*que el perito indique si esas llamadas han sido realmente efectuadas*". En el primer caso, la pregunta obedece a la incumbencia de un perito informático, en cambio en el segundo caso, la incumbencia profesional es la de un perito en comunicaciones. En este segundo caso, el perito informático no está obligado a responder y puede excusarse.
c) Que existan puntos de pericia que no son del todo claros, para que el perito entienda lo que debe responder. Ante esta situación, es posible que el perito se apersone al Tribunal y solicite aclaración sobre tal requerimiento. Esto puede hacerse en forma verbal o por escrito.

   Finalmente, es necesario tener bien en claro el fuero en el que se encuentra planteada la causa, a los efectos del momento en el que se presente el informe pericial con sus copias correspondientes.

Pues, en el caso del Fuero Penal, el informe pericial debe presentarse en original y solamente con una copia. Para los demás fueros, debe presentarse con original y una copia para cada parte, teniendo en cuenta si existen co-demandados o varios actores (es decir, debe presentarse una copia para cada uno de ellos). De no respetar esta parte del procedimiento, es posible que el Tribunal requiera al perito las copias faltantes, y esto será vía intimación.

3.4. Etapa III – Adquisición de la evidencia digital

Esta etapa es absolutamente técnica.

Es importante considerar qué es lo que se entiende por evidencia digital De acuerdo con el Guidelines for the Management of IT Evidence **[GUI008],** la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático".

Puede suceder que no siempre sea necesario adquirir evidencia digital, pero en el caso que así sea, debe tenerse en cuenta lo siguiente:

- El tipo de evidencia digital que se cuenta para el análisis.

  Es decir, puede contarse para análisis elementos digitales como CPU´s, discos rígidos, dongle, tablets, pendrives, smartTV´s, smartwatches, soportes ópticos (CD-ROM – DVD) o teléfonos celulares (smart phones, celulares de tecnología Android, Apple, MicroSoft, industrias chinas, entre otros)

  Concepto de forensia, conforme lo establece el FBI:

  "L*a informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional".*

- La forma en la que se va a realizar la extracción.

  En el caso de evidencia digital, se deberá conectar el elemento para hacer una copia de forensia (copia imagen de la fuente, hecha bit a bit), en modo de "protección de escritura".

  En el caso de contar con equipos PC o servidores, se debe extraer el disco rígido, sin encender o "arrancar" la computadora, para evitar la contaminación de la prueba, y con ello un posible planteo de nulidad de la pericia.

  Esta protección se puede aplicar a través de

  - Dispositivos físicos, como
    - Tableau Dead Collection: se utiliza para prevenir la escritura sobre aquellos dispositivos de almacenamiento que fueron secuestrados o aportados como prueba
    - F-Response - Network Acquisition - Write Blocker Dead Collection: permite la protección de escritura sobre dispositivos con conexión del tipo USB
  - Dispositivos de software como
    - EnCase: posee varios módulos de aplicación, entre ellos la realización de una copia forense o imagen de discos o dispositivos magnéticos, ya sea desde un disco secuestrado o en el momento de un allanamiento (conocido como Dead/Live Collection)

    Esta herramienta posee varios módulo y facilidades, entre ellas, la generación de un reporte forense, el cual debe ser interpretado por el perito, a os efectos de incluirlo en el informe pericial y explicar en forma clara y precisa el al significado y alcance del mismo.

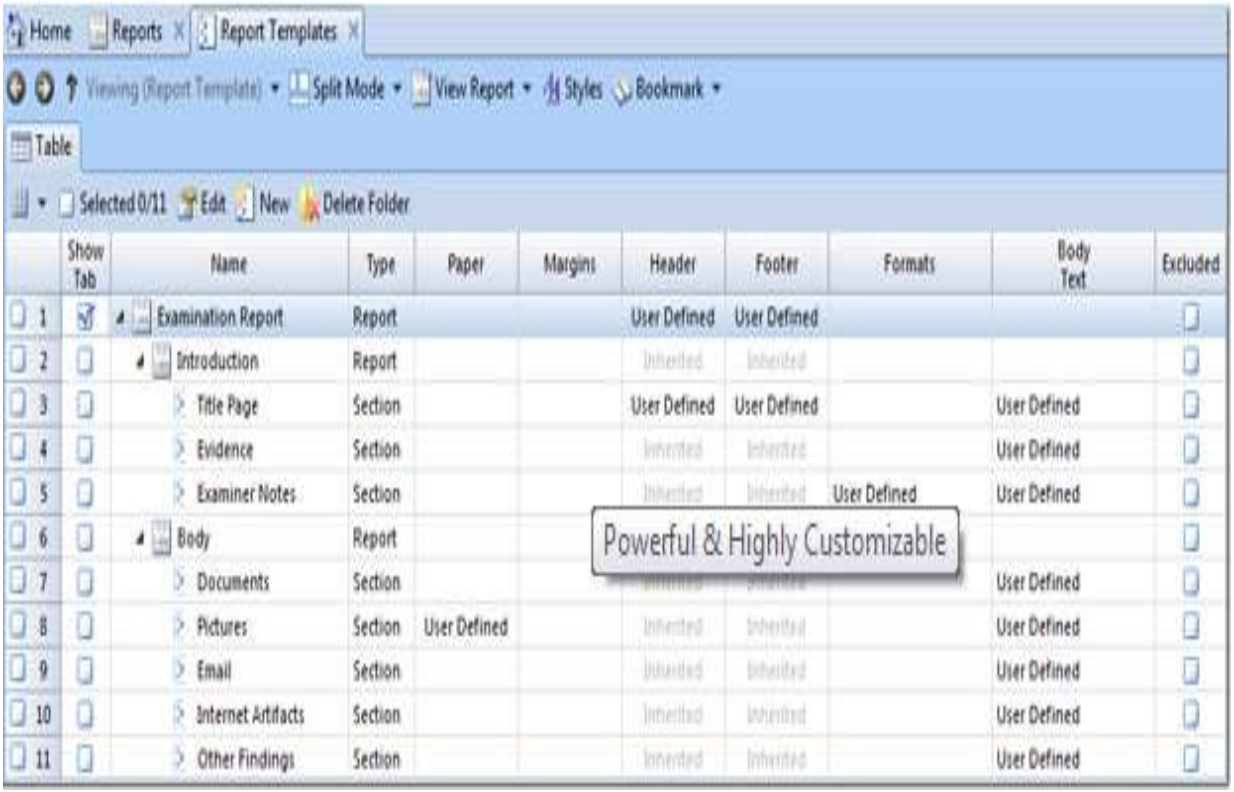

Figura 6 – Modelo de reporte de Forensia de la herramienta EnCase 7.0

- FTK: permite realizar copias imagen de dispositivos magnéticos secuestrados o en el momento del allanamiento (módulo conocido como Dead/Live Collection).

  A continuación se exhibe una pantalla de inicio de esta herramienta, en la que se muestra los aspectos requeridos para iniciar una copia de imagen forense, en la cual se debe “montar” o informar el dispositivo sobre el cual se debe realizar la copia imagen.

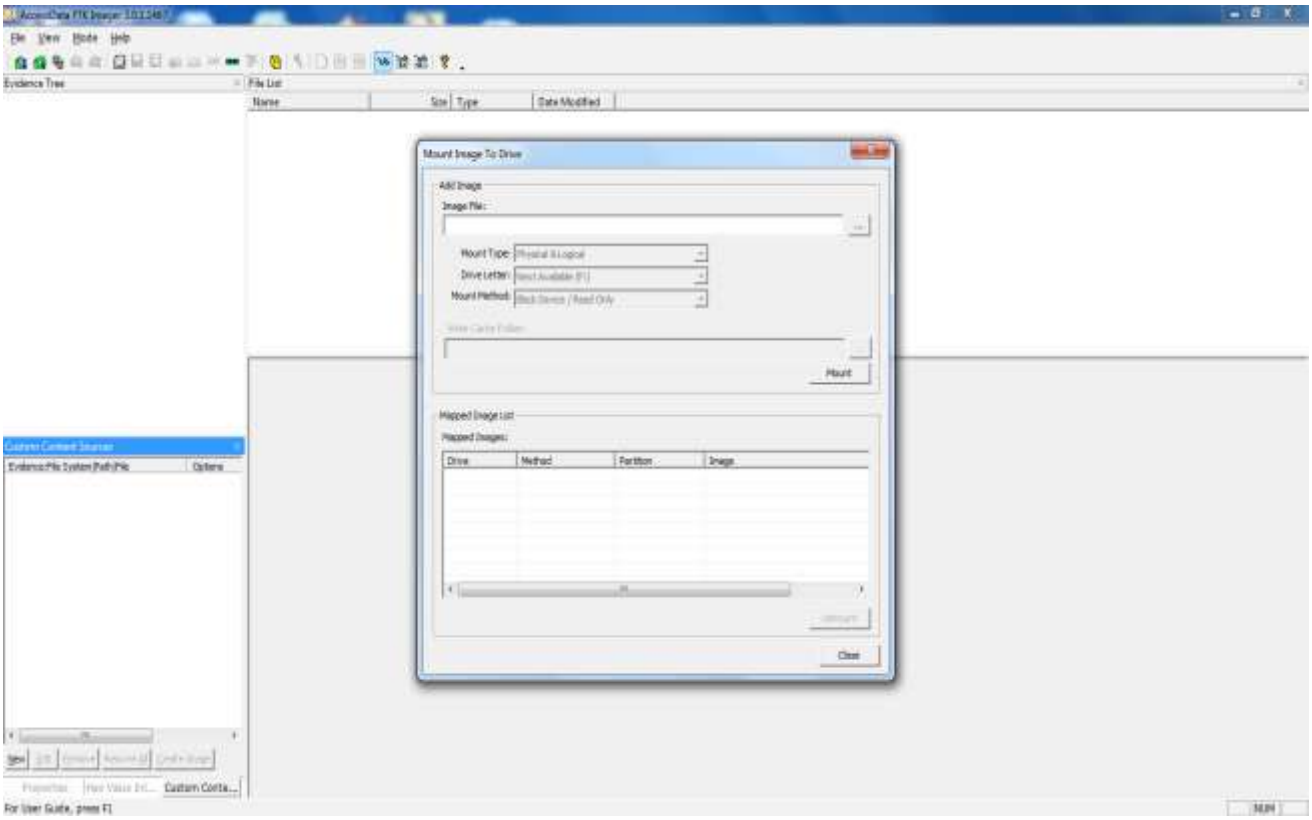

Figura 7 – Modelo de pantalla de inicio para realizar copia forense a través del FTK (Forensics Tool Kit)

- Linen Cross Over Acquisition: permite realizar copias de información almacenada en dispositivos magnéticos, de manera segura y en vivo, durante un allanamiento.

  Es de aclarar que estas herramientas permiten realizar copias o adquisiciones digitales con protección de escritura, pero aún con la computadora en funcionamiento. Esto es de vital importancia en el caso de allanamientos de morada, en los que no sería conveniente secuestrar un servidor. Pues en cuyo caso, puede existir dejar fuera de funcionamiento a una empresa, siendo no necesario proceder al secuestro físico, sino al “secuestro lógico de los datos”. Para estos casos, es vital respetar el protocolo adecuado de detección de la información a secuestrar, proceder a la

copia de la misma (con protección de escritura) e identificación adecuada para su posterior estudio pericial.

Es fundamental respetar estos pasos, ya que seguramente no podrán repetirse en otro momento. No será el mismo escenario para secuestrar prueba.

iv. Existen herramientas que permiten agilizar situaciones especiales, para analizar áreas específicas de discos o acelerar copias, cuando se trata de varias unidades digitales a copiar. Estas pueden ser:

- Disk Jockey: se utiliza para la duplicación de discos rígidos, en forma paralela
- Zero View: permite leer las cabeceras de los discos rígidos

v. En el caso de teléfono celulares, las posible herramientas a aplicar, son las siguientes:

1. Cellebrite – UFED: permite realizar un análisis forense del contenido de una gran variedad de teléfonos celulares sobre todos los modelos existentes en el mercado internacional. Incluye gran variedad de teléfonos de origen chino, que generalmente son muy complejos de estudiar. Pues hay muchas tecnologías disponibles en el mercado, y entre ellas, hay casos que soportan hasta seis (6) chips distintos.

   Esta herramienta permite identificar la información contenida en el dispositivo, incluyendo mensajes entrantes – salientes, lista de contactos, llamadas entrantes – salientes, correos electrónicos entrantes y salientes, además de detectar el número de identificación específico o IMEI del dispositivo celular.

A continuación, en figuras 8.a y 8.b se muestran tanto las características físicas de la herramienta UFED, como un breve detalle de las distintas funciones que posee el software que soporta el dispositivo.

Es fundamental disponer de una licencia actualizada de la herramienta, con el objetivo de poder absorber los permanentes cambios en las tecnologías asociadas a los teléfonos celulares, tabletas y demás dispositivos similares, que son objeto de pericias informáticas.

Hoy día, prácticamente el 60 % de las pericias incluye análisis forense de teléfonos celulares o tablets.

http://www.cellebrite.com/mobile-forensic-products

Figura 8. a - Herramienta para Forensia en celulares UFED

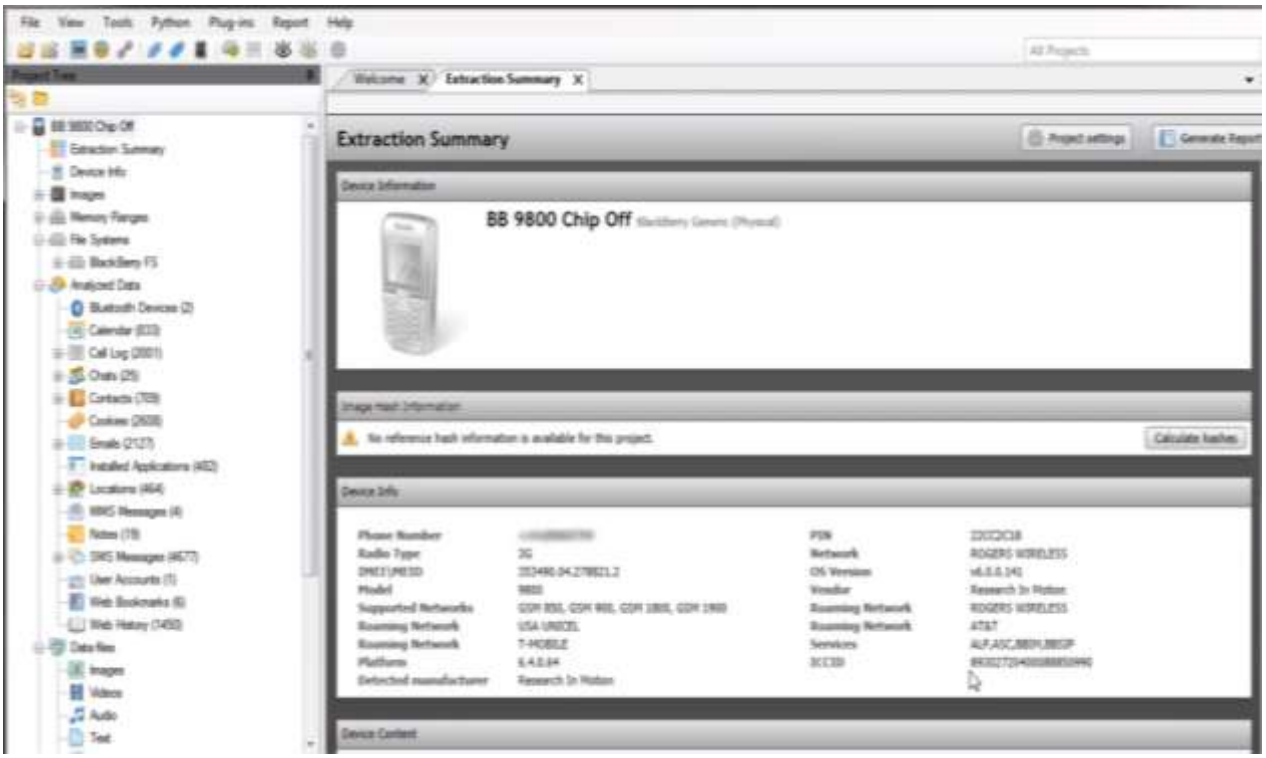

Figura 8. b - Análisis Forense en celulares con la herramienta UFED

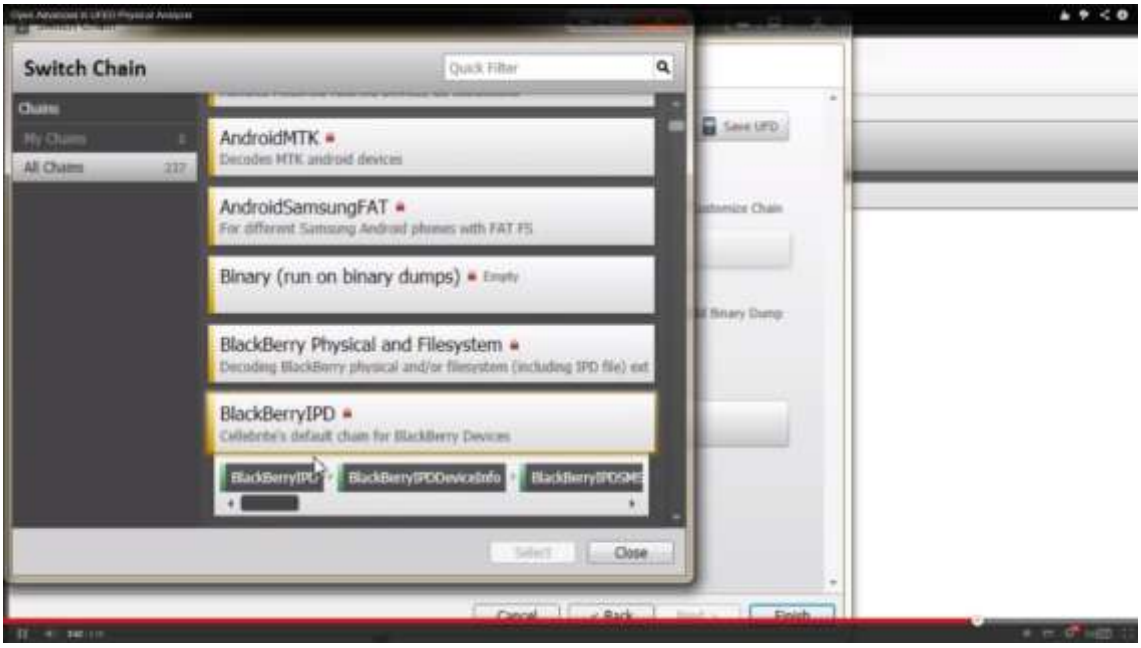

Figura 9- Distintas tecnologías en celulares - UFED

2. XRY: permite realizar un buen análisis de los smartphones o teléfonos inteligentes, sobre distintas aplicaciones y modalidades de comunicaciones

realizadas por ejemplo a través de FaceBook, Gmail, SnapChat, WhatsApp, Instagram, Skype, Viber, WeChat, entre otras aplicaciones.

Esto permite advertir una importante potencialidad de la herramienta, a la hora de tener que analizar distintas plataformas que aplican la gran variedad de herramientas utilizadas a través de las redes sociales que hoy día están vigentes.

https://www.msab.com/en/product

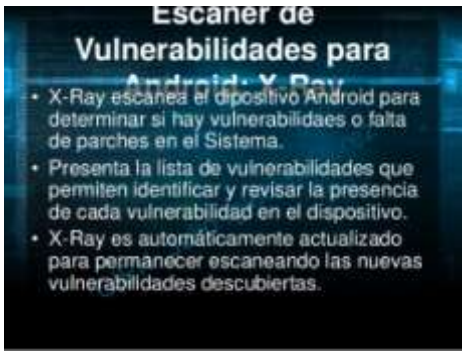

Figura 10- Herramienta para Forensia en Celulares X Ray

- Finalmente, y dependiendo del problema a analizar, se sugiere aplicar una combinación de herramientas, para asegurar la efectividad que se debe tener en estos casos donde la libertad de las personas puede estar comprometida, y ello podría depender del resultado de una pericia informática aplicando en forma adecuada las herramientas de forensia.

  Por lo tanto, existen consideraciones a tener en cuenta para la elección de las herramientas (o combinación de ellas) a aplicar en estos procesos. Las mismas son:

  i. Antecedentes de la herramienta en el mercado

  ii. Potencia de la misma

iii. Limitaciones que pueden tener (en función de búsquedas forenses, cantidad de vocablos a considerar por búsqueda, cálculo de hashes, recuperación de archivos borrados, detección de vocablos en slack spaces, entre otros aspectos)

iv. Dominio de la herramienta por parte del perito que la aplica, con el objetivo de aprovechar al máximo sus posibilidades y facilidades

v. Experiencia y entrenamiento en el uso de la herramienta

vi. Conocimiento actualizado sobre las últimas versiones disponibles en el mercado

- Como parte final del protocolo de trabajo, es fundamental que se requiera el cálculo de los códigos “hash”, es decir, se debe calcular el MD5 y el SHA1. Esto es lo que se considera la “franja virtual” de la evidencia, para preservar adecuadamente la misma, y asegurar en forma indubitable la prueba, en caso que deba usarse la misma en otra pericia, o sea necesario repetir la pericia.

  Es una buena práctica el cálculo de ambos algoritmos en el mismo proceso

- Es fundamental tener en cuenta que el disco destino donde se realiza la copia de forensia, haya sido debidamente “sanitizado”, es decir, que se encuentre adecuadamente borrado o “wipeado”, de manera tal que no exista ningún dato remanente de otra actividad de forensia o de datos previamente contenidos en dicho dispositivo.

  Pues de no ser así, existe la posibilidad que el análisis forense sea contaminado involuntariamente.

3.5. Etapa IV – Análisis de la evidencia obtenida

En esta etapa se debe analizar básicamente los siguientes aspectos:

- El tipo de evidencia digital que se dispone para su análisis
- La herramienta a aplicar
- Posible combinación de herramientas

A continuación se realiza una breve descripción de estos aspectos:

a. En primer lugar se debe analizar el dispositivo objeto de la pericia. Por ejemplo: si es un disco rígido o un teléfono celular.

   En el caso de un disco rígido, es posible que se necesite investigar sobre:

   - las características del sistema operativo (SO) instalado en el disco rígido
   - si existen archivos borrados en un disco rígido secuestrado
   - verificar las fechas de creación, modificación, borrado o último acceso a los archivos
   - buscar archivos en espacios liberados por el sistema operativo (FREE SPACE) que posee el disco rígido
   - analizar si los discos fueron cambiados
   - analizar la posibilidad de encontrar evidencia en los espacios liberados y parcialmente ocupados por otra información distinta a la original (SLACK SPACE)
   - buscar en archivos que poseen claves (Password) y que no han sido provistas en forma previa al análisis de la información
     En el caso de un teléfono celular, es posible que se necesite investigar sobre:

     - mensajes de texto enviados y recibidos
     - correos electrónicos enviados y recibidos
     - contactos guardados en el dispositivo
     - imágenes
     - mensaje de voz
     - geo referenciación de los archivos

Es de señalar que no todos las marcas y modelos de teléfonos celulares tienen las mismas posibilidades de búsqueda y hallazgos, particularmente los de origen chino, que en algunos casos llegan a poseer hasta seis (6) chips.

b. **Protocolo a seguir una vez clarificado el objetivo**: una vez evaluado el dispositivo celular o elemento óptico o magnético a estudiar, es necesario definir:

- si se va a aplicar sobre un teléfono celular, se debe analizar sobre las herramientas de forensia que se disponen, si se aplican aquellas que se encuentran con hardware y software integrado o aquellas que se aplican a través de software solamente

- si se va aplicar sobre elementos magnéticos – comunes o de estado sólido (por ejemplo pendrives, discos rígidos), se debe aplicar duplicadores forenses, que permiten generar una copia imagen del disco origen, sin alterarlo. También se aplican elementos de protección contra escritura o bloqueadores, con el objetivo de evitar contaminar la prueba. Esta protección de escritura puede ser por hardware o software.

- existe la posibilidad de tener que realizar la forensia informática in situ, es decir en el momento del allanamiento. Para ello existen soluciones de herramientas “portables”, que permiten obtener pruebas bajo protocolos de forensia, sin contaminar la prueba y sin retirar o secuestrar los elementos del lugar que se allana.

  Esto permite aplicar criterios prácticos al momento del procedimiento del pedido de secuestro, pues existen situaciones que el parque de computadoras que se investiga es muy grande (por ejemplo, mas 50 equipos), y sería muy complicado retirar todos los elementos, cuando se sospecha que solamente en alguno de ellos puede existir información de interés para la causa que se investiga - **[COFO002] Good Practice Guide for Computer-Based Electronic Evidence - Official release version**

c. Se debe considerar que cada herramienta cumple una finalidad específica, y a igualdad de objetivos, existen algunas que son más eficientes que otras.

Por ejemplo, existen herramientas que son muy intuitivas para realizar búsqueda información sobre palabras clave que generalmente ordena un Juez, y que son las que deben figurar en forma explícita en los puntos de pericia. Pero puede suceder que a la hora de realizar un bloqueo de escritura, presente debilidades.

Otras que permiten un excelente bloqueo de escritura para preservar la prueba de contaminación digital, pero no son ágiles para búsqueda y análisis sobre palabras clave.

Es de señalar que pueden presentarse tres (3) situaciones posibles, al momento de analizar la evidencia obtenida:

- Que el Juez haya ordenado en forma clara y precisa los vocablos o palabras clave para la búsqueda, con todas sus variantes. Por ejemplo, se solicita buscar datos asociados a “Juan Pérez”, y se especifica “Juan”, “Pérez”, “Perez”, “J Pérez”, “J Perez”, “J.Pérez”, “J Perez”, e inclusive sus variantes con todas mayúsculas o con todas las letras minúsculas.
- Que el Juez haya ordenado en forma clara y precisa los vocablos o palabras clave para la búsqueda, pero sin indicar todas las variantes. Por ejemplo, indica “Juan Perez”, y el perito deberá especificar en la herramienta de forensia las distintas variantes que pueden asociarse a la búsqueda en cuestión.
- Que el Juez haya indicado los conceptos de búsqueda, sin precisión de las palabras clave, y que quede en el criterio del perito la definición de tales vocablos

  En estos casos, se debe la necesidad de aclarar los puntos de pericia requeridos por el Juez. Ello debido a que muchas veces se le pide al perito la búsqueda de evidencia digital en forma amplia o

genérica. Es decir, no se definen por ejemplo las “palabras clave” sobre las que se debe realizar el análisis digital.

Pues para realizar esta tarea, sobre la copia o imagen forense obtenida anteriormente, es necesario ser muy preciso en lo que se debe analizar, ya que guarda directa relación sobre el objeto. Por ejemplo, se puede especificar el número de una cuenta bancaria, una dirección de IP, la especificación de un correo electrónico, la especificación de una imagen, etc.

Esto es fundamental que se encuentre especificado en los puntos de pericia, pues de lo contrario puede quedar librado al criterio del perito que realiza la tarea, y probablemente dicho criterio puede no coincidir con la estrategia de investigación que se sigue.

Finalmente, es importante considerar que existen otras variables a aplicar en el momento del a búsqueda de evidencia, las mismas son:

- El conocimiento que el perito tiene sobre el uso de la herramienta (para poder realizar un verdadero aprovechamiento de todas las facilidades de la misma, aplicando distintas configuraciones, entre otros aspectos). Es decir, frente a un mismo hardware se pueden aplicar distintas configuraciones de la herramienta de forensia.

- Experiencia en el uso de la misma. Es decir, cuanto más haya utilizado la herramienta de forensia, mejor preparado va a estar para considerar las posibles variantes de hardware que se presenten durante la pericia.

Es decir, podrá evaluar y adecuar su tarea si es un disco SATA, IDE, SCSI-I/II o de estado sólido, o es una memoria SSD, o es una PC, NoteBook, NetBook, tecnología MAC u otra. En todos los casos la herramienta y configuración a aplicar es la misma, pero el hardware no. **[GUI004] Chapter 1. Electronic Devices Types, Description, and**

Potential Evidence - [GUI006] Guidelines for the Management of IT Evidence - [COFO001] Computer Forensics – Part 2: Best Practices - Information Security and Forensic Society

Por ello, a veces es necesario integrar más de un perito a la tarea pericial. Pues a pesar que tengan todos la misma especificidad, es muy probable que no todos cuenten con la misma especialidad, experiencia y grado de conocimiento sobre la tarea a realizar, los distintos elementos que intervienen en la tarea pericial, como así también las herramientas asociadas. **[ReEx01] Recovering and Examining Computer Forensic Evidence - [ScWo01] Scientific Working Group on Digital Evidence.**

En figuras 11 y 12 se muestra una parte de todo el probable material informático a analizar durante un proceso de forensia y pericia informática. En las mismas es posible observar desde discos del tipo ZIP DRIVE, pasando por diskettes hasta todo tipo de tecnología en discos rígidos.

Figura 11 – Distintas tecnologías en discos rígidos [GUI003]

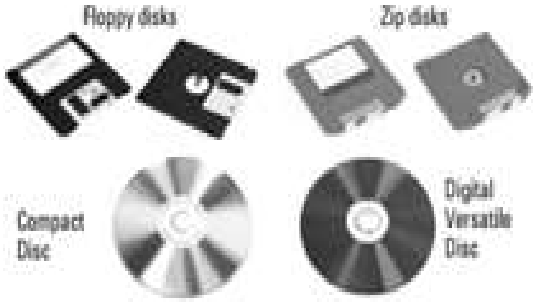

Figura 12 – Distintas tecnologías en medios removibles (CD´s – DVD´s) [GUI003]

Figura 13 – Distintas tecnologías en medios removibles (dispositivos USB storages) [GUI003]

Teniendo en cuenta la variedad de elementos a peritar y considerando que muchas veces los expertos en informática que intervienen en una pericia, poseen conocimientos limitados a ciertas tecnologías (pues es muy difícil poseer experiencia y conocimiento integral en todos los elementos y dispositivos informáticos), es de fundamental importancia que el Juez comprenda la necesidad de formar un equipo interdisciplinario de peritos, de manera tal que se pueda compartir e integrar las habilidades y expertise de un equipo de trabajo.

3.6. Etapa V – presentación de la Evidencia Digital obtenida

Esta etapa se basa en la forma de exponer la evidencia digital obtenida en la investigación realizada, para que sea de fácil interpretación por quien debe impartir justicia, es decir por parte del Juez.

Es de fundamental importancia evaluar la forma en que se va a entregar al Juzgado la evidencia digital obtenida, juntamente con el informe pericial ordenado.

El propio FBI plantea expresa que se debe considerar la forma de "*presentar*" dicha evidencia **[IOCE06] International Organization of Computer Evidence**. De esta manera se hace clara referencia a que una vez obtenidos los hallazgos, es importante evaluar la manera de estructurar los mismos para que el Juez pueda entenderlos y considerarlos para valorarlos en la administración de la justicia. Pues es importante tener en cuenta que cualquier objeto que pertenece a la escena del crimen, siempre deja un rastro en dicha zona o en la víctima, en otras palabras: "cada contacto deja un rastro" **[EviDig05]**

Pues normalmente las herramientas de forensia informática producen reportes que no son intuitivos de entender por alguien que no trabaja a diario con estos elementos. Si esta parte no se respeta, la pericia puede haber sido muy bien hecha, pero no le sirve de mucho al Juez, si no la puede entender bien.

A modo de ejemplo, se exhibe a continuación una imagen del resultado obtenido a través de la aplicación de la herramienta de forensia informática, conocida como FTK (Forensic Tool Kit) imager:

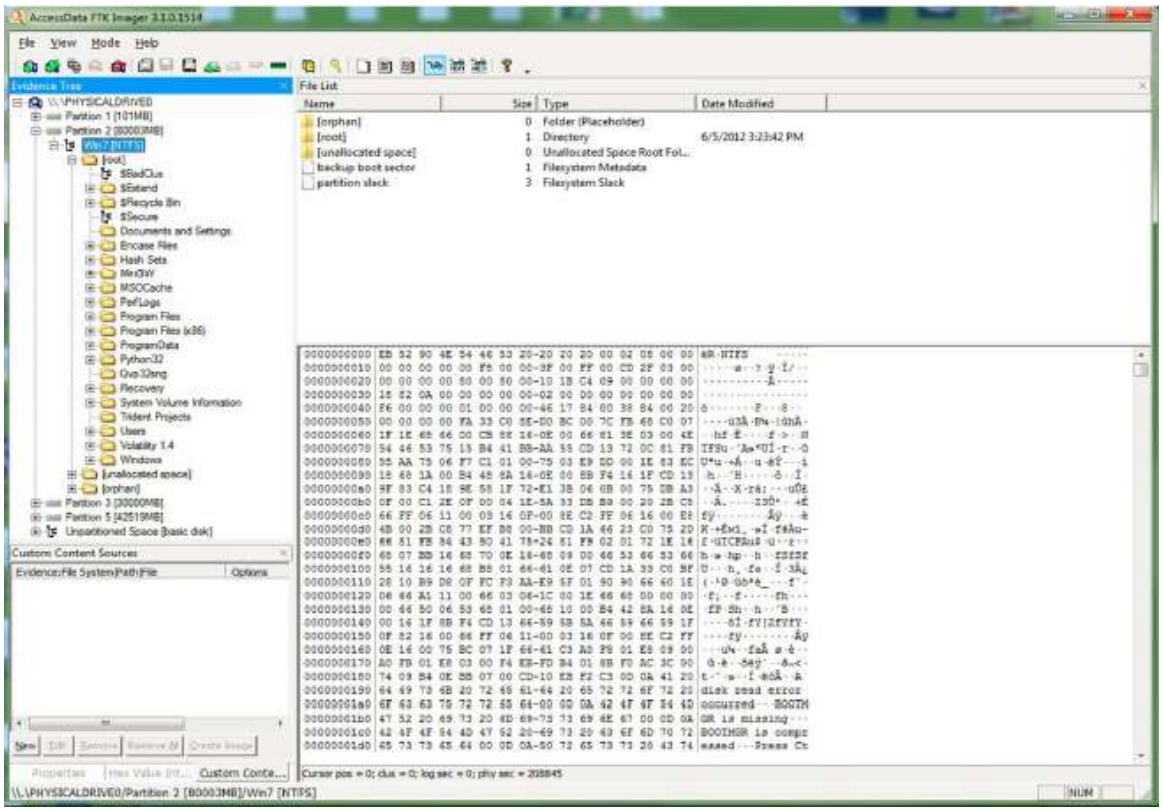

Figura 13 .a. – Visualización de una copia forense para análisis

En la figura exhibida, es posible visualizar un árbol de estructura de datos, obtenidos en la realización de una copia de forensia (imagen) de un disco secuestrado en una causa penal. Sobre el cuadrante inferior derecho, se puede apreciar una serie de caracteres en formato hexadecimal, como a continuación se exhibe, algo que evidencia na seria dificultad para comprensión de un letrado, si se presenta de esta manera:

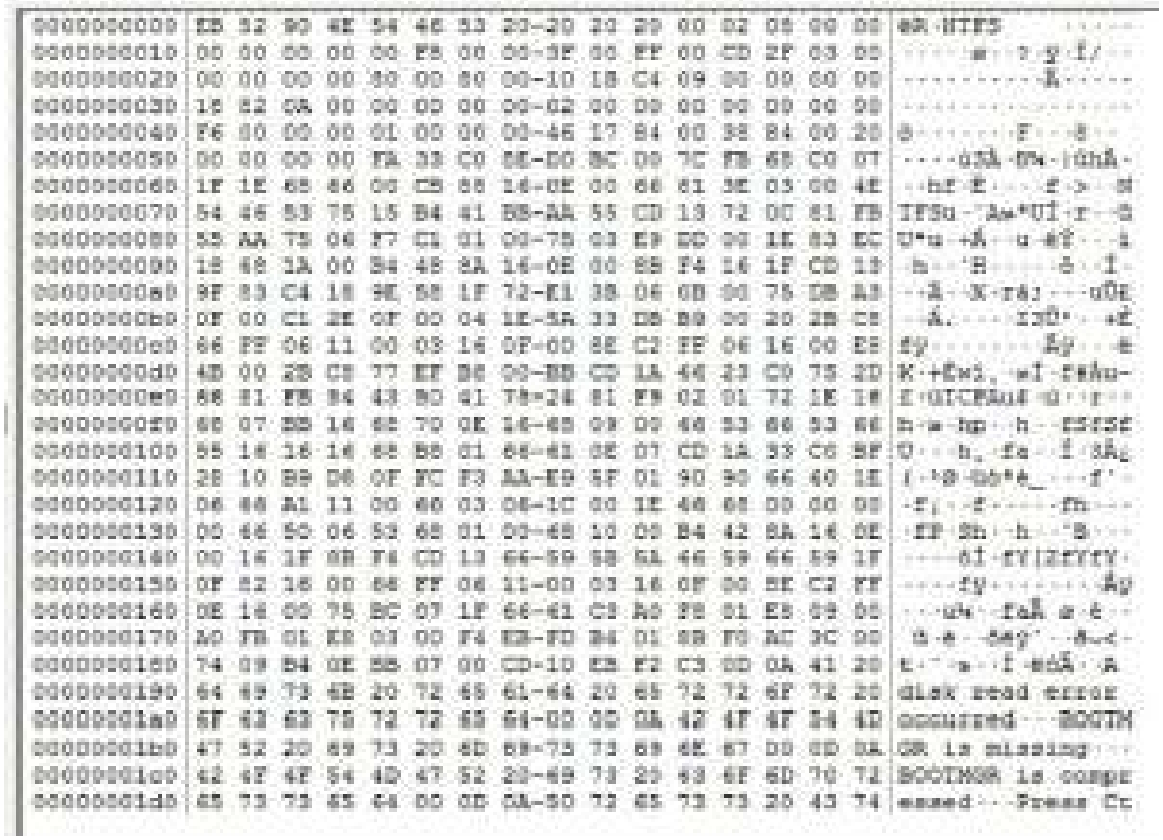

Figura 13. b. – Interpretación de la copia forense de un archivo

Sobre la base de lo exhibido, es posible observar que existe una seria dificultad para ¨entender¨ por parte de un letrado (ya sea el juez o de los abogados de las partes), el significado del contenido digital y su relación con la investigación que se realiza.

Este es uno de los mayores desafíos para un perito informático.

Pues debe informarse en lenguaje claro y llano tanto el contenido de los hallazgos digitales obtenidos como también un detalle exhaustivo de todas las tareas técnicas desarrolladas.
Además, debe acompañarse la descripción técnica de la herramienta informática aplicada, que debe permitir manejar el alto volumen de datos que muchas veces se obtiene durante el desarrollo de los pasos anteriores. Esta herramienta generalmente

no es la misma que la utilizada en las etapas II, III y IV, desarrolladas en este documento, sino que debe ser de fácil comprensión y manejo por alguien que no entiende de informática.

Muchas veces se solicita separar los mensajes de texto de las imágenes, de los documentos en Word o de las planillas en Excel. También, el juzgado suele requerir que los correos electrónicos sean enviados en una interfase de fácil comprensión para el administrador de justicia.

En muchos casos se aplica por ejemplo, el “mailnavigator”. Esta es una herramienta free, que suele interpretar varios formatos de correos electrónicos, de manera tal que sean de fácil visualización e interpretación en el juzgado que debe evaluar el resultado de la pericia, entender la información que aplica para la investigación, y sobre ella administrar justicia.

A continuación se exhibe la herramienta en cuestión:

MailNavigator ***www.mailnavigator***

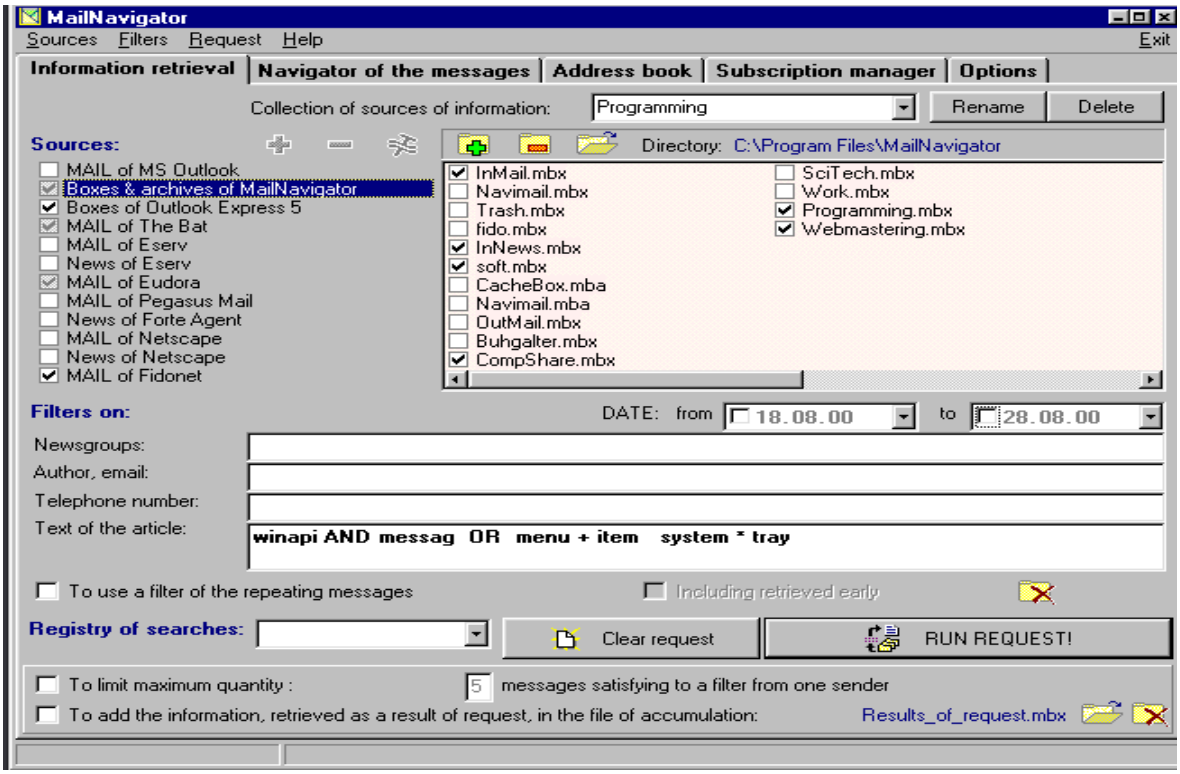

Figura 14 – Herramienta para interpretación de correos electrónicos obtenidos durante el análisis forense

Finalmente, es fundamental poseer conocimientos y capacidad para explicar y demostrar objetivamente (por ejemplo, mediante diagramas), de manera clara y lógica las evaluaciones y sus conclusiones, de manera que resulten comprensibles para personas sin la formación científica – informática **[GUID002] Guía para el desarrollo de la capacidad de examen forense para documentos.** Es de recordar que el destinatario de este informe pericial, es el propio Juez, encargado de administrar e impartir justicia.

3.7. Etapa VI – Preservación de la Evidencia Digital – Entrega al Tribunal

La sexta etapa se basa en preservación de la evidencia digital obtenida y analizada, considerando que puede ser necesario volverla a utilizar en eventuales nuevas etapas de investigación, cuya fuente sería la misma evidencia digital aplicada anteriormente.

Para ello, se consideran las siguientes sub etapas, una que describe los pasos a seguir con la preservación e identificación de la prueba digital, y la otra que contempla las posibilidades que pueden presentarse para el tratamiento de los elementos en cuestión, con posterioridad a la pericia.

3.7.1. Protocolo a aplicar.

A los efectos de mantener en forma inalterable la prueba informática y considerando su alta volatilidad, y profundizando el protocolo en desarrollo, se debe complementar con una lista de pasos ordenados y necesarios que permitan satisfacer las necesidades periciales y de forensia: Los puntos que se proponen son los siguientes:

a. Se debe calcular el hash correspondiente y registrarlo en el informe pericial o acta de devolución de los elementos informáticos.
   A tales efectos, se debe calcular dicho código a través de dos algoritmos: de seguridad, que son MD5 y SHA1.

   De esta manera, es imposible que se generen los dos mismos hashes para distintos datos. Es decir, estamos asegurando que si se calculan y comparan dos hashes (MD5 y SHA1) y dan iguales, estamos hablando exactamente de la misma información.

   Conceptualmente, podemos decir que este tipo de seguridad para evitar manipulación de datos, se llama **"franjado virtual"** de elementos informáticos (Mg. Darío A. Piccirilli – Curso de Postgrado Pericias Informáticas – Facultad de Informática – UNLP), y es mucho más eficiente que el franjado físico.

b. Luego se debe realizar un resguardo físico.
   Este paso permite continuar con la preservación de la prueba desde el punto de vista físico. Ello, con el objetivo de desalentar otras posibles manipulaciones en los datos.
   Es de aclarar que si bien se ha resguardado la prueba desde el punto de vista lógico (cálculo de hashes), es bueno contemplar la opción de resguardo físico, con el objetivo de evitar la destrucción involuntaria de la prueba, por ejemplo por mal trato. Muchas veces, el traslado de la prueba es realizado por personal de las fuerzas de seguridad que no es técnico, y por lo tanto no entiende del rigor de cuidado que hay que tener con elementos tan sensibles y volátiles, como son las pruebas informáticas.

Para ello, es conveniente:

a) Si son discos rígidos, pendrives o similares, es conveniente colocarlos en bolsas antiestáticas, y protegidos con espuma antiestática

b) Proceder a envolver los elementos (discos, PC´s en todos sus expresiones (notebook, netbook, ultrabook, etc.), en papel de embalaje y protección contra golpes

c) Envolver en papel madera, todos los elementos

d) Generar una franja (tipo secuestro), en la que se identifica:
    - La carátula de la causa (nombre y número de la misma)
    - El Tribunal interviniente (Juzgado – Secretaría, Fiscalía, Cámara, Corte, etc.)
    - Datos básicos del elemento protegido
    - Fecha del procedimiento
    - Firmas de los intervinientes (peritos, fuerza de seguridad)

e) Cubrir dicha franja con cinta de embalaje transparente (no utilizar cinta de embalaje color marrón)

f) Cerrar todas las partes del envoltorio con dicha cinta, de manera que no quede un espacio posible de abrir, sin ser sellado por la cinta de embalaje.

g) Completar el formulario de cadena de custodia, con los datos señalados en el punto d)

h) En caso de teléfonos celulares, se deberá realizar lo planteado en los puntos anteriores, pero es

conveniente que vayan sin la batería inserta, sino embalada junto al aparato.

i) En caso de elementos ópticos, aplica lo detallado en los puntos b) a g).

3.7.2. Etapas posteriores a la pericia y práctica forense

a) Remisión de los elementos al Tribunal de origen.

Esta etapa consiste en la devolución de todos los elementos utilizados en la pericia, al Tribunal que los haya remitido para su análisis.

b) Es posible una repetición / ampliación pericial:

- la repetición de la pericia, por otro perito informático
- una ampliación de la pericia, por el mismo u otro perito informático

c) Luego el Juez deberá decidir sobre:

- La **devolución** de los elementos al origen (dueño de los elementos o empresa en la que se secuestraron los elementos)
- La **destrucción** de los elementos

A continuación, en la **Figura 15**, se desarrolla un gráfico que permite apreciar en forma integrada, las seis (6) etapas del protocolo propuesto, en el que se especifica la etapa, su orden y los alcances de la misma.

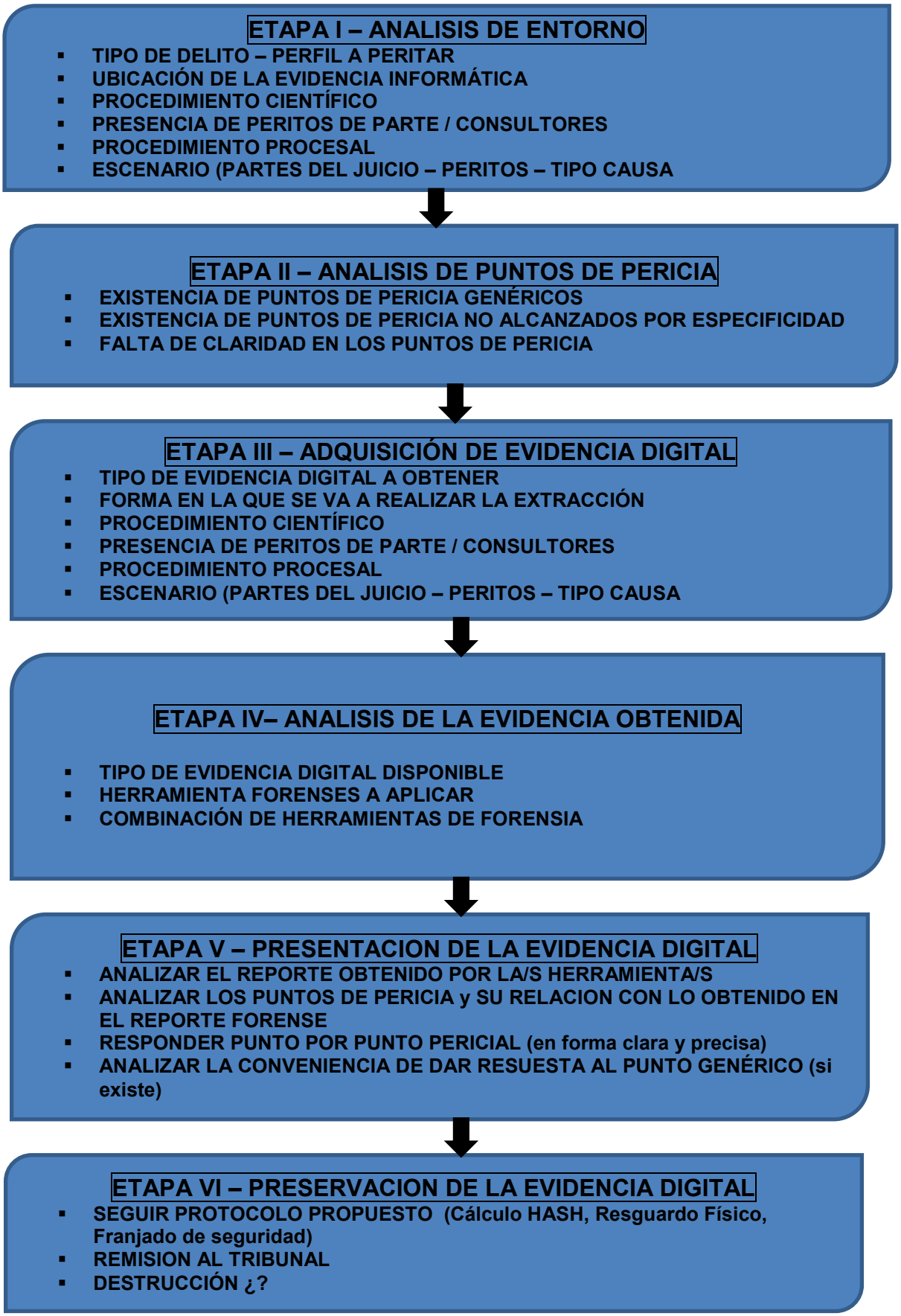

Figura 15- Cuadro resumen de las etapas base para el protocolo pericial y forense

CAPITULO 4. CASOS DE ESTUDIO

A continuación se especifican fallos relacionados con los conceptos vertidos durante el presente trabajo, relacionados con:

4.1.- Fallo A - [FALLO1] (lo resaltado en el texto me pertenece)

Cadena de Custodia ¨Pericias informáticas - E-mail de Vázquez - Causa Jaime¨
http://es.scribd.com/doc/129710378/Pericias-informa-ticas-E-mail-de-Va-zquez-Causa-Jaime#scribd

Causa n° 46.744 "*Fiscal s/ apela declaración de nulidad de informe pericial" Jdo. Fed. N° 7 - Sec. N° 14 Buenos Aires, 24 de mayo de 2012.*

VISTOS Y CONSIDERANDO:
Vuelve a intervenir el Tribunal con motivo del recurso de apelación interpuesto por el Fiscal de 1ª. Instancia contra el punto II del auto obrante a fs. 288/309 que resuelve "decretar la nulidad en la presente causa n° 12446/08 y respecto de la pericia practicada por la División Apoyo Tecnológico de la Policía Federal Argentina sobre las computadoras secuestradas en los domicilios de la calle Juncal 790 piso 7 y en la calle Salta 324 piso 4 "A" ambas de esta Ciudad; como también así de todo acto que hubiere tenido lugar en la causa en su consecuencia: particularmente la pericia encomendada a los técnicos de la Universidad de Buenos Aires, sus conclusiones, la información obtenida y la extracción de testimonios ordenadas al respecto.
Al deducir el recurso, el titular de la acción reparó especialmente en un peritaje llevado a cabo por el Ingeniero en Informática Forense Gustavo Daniel Presman, en el marco de la causa 1219/09 del Juzgado nro. 10 del fuero, sobre el mismo material secuestrado en esta investigación. Ese dictamen llevó al Fiscal a sostener "que la evidencia obtenida por los profesionales de la UBA -en concreto, los correos electrónicos que constituyen la evidencia probatoria para este y otros expedientes no sufrió alteración alguna con posterioridad a su secuestro". Al mismo tiempo, destacó que más allá de las buenas prácticas forenses no existe un protocolo de actuación que prevea la observancia obligatoria de aquéllas para realizar peritajes sobre material informático (fs. 310/315). En esta instancia, el Fiscal General presentó memorial escrito. Dijo que la pretensión del órgano era obtener la revocatoria de la decisión por encontrarla arbitraria debido a haberse apartado de las constancias fácticas y de las normas que regulan el supuesto de hecho. Sostuvo que no

existió ruptura de la cadena de custodia de donde derivó que "no ha existido una ventana temporal que permita inferir la adición a las máquinas de algún contenido que no se encontrara radicado en ellas desde un inicio, contrariamente a lo sostenido por el magistrado". Esa afirmación la respaldó con el hecho de que los elementos pasaron de estar en poder del imputado a estar en la órbita de funcionarios públicos. Distinguió los casos en que la prueba era adquirida violando la norma, de aquellos en los que la cadena de custodia se vio comprometida; afirmó que sólo a los primeros se los fulmina de nulidad y, en relación a los segundos, llamó la atención sobre el valor del testimonio del personal policial. Relativizó la denuncia de violación de la cadena de custodia que hicieran los expertos de la UBA criticando que se haya dado trascendencia al hecho de que los puertos de alimentación eléctrica no estuvieran fajados, a la vez que opuso la falta de hallazgo de indicios de operaciones destinadas a la modificación de los datos y calculó el tiempo que insumiría realizarlas. Insistió también en lo afirmado por el Ingeniero Presman, en el sentido de que las modificaciones encontradas obedecerían a reservorios o registros del sistema como consecuencia de no haber utilizado programas de protección de escritura, pero que ninguno se correspondía con correos electrónicos. Consideró como una tarea imposible de realizar, en el poco tiempo en el que los ordenadores estuvieron en la Policía Federal Argentina, la creación de 7546 archivos y su inserción a través de los puertos de alimentación eléctrica. Por último, efectuó una extensa alocución en contra de lo que el Dr. Moldes denomina "deformación ideológica de las garantías constitucionales" y "fundamentalismo garantista". Las defensas de Ricardo Jaime y de Manuel y Julián Vázquez mejoraron los fundamentos del fallo.

1°) Este incidente que la Cámara tiene por segunda vez a su conocimiento -en el marco de la causa que se instruye contra el ex Secretario de Transporte de la Nación, Ricardo Jaime, por el delito de enriquecimiento ilícito- se inició a raíz de la presentación efectuada a fs. 1/7 por la defensa de Manuel y Julián Vázquez, a la que luego adhirió la defensa del nombrado Jaime por sus argumentos (fs. 20/24), por la por la cual pretenden la exclusión de una de las pruebas en que se sustentan la investigación y la imputación que se les formula, al primero como autor del delito y a los dos restantes como personas interpuestas. En resumidas cuentas, lo que se denuncia es que inmediatamente después del secuestro de computadoras efectuado en los domicilios de los Vázquez, se ordenó a la División Apoyo Tecnológico de la Policía Federal hacer una pericia sobre dichas computadoras para conocer el contenido de sus discos rígidos, cuya realización no fue notificada a la Defensa -en violación a lo dispuesto por los arts. 200, 201 y 258 del CPPN- con el argumento de que se trataba de una operación extremadamente sencilla y reproducible en el futuro, y que una vez culminada esa pericia, de cuya ejecución el Fiscal sí estaba al tanto, se ordenó a pedido de éste practicar otra con intervención de técnicos de la UBA, nueva pericia ésta cuya realización fue anoticiada a las defensas, pero cuyo resultado (el hallazgo de documentos electrónicos que el Fiscal pretende utilizar como prueba de cargo) se encuentra precedido de la advertencia de los peritos de la UBA de que el material que recibieron no había sido debidamente resguardado, habiéndose violado la cadena de su custodia. Se pide, en consecuencia, que se anulen ambos peritajes, el primero por la omisión de

practicar la notificación que manda la ley procesal y la consecuente violación del derecho constitucional de controlar la producción de prueba, y el segundo por la sospechosa contaminación de la evidencia puesta de resalto por los profesionales de la UBA luego de una primera revisión en la que la defensa fue excluida indebidamente.2°) Al pronunciarse esta Cámara el pasado 5 de mayo de 2011 en este mismo incidente (resolución registrada bajo el n° 428), se indicó que "…la verdadera discusión se vinculaba con la posibilidad de utilizar prueba obtenida por medios ilícitos o prohibidos …" pues "… más allá de la autenticidad o no de los intercambios epistolares, las partes introducen la posibilidad de que los documentos electrónicos hayan sido colocados clandestinamente en las computadoras mientras se encontraban secuestradas a disposición del Juzgado …"

y expresamente se señaló que la sospecha introducida por las defensas, que resultaba necesario disipar a través de las diligencias pertinentes, se nutría

"… primero, del escaso control permitido a las partes -por ejemplo, omitiendo notificaciones -; segundo, de la existencia de dos estudios con resultados opuestos (v. fs. 1093/1099 y 12.319); y tercero, dela afirmación de los expertos de la Universidad de Buenos Aires que manifestaron … en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia…"

.En esa ocasión se anuló la resolución adoptada en primera instancia que había rechazado la nulidad impetrada por la defensa y se ordenó practicar nuevas diligencias tendientes a esclarecer las circunstancias bajo las cuales se produjeron los peritajes practicados tanto por la División Apoyo Tecnológico de la Policía Federal cuanto por la Facultad de Ciencias Exactas y Naturales de la UBA, para luego volver a decidir en consonancia con el resultado de esas diligencias y en función del resto de las constancias de la causa atinentes a la incidencia planteada.3°) La cuestión a decidir se refiere a lo que en doctrina se conoce como límites formales para la averiguación de la verdad, concepto que remite al conflicto que suele suscitarse entre el compromiso del Estado en la averiguación de la verdad y la protección del individuo imputado de un delito. Esos límites se traducen en reglas que, en palabras de Maier, estabilizan el sistema pues evitan que "…la meta de averiguar la verdad lo desequilibre, al ser cumplida aún a costa del ser humano individual y de cierto ámbito de privacidad que le garantiza el Estado de Derecho…" (Maier, Julio B. J. "Derecho Procesal Penal. I. Fundamentos", Editores del Puerto, Buenos Aires, 1999, pág. 664).Por eso, como dice la Corte Suprema de Justicia de la Nación, "…la actividad legislativa enfrenta permanentemente el desafío de lograr un adecuado equilibrio entre un proceso penal ´eficiente´ y uno que le dé al imputado la oportunidad de defenderse en un marco de verdadera imparcialidad…" (Fallos 327:5863), concepto que se extiende a la actividad judicial en tanto, en palabras del propio Máximo Tribunal "… el conflicto entre dos intereses fundamentales de la sociedad: su interés en una rápida y eficiente ejecución de la ley su interés en prevenir que los derechos de sus miembros individuales resulten menoscabados por métodos inconstitucionales de ejecución de la ley…" debe resolverse a favor del individuo pues resultaría comprometida la buena administración de justicia al pretender constituirla en beneficiaria de tales métodos inconstitucionales (Fallos 303:1938 y decenas posteriores que siguen esa doctrina).

Es decir, en algunos casos, la averiguación de la verdad, herencia del modelo inquisitivo y meta general del procedimiento -cfr. art. 193 CPPN-, debe ceder frente aciertos resguardos pensados en función de la seguridad individual. Las reglas de garantía tienen la misión de apuntalar aquellos límites. De tal modo, para asegurar el derecho de defensa ("Es inviolable la defensa en juicio de la persona y de los derechos" –art.18 de la Constitución Nacional-) se prevé que la persona imputada de cometer un hecho delictivo cuente con asistencia técnica, declare ante un juez y tenga conocimiento previo tanto de la imputación como de la prueba de cargo. Vinculado con este último -el control de la prueba-, otras reglas de garantía imponen la obligación de notificarlo de la realización de las medidas probatorias, sobre todo aquellas irreproducibles y de ofrecerle, en su caso, la posibilidad de proponer peritos, puntos sobre los cuales se ha fundado la protesta de la defensa en esta causa. Junto al control de la prueba, como derivado del derecho de defensa, también se encuentra involucrada la aplicación de otras reglas de garantías asociadas al derecho a la intimidad y a la inviolabilidad de la correspondencia epistolar y los papeles privados ("El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados…" –art. 18 CN), pues éstos sólo pueden ser intervenidos y utilizados como prueba de cargo cuando un juez lo autorice, por decisión fundada, a través de un procedimiento regularmente cumplido. En aquella primera intervención de esta Cámara a la que antes se hizo alusión, se adelantó que el desconocimiento de esas reglas de garantía conducía a excluir la prueba y así fue que la encuesta se direccionó a superar el interrogante que contemplaba la posibilidad de que en autos se hubiese producido una actuación ilegítima o irregular en la incorporación de elementos de cargo a esta causa, en violación a las señaladas reglas. Con el resultado de las diligencias ordenadas es que, entonces, han vuelto las actuaciones a decisión del Tribunal. Ellas, aunadas a las constancias del expediente obrantes con anterioridad, abonan a nuestro entender el planteo de la defensa de losimputados.4°) En primer lugar, tenemos en consideración que la orden de practicar la primera de las pericias, aquella que fue llevada a cabo por la División Apoyo Tecnológico de la Policía Federal (ver auto de fecha 29/7/2009, a fs. 941), no fue notificada a las defensas de los imputados para que pudieran controlar su producción, pese a la expresa solicitud formulada por una de ellas de tener "…intervención… en todas las… pericias, inspecciones…que se lleven a cabo en la instrucción de la presente causa…" (ver escrito del 31/7/2009 a fs.1082 de la causa principal), cuando, por el contrario, la lectura del expediente evidencia que la Fiscalía sí estaba avisada de dicho peritaje en curso (ver notificaciones de fs. 1007 vta. y fs.1040 vta., también del principal, ambas del 31/7/2009).El art. 258 del CPPN (del capítulo correspondiente a la prueba pericial)dice que cuando un juez ordenare la realización de una pericia "…notificará esta resolución al ministerio fiscal, a la parte querellante y a los defensores antes que se inicien las operaciones periciales, bajo pena de nulidad, a menos que haya suma urgencia o que la indagación sea extremadamente simple…", disposición que resulta coherente con la manda general en materia de prueba contenida en el art. 201 del CPPN que establece que "…antes de proceder a realizar alguno de los actos que menciona el artículo anterior [art. 200 "…reconocimientos, reconstrucciones, pericias e inspecciones…que por su naturaleza y características se deban considerar definitivos e irreproducibles…"] …el juez dispondrá, bajo pena de nulidad, quesean notificados al ministerio

fiscal, la parte querellante y los defensores… Solo en casos de suma urgencia se podrá proceder sin notificación…bajo pena de nulidad". Basta con dar lectura a los dos informes periciales cuestionados (Policía Federal a fs. 1093/1095 y 1097/1099 y UBA a fs. 12.318/12.323) como así también al producido luego por la Universidad Tecnológica Nacional (fs. 267/284), para descartar de plano y categóricamente que la peritación ordenada fuese una operación "extremadamente simple" de las que alude la norma citada (art. 258 CPPN), sobre todo si se tienen en cuenta las innumerables prevenciones señaladas por los mismos técnicos de la Universidad de Buenos Aires a fs. 12.318vta./12.319, así como la complejidad propia de las operaciones tendientes a la preservación de la evidencia, al uso de bloqueadores de escritura, a la búsqueda y recuperación de archivos informáticos, a su copiado, al uso de programas de recuperación de archivos eliminados o de observación de archivos ocultos, etc., etc., etc. Sobre este punto, que hace al núcleo del planteo de la defensa y que es relevante por lo antes expresado, los fiscales intervinientes nada han dicho.4°A) La "urgencia" alegada para realizar el peritaje sin notificación a las partes (puntualmente a quienes les fueron secuestradas las computadoras y que resultan también imputados en la causa junto a Ricardo Jaime, no así al Fiscal que sí estaba anoticiado)tampoco aparece explicada en el auto que ordenó la medida más allá de su mera invocación(ver fs. 941). La mera trascripción de esa palabra no puede suplantar la indicación de los motivos en los que ella se debe asentar, pues está en juego un derecho que la ley acuerda a las defensas bajo expresa sanción de nulidad. Y a juzgar por las constancias del expediente inmediatamente posteriores al examen (ver auto de fecha 4/8/2009 a fs. 1131/1132) el "apuro" originario se dirigió, antes que a estudiar el contenido y utilidad probatoria de los archivos electrónicos que halló la División Apoyo Tecnológico de la Policía Federal, a requerir –sin mayores explicaciones- un nuevo examen de las mismas computadoras con el objeto de buscar otros archivos electrónicos distintos (ver pedido fiscal del 7/8/2009 a fs. 1302 y del auto del juez del 10/8/2009 a fs. 1310), esta vez sí, curiosamente muy poco tiempo después de la primera, a la vista de las defensas. Qué fue lo que marcó la diferencia entre la primera y la segunda pericia para negar a las defensas su intervención en una y concederla en otra (con tan corto plazo de diferencia) no se sabe, pero del expediente surge con seguridad que no fue precisamente la urgencia (sobre todo si, además de lo ya dicho, se presta atención a que la UBA presentó su informe un año y medio después) y sobre esto, que hace al núcleo del planteo de las defensas, tampoco los fiscales intervinientes hicieron mención. El fiscal, en procura de dar legal contención a lo aquí ocurrido, evoca la regla jurisprudencial sentada por la Cámara Nacional de Casación Penal según la cual la nulidad prevista en el Código Procesal sería de carácter relativo y puede considerarse subsanada si la defensa no la opone concretamente en tiempo y forma oportunos. No obstante, ella no encuentra aplicación en el caso desde que el planteo invalidante fue efectuado en esta causa dentro del plazo previsto en el art. 170, inc. 1°, del CPPN e, incluso, había mediado una petición formal de una de las defensas de participar "…de todas las…pericias, inspecciones…que se lleven a cabo en la instrucción de la presente causa…" antes de que la pericia en cuestión fuera llevada a cabo (conf. fs. 1082 de la causa principal).4°B) El carácter "irreproducible" de la primera de las pericias practicada (División Apoyo Tecnológico de la Policía Federal) si bien resultó acreditado con las

comprobaciones efectuadas posteriormente sobre el modo como aquélla se llevó a cabo y sobre el resguardo (mejor dicho, no resguardo) de la evidencia por parte de dicha autoridad policial, ya se proclamaba -en esencia- desde mucho antes. En efecto, la sola naturaleza de los elementos sometidos al examen pericial era ya suficiente alerta sobre la cautela y precauciones que correspondía adoptar, especialmente la observación de cada una de las solemnidades que debía revestir todo acto que los tuviera por objeto, tal como el máximo control en su desarrollo. Sin embargo, ninguna de esas circunstancias halló lugar aquí. Ello condujo, tal como los peritos de la UBA primero sugirieron y luego comprobaron, a la imposibilidad de aseverar que las computadoras secuestradas contuvieran -sin alteraciones, supresiones o adiciones- los mismos archivos que tenían registrados al momento de su secuestro y, por tanto, a tornar ilusoria la exacta reproducción de un estudio sobre ellas. La forma en que fue ordenado y conducido el peritaje hecho por la Policía Federal frustró así un segundo examen que, sin resquicio a duda, permitiera afirmar que los archivos consultados eran los mismos que se encontraban presentes en los ordenadores desde su incautación. Al respecto cabe recordar, en primer lugar, el informe producido por los técnicos de la Facultad de Ciencias Exactas y Naturales de la UBA obrante a fs.12.318/12.323, donde previnieron expresa y puntualmente acerca de las condiciones en que recibieron las computadoras y dieron cuenta de la imposibilidad de asegurar -en vistas del modo como se llevó a cabo el estudio anterior- la cadena de custodia de la evidencia que habrían de analizar. En ese informe, a fs. 12.318/12.319, se da cuenta de lo siguiente: "… 1) ENCABEZADO DEL INFORME… 2) INTRODUCCIÓN…

3) VALIDACIÓN YVERIFICACIÓN DE LA CADENA DE CUSTODIA:

A. Mediante escrito de fecha22/12/2009 se fijó fecha para el inicio de la pericia el día 2 de febrero de 2010. En el mismo escrito se solicitó al Juzgado la información correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indicase fechas y horas en que dicho material fue obtenido por primera vez, y las fechas y horas en que el mismo fue utilizado en previa/s pericia/s si las hubiere, como así también los métodos informáticos utilizados para evitar la contaminación de la prueba.

B. En la fecha 2 de febrero de 2010 al iniciarse la pericia, y en el momento de entrega del material a periciar, el Juzgado no proveyó la correspondiente documentación respaldatoria del mantenimiento de la cadena de custodia, indicando solamente en forma verbal que el material habría sido secuestrado el día 28/7/2009 y la pericia anterior fue finalizada el día 3/8/2009.

C. La cadena de custodia se refiere a la fuerza o cualidad probatoria de la evidencia. Debe probarse (si fuese requerido por el juez o fiscal) que la evidencia presentada es realmente la misma evidencia recogida en la escena del crimen, o recuperada a través de algún testigo, entregada por la víctima, o por otros sujetos o adquirida originalmente de alguna otra forma.

D. Para cumplir con este requisito debemos mantener un registro minucioso de la posesión y de la cadena de custodia de la evidencia. Este puede asegurarse mediante un sistema de recibos y registro minucioso. E. La cadena de custodia también implica que se mantendrá la evidencia en un lugar seguro, protegida de los elementos, que no se permitirá el acceso a la evidencia a personas que no están autorizadas. F. En el documento anexo denominado "Descripción narrativa de la recepción de los efectos" puede observarse que el material recibido del

Juzgado no se encontraba adecuadamente protegido para su uso, ya que los puertos de alimentación eléctrica no estaban adecuadamente inhabilitados. G. Es una buena práctica de la profesión forense informática "mantener y verificar la cadena de custodia" para asegurar que todos los registros electrónicos originales no han sido alterados.
H. En tal sentido y en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia.
I. Consultado el juzgado sobre esta situación el día 9 de febrero en el momento de la devolución de la evidencia, el señor prosecretario, Dr. Eduardo Córdoba, manifestó conocer esta situación indicando que el juzgado igualmente deseaba obtener el resultado de la pericia. Si las constancias de la causa obrantes al tiempo de la anterior resolución de esta Cámara ofrecían serias dudas sobre la legitimidad del modo en que se procedió, las diligencias practicadas con posterioridad conducen a nuestro juicio a excluir la prueba cuestionada. Por supuesto que son serias algunas de las objeciones que, al menos desdelo fáctico -pero sólo desde lo fáctico-, oponen tanto el Fiscal de 1ª Instancia como el de Cámara para intentar salvar jurídicamente la validez de lo actuado, pero cada una de esas objeciones presenta su propia debilidad a poco que se las analiza en profundidad en base a las constancias de la causa y, en última instancia, ninguna de ellas salva el problema que se ha señalado más arriba: que según la ley, bajo pena de nulidad, la defensa tenía derecho a participar y controlar la producción de una pericia y fue excluida sin una justificación válida, y que luego se pretende utilizar en su contra una prueba que se dice hallada a través de un procedimiento cuya regularidad y eficacia se encuentran científicamente cuestionadas por no haberse preservado adecuadamente la evidencia, como también manda la ley. Veamos: Que los peritos de la UBA fueron más prolijos y exhaustivos que los dela Policía Federal en la confección de sus respectivos informes por escrito no caben dudas en cuanto se repasa el contenido de dichos informes, pero que hubieran utilizado una herramienta informática de búsqueda más sofisticada o eficaz -como argumentan los Fiscales para ofrecer una explicación al hallazgo de otros archivos electrónicos por parte de la UBA- es una afirmación que ofrece reparos, pues se encuentra contradicha. ***El Licenciado en Sistemas Darío A. PICCIRILLI de la Universidad Tecnológica Nacional (responsable de la tercera pericia practicada) sostuvo a fs. 273 que "no es posible afirmar si se utilizaron o no idénticos programas y/o métodos de búsqueda****" pero arribó a esa conclusión -según él mismo explica-sólo en base a que los informes de la Policía Federal no lo especificaron en tanto el de la UBA sí lo hizo, es decir, se estuvo únicamente a lo que consignaron por escrito unos y otros peritos. No puede soslayarse, sobre este punto, que al ser interrogados los peritos policiales acerca del programa de búsqueda por ellos empleado, si bien el Sargento Daniel Héctor RODRIGUEZ dijo que no lo recordaba (ver testimonio de fs. 167/168), el Oficial Ayudante Sebastián TERENTI incluyó el mismo programa utilizado por la UBA dentro de los posiblemente empleados ("…no lo recuerda específicamente pudiendo haber utilizado el mismo motor de búsqueda de Windows, software encase forensic o FTK…" -ver testimonio de fs. 164/166-), en tanto que el Inspector Víctor AQUINO afirmó de modo contundente haber utilizado "…el software encase forensic portable… corrido sobre la memoria volátil del ordenador a analizar…entendiendo que fue el mismo que el utilizado por los*

peritos de la UBA …" (ver testimonio de fs. 181/183). Véase, además, que los patrones de búsqueda de información resultaban ser los mismos en uno y otro peritaje (conf. auto de fs. 941 y auto de fs. 1310). ***El informe del Lic. PICCIRILLI de la Universidad Tecnológica Nacional agrega otro dato útil para comparar, en punto a la eficacia del método de búsqueda al que hacen alusión los fiscales*** *(no a la preservación de la evidencia) la labor realizada por los técnicos de la Policía Federal y de la UBA: "no es posible discernir si dentro de la configuración de búsqueda se ha incluido alguna opción que incluya la verificación de archivos ocultos" (respecto de la pericia de la Policía Federal) y "si bien especifica opciones de búsqueda en espacios libres (no utilizados) del disco rígido, no especifica que se haya aplicado la opción de búsqueda sobre archivos ocultos"(respecto de la pericia de la UBA) -ver fs. 273 a 275-.4°C) El análisis efectuado por el Fiscal de Cámara en los puntos IV a VI de su dictamen sostiene, en resumidas cuentas, que no es "lógico" pensar que al tiempo de practicarse la primera pericia (Policía Federal) se introdujeran en las computadoras secuestradas 7546 archivos para que luego se omitiera señalar su hallazgo en el informe presentado al Juzgado. Sin embargo, frente a esa "lógica" del Sr. Fiscal de Cámara, las defensas oponen otra que desde el punto de vista "lógico" tiene igual grado de probabilidad: el primer estudio pericial fue realizado sin darles participación bajo el argumento falso de que se trataba de una operación extremadamente sencilla, urgente y repetible, y el sorpresivo hallazgo de los archivos electrónicos fue efectuado después, en un segundo peritaje, con su presencia pero sobre un material que no controlaron, habiéndose comprobado que no se habían adoptado los recaudos necesarios para asegurar la cadena de custodia de las computadoras, de suerte que los archivos electrónicos, que no estaban originalmente en ellas, habrían sido insertos luego del secuestro. La deducción que hacen los Fiscales acerca de que la evidencia obtenida de las computadoras por los peritos de la UBA no habría sufrido modificación alguna con posterioridad a su secuestro, que en apariencia se sostiene en la tarea del perito Gustavo PRESMAN en el estudio presentado en el marco de la causa n° 1219/09 del Juzgado n° 10 del fuero (ver fs. 244/248) es controvertible, por un lado, debido a que el propio perito PRESMAN fue categórico al reconocer que se había violado la cadena de custodia del material mientras estuvo a disposición de la División Apoyo Tecnológico de la Policía Federal(ver su declaración de fs. 249) y, por otro, porque no asegura que los archivos electrónicos que luego hallaron los técnicos de la UBA hubieran estado originalmente en las computadoras, y esto último, que es precisamente aquello que habían denunciado las defensas y a lo que daba pábulo lo advertido por estos últimos profesionales (al señalar al deficiente forma de preservación de la evidencia),* ***aparece ahora corroborado por la conclusión del nuevo peritaje practicado por el Licenciado en Sistemas Darío PICCIRILLI de la Universidad Tecnológica Nacional: "no se puede afirmar inequívocamente que el contenido encontrado por los peritos de la Universidad de Buenos Aires era el mismo que al momento del secuestro"*** *(ver fs. 267/284 de este incidente).*

Y por si fuera poco, no ya sobre la preservación sino directamente sobre la autenticidad misma de la evidencia, se advierte el hallazgo de numerosos archivos creados con anterioridad al secuestro de las computadoras que aparecen modificados en el tiempo en que éstas estuvieron a disposición de la

División Policial, o bien que fueron directamente creados en ese espacio de tiempo ***(ver punto F del informe pericial del Lic. PICCIRILLI -Universidad Tecnológica Nacional- entre fs. 278 y 281 y el Anexo VII allí mencionado que tenemos a la vista).****La importancia de dicho hallazgo no es menor pues, de la lectura de dicho anexo, puede advertirse la existencia de archivos creados o modificados en aquel lapso que se refieren, en concreto, a algunas de las operaciones presuntamente delictivas que el Sr. Fiscal mencionó en la presentación efectuada a fs. 14.605 a partir de lo que había informado la UBA (vgr. "…la compra de material rodante ferroviario a España y Portugal … re concesión del Ferrocarril Belgrano Cargas… contrato de consultoría…"). Así, y más allá de cuál pudo haber sido la entidad o la extensión de la operatoria que los afectó, lo cierto es que este sólo aspecto –su modificación en un tiempo en el cual debieron permanecer imperturbables- impide a la magistratura acordarles algún valor probatorio. En este sentido, y a simple modo de ejemplo, pueden evocarse los siguientes datos obtenidos por el perito:*

PC5 – MODIFICADOS – PARTICION 1

Nombre	Encontrado en	Tamaño	Modificado	Creado	Tipo
Banco Nación	G:/General/General/00/Proyectos/00 Comp Esp y Port Mat Ferrov.	Carpeta	29/7/2009	10/6/2009	Carpeta de Archivos
Material de Trabajo Juan	G:/General/General/Licitaciones/F Belgrano Cargas	Carpeta	29/7/2009	10/6/2009	Carpeta de Archivos
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	97 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File

PC5 – MODIFICADOS – PARTICION 2

Nombre	Encontrado en	Tamaño	Modificado	Creado	Tipo
Banco Nación	G:/General/General/00/Proyectos/00 Comp Esp y Port Mat Ferrov.	Carpeta	29/7/2009	10/6/2009	Carpeta de Archivos
Material de Trabajo Juan	G:/General/General/Licitaciones/F Belgrano Cargas	Carpeta	29/7/2009	10/6/2009	Carpetade Archivos

PC5 – CREADOS – PARTICION 2

Nombre	Encontrado en	Tamaño	Modificado	Creado	Tipo
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	97 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File
Thumbs.db	G:/General/General/Varios/Carpetas Desactualizadas 00/Compra a España y Portugal	5 KB	29/7/2009	29/7/2009	Data Base File

PC8 – B- MODIFICADOS – PARTICION 2

Nombre	Encontrado en	Tamaño	Modificado	Creado	Tipo
Tomo # Legislación del proceso li …	G/General/3/3/Alstom/Material para informe de consultoria/informe 1/ 01 Belgra …	Carpeta	30/7/2009	16/2/2006	Carpeta de Archivos

No es posible pasar por alto, en este punto, todos los párrafos dedicados en el dictamen fiscal obrante a fs. 343/352 para relativizar aquellas advertencias que habían hecho los profesionales de la UBA acerca del estado del material recibido para estudio, minimizándolas al punto de sostener que lo único que dichos profesionales habían cuestionado era que no se encontraban resguardadas "las tomas de corriente eléctrica de las computadoras", afirmación que llevó a decir a renglón seguido que "… para ponerlo ´enroman paladino´: es imposible que un solo archivo y mucho menos 7546 documentos sean ingresados por el puerto de alimentación eléctrica …". ***A la par de las explicaciones que al respecto brindó el perito PICCIRILLI, no puede soslayarse que las advertencias de los profesionales de la UBA no se limitaron al punto señalado por el Fiscal.*** *Por el contrario, como se dijo antes, el énfasis fue puesto en la falta de "la documentación correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indicase expresamente fechas y horas en que dicho material fue obtenido por primera vez y las fechas y horas en que el mismo fue utilizado en previa/s pericia/s si las hubiere, como así también los métodos informáticos utilizados para evitar la contaminación de la prueba" ver fs. 12.318 vta./12.319).En esas advertencias los peritos de la UBA no se refieren a la ausencia de fajado de los puertos de alimentación eléctrica a los que alude el Sr. Fiscal de Cámara como si sólo eso hubieran dicho, sino a las circunstancias de lugar, tiempo y modo en que las computadoras secuestradas fueron manipuladas antes de que aquellos peritos las tuvieron a su disposición luego para estudio. Y entre esas circunstancias se encuentra, entre muchas otras que hablan de los rudimentarios métodos empleados por la Policía Federal, una de vital importancia: a diferencia de los peritos de la UBA, que emplearon sistemas bloqueadores de escritura de hardware (marca Tableau, tecnología SCSI, en todos los casos salvo en dos, que se empleó un Live CD de Linux denominado Knoppix) para "…evitar que al acceder a los discos rígidos se inserte información espuria contaminando la evidencia..." (conf. fs. 12.319*

*y12.320) los peritos policiales no utilizaron ningún sistema de ese tipo (**conf. pericia del Lic. PICCIRILLI de la UTN a fs. 267/284** y del Ing. PRESMAN a fs. 44/248).De los rudimentarios métodos utilizados por la Policía Federal Argentina para la preservación de la evidencia es muestra también el hallazgo posterior de numerosos "archivos con fecha de modificación anterior a la fecha de creación" lo que resulta una "inconsistencia…inexplicable desde el punto de vista técnico" **(ver informe del Lic. PICCIRILLI –Universidad Tecnológica Nacional- a fs. 281 y Anexo VIII al que remite).**Véase además que el propio perito PRESMAN, que citan los Sres. Fiscales, da cuenta en su informe en copia obrante a fs. 244/248 que "…del análisis de los informes técnicos periciales existentes a fs. 1093 y 1098 del Expte. 12446/2008 del Juzgado Federal n° 7, se observa que en ninguno de ellos se describe con claridad las operaciones técnicas utilizadas, herramientas empleadas ni se hace mención a la utilización de bloqueadores de escritura. Tampoco se precisan las fechas en que se realizaron las operaciones…", como así también que "…las alteraciones a las que se refiere… serían producto de una negligencia operativa en las pericias informáticas efectuadas…".Por último, dada la insistencia de los Sres. Fiscales en punto a que ninguno de los archivos creados o modificados durante el período en que las computadoras estuvieron a disposición de la División Apoyo Tecnológico de Policía Federal fueran archivos electrónicos correspondientes a mails o correos electrónicos, **se advierte también de la lectura del Anexo VII de la pericia practicada por el Lic. PICCIRILLI de la Universidad Tecnológica Nacional, que ello no sería así, a poco que se repara en el listado correspondiente a la PC6 – ACCEDIDOS – PARTICIÓN 1, y PC6 – CREADOS – PARTICIÓN 1,** del citado Anexo VII, entre otros. No es que cándidamente se pretenda la más alta sofisticación en las prácticas de informática forense*
("se tornan impracticables debido al cúmulo de causas a trabajar y al tiempo que demora aplicar estas recomendaciones en cada caso" -ver declaración del Inspector Víctor Aquino a fs. 182-) desconociendo las limitaciones que pueden manifestarse en el orden local, sino simplemente que se preserve la prueba (conf. arts.184, inc. 2°, y 261 primer párrafo, del CPPN) en lugar de contaminarla o poner en duda su contenido mediante operaciones desaprensivas sustraídas al control de las partes. Para mostrar el contraste entre ese proceder irregular y el actuar correcto y respetuoso del derecho de defensa, es forzosa la comparación con el imprevisto que aconteció al momento de practicarse el estudio de la UBA. Relató Rodolfo Baaer que al querer utilizar un dispositivo de hardware bloqueador -para tomar evidencia sin alterarla- se encontraron con que en uno de los casos ese dispositivo no soportaba la tecnología, por lo que, una vez avalado por los peritos de parte ,se empleó un software para acceder (ver declaración testimonial a fs. 172/173).De lo dicho hasta acá se desprende que las prácticas llevadas adelante por la Policía Federal Argentina sobre el material secuestrado contaminaron la evidencia, convirtiendo lo que el juez instructor había considerado una "operación pericial extremadamente simple" y "repetible" en una medida irreproducible. De haberse dado la debida intervención a las defensas para que pudiesen presenciar y controlar aquellas prácticas, tal como sucedió con el estudio de la UBA, el inconveniente podría haberse superado, pero ello no sucedió. Se violó la regla de garantía contemplada expresamente por el artículo 201 del código de rito -como derecho constitucional reglamentado- lo que cual conduce a la necesaria aplicación de la sanción que allí mismo

también se establece (cfr. Maier, ob. cit., pág. 163).Es por eso que se afirma que la peritación recién adquiere estado procesal cuando se cumplen todas las formalidades previstas por la ley (Clariá Olmedo, Jorge A. "Derecho Procesal Penal", Tomo Segundo, Marcos Lerner, 1984, Córdoba, pág. 401); y que "cuando la ley impusiera alguna formalidad especial para su producción, relacionada con el derecho de defensa de las partes, la observancia de ella será también condición sine que non para que la prueba que se obtenga pueda ser regularmente incorporada. Por ejemplo, si se tratara de un acto definitivo e irreproducible, se deberá notificar previamente a los defensores (arts. 201)…" (Cafferata Nores, José I. "La Prueba en el Derecho Penal", Editorial Depalma, Buenos Aires, 1994, pág. 18).Por más que pueda comprenderse la frustración evidenciada por los representantes del Ministerio Público Fiscal, de quienes es dable esperar igual esfuerzo y pasión por el resultado eficaz de las investigaciones de hechos de corrupción como por que éstas se lleven a cabo en correcta forma correcta (pues no se trata de terceros observadores sino de sujetos procesales especialmente comprometidos por imperio constitucional con la construcción, dentro del marco de la legalidad, de la verdad procesal entendida como meta del procedimiento), las restricciones impuestas a la actividad probatoria a través de las aludidas reglas de garantía carecerían de sentido si la inobservancia de los preceptos no provocara la inadmisibilidad de incorporar al proceso los elementos de prueba obtenidos ilegítimamente, o bien excluirlos, si ya fueron incorporados (Maier, ob. cit., pág. 695). Es que "…como resulta notorio, las razones de conveniencia -eventualmente, eficacia o celeridad- ceden -y deben ceder siempre- ante las garantías constitucionales en una estricta aplicación de éstas…" (María Angélica Gelli, "Constitución de la Nación Argentina, Comentada y Concordada", Editorial La Ley, Buenos Aires, 2008, Tomo I, pág. 296).Sin caer en una moralina judicial impropia para quien pretende ejercer la magistratura con seriedad, este Tribunal, en su anterior intervención, advirtió las consecuencias que podían derivarse del planteo constitucional que hacía la parte. A ello se debió que encomendase avanzar en el conocimiento de lo sucedido con el material secuestrado. Si la tarea realizada en primera instancia consolidó los indicios de violación de las reglas de garantía no es posible poner a cargo del titular de esas garantías la prueba fehaciente de su cumplimiento por parte del Estado y, mucho menos aún, justificar su inobservancia por el resultado buscado, incluso si se coincide con alguna de las ideas que con la elocuencia que lo caracteriza puso de resalto el Sr. Fiscal de Cámara en su dictamen obrante a fs. 343/352, desde que lo contrario importaría hacer prevalecer un principio de "in dubio pro prueba" contrario a la autolimitación que el Estado por ley se impuso. En el presente caso existían dos cosas que resultaba muy sencillo hacer y que se omitieron sin una justificación válida: una notificación a la defensa que manda la ley bajo pena de nulidad (arts. 200, 201 y258, segundo párrafo, del CPPN) y la preservación adecuada de la evidencia que pretende usarse contra un individuo, exigida también por la ley (arts. 184, inc. 2°, y 261 primer párrafo, del CPPN). Sólo es permitido arribar a la verdad por los medios y en la forma que la ley lo autoriza. Ese es el sentido de las reglas de garantía y si ellas no se han respetado, es misión ineludible de la magistratura, así declararlo (arts. 166, 167, inc. 3°, y ccdts. del CPPN).Para finalizar, podría recurrir el Tribunal al mismo autor cuya doctrina en parte recoge el Sr. Fiscal de Cámara en su memorial cuando, frente a la pregunta acerca de

qué opciones tienen los jueces, Guariglia responde: "Cuando la justicia penal no está a la altura de su propia retórica y las normas que reglamentan su actuación son circunvaladas o ignoradas sin mayores consecuencias, el derecho simplemente se vuelve deshonesto. Y un derecho deshonesto es un mal derecho" (Guariglia, Fabricio "Concepto, fin y alcance de las prohibiciones de valoración probatoria en el procedimiento penal. Una propuesta de fundamentación", Editores del Puerto, Buenos Aires, 2005, pág. 124).Sin embargo, frente al discurso a través del cual, por no hacer caso omiso a lo que la ley manda, se nos recrimina por adelantado "en roman paladino" seguir un supuesto "evangelio" del "fundamentalismo garantista" y utilizar una "máquina de triturar … el más elemental sentido de sensatez y raciocinio" con cuyo uso " … lo que queda a la vista del ciudadano de a pie son los malhechores victoriosos y una justicia desbaratada …" (ver acápite VII del memorial de fs. 343/352), es inevitable señalar que ideas o expresiones como éstas y otras tantas utilizadas por el Sr. Fiscal, aparecen cuando se acaban los argumentos y se hace necesario ocultarlo alimentando públicamente sospechas o interpretaciones torcidas sobre la intención de los órganos judiciales que -en definitiva- hacen respetar el ordenamiento jurídico. En el "roman paladino" que utilizó la propia Corte Suprema de Justicia de la Nación "… demasiados problemas han ocasionado a la república las represiones ilegales del pasado para que ahora se intente la represión de los delitos contra la administración o que perjudiquen el erario público por caminos aparentemente revestidos de legalidad pero en definitiva ilegales … con el agravante de provenir de los encargados de asegurar el imperio del derecho y la consiguiente paz social. No es cuestión de satisfacer a la opinión pública presentándose como adalides de la lucha contra la corrupción administrativa sino de aplicar rigurosamente el ordenamiento jurídico, sancionando mediante la utilización de los medios legítimos suministrados por el derecho, a aquéllos que lo violan..." (sentenciaS.471.XXXVII, del 20/12/2001).5°) En cuanto a los efectos de la nulidad que habrá de decretarse, ella queda limitada a la evidencia recogida en las pericias practicadas a fs. 1093/1095 y fs.1097/1099, y a lo actuado en consecuencia, en especial, la pericia realizada a fs.12.318/12.323, pero en modo alguno afecta la validez de la causa. La investigación por enriquecimiento ilícito del imputado Ricardo Jaime y sus consortes de causa deberá proseguir con lo que resulte de las múltiples probanzas ya existentes en la causa o que se alleguen a ésta en el futuro, y que resultan independientes a la obtenida en dichas pericias (art. 172 del CPPN).Por lo expuesto, corresponde por confirmar la anulación de los peritajes producidos a fs. 1093/1095 y fs. 1097/1099 por la Policía Federal y a fs. 12.318/12.323 por la UBA (con sus respectivos anexos), debiendo proseguirse con la investigación del delito de enriquecimiento ilícito denunciado.
En mérito de los argumentos expuestos, el Tribunal RESUELVE

CONFIRMAR
La resolución de fs. 288/309 en cuanto anula los peritajes producidos a fs. 1093/1095 y fs. 1097/1099 por la Policía Federal y a fs.12.318/12.323 por la UBA (con sus respectivos anexos), debiendo proseguirse sin esos elementos con la investigación del delito de enriquecimiento ilícito denunciado.

Regístrese, hágase saber a la Fiscalía de Cámara y devuélvase al Juzgado de Primera Instancia para que se cumpla con el resto de las notificaciones. Sirva la presente de atenta nota de envío. Jorge L. Ballestero Eduardo G. Farah.
Ante mí: Eduardo Ariel Nogales – Prosecretario de Cámara.

Nota: los resaltados me pertenecen

4.2.- **Fallo B** **[FALLO2]** (lo resaltado en el texto me pertenece)

Pre constitución de la prueba informática: AUTOS: BALBI, JUAN JOSÉ C/ CENTRO DE OJOS BUENOS AIRES S/ DESPIDO.

Buenos Aires, 25 de setiembre de 2007

Poder Judicial de la Nación
JUZGADO NACIONAL DE PRIMERA INSTANCIA LABORAL
SENTENCIA N° 9725 EXPEDIENTE N° 27.317/05
AUTOS: BALBI, JUAN JOSÉ C/ CENTRO DE OJOS BUENOS AIRES S/ DESPIDO.
Buenos Aires, 25 de setiembre de 2007
Y VISTOS: Estos autos en estado de dictar sentencia, a través de los que el actor, persigue el cobro de los importes que detalla en la liquidación de la demanda y que corresponden a los distintos conceptos allí señalados. Fundamenta sus pretensiones en la ruptura de la relación laboral que imputan a la actitud arbitraria de la empleadora……
"Que la pericia en sistemas de fs.263 y siguientes, dictamina la autenticidad de los mails o correos electrónicos intercambiados entre el actor y el Dr. Suárez, lo que se encuentra confirmado a su vez, ***con la declaración de fs.423, de Piccirilli, quien reconoce las fs. 59/77 del cuadernillo obrante en el sobre N° 3889.*** *De estas circunstancias se desprende que hubo tres mails remitidos por Balbi durante el mes de julio del 2005. . . . . ."*

Nota: el resaltado me pertenece

4.3.- **Fallo C** - **[FALLO3]** (lo resaltado en el texto me pertenece)

Cámara Federal de Casación Penal

REGISTRO Nro: 337/13

Causa Nro. 16339 -Sala IV– C.F.C.P. "GIL, Juan José Luis s/ rec. de casación"

– *///la ciudad de Buenos Aires, a los veintidós (22) días del mes de marzo del año dos mil trece, se reúne la Sala IV de la Cámara Federal de Casación Penal integrada por el Juan Carlos Gemignani como Presidente, los doctores doctor Mariano Hernán Borinsky y Gustavo M. Hornos como Vocales, asistidos por la Prosecretaria de Cámara Doctora Jesica Y. Sircovich, a los efectos de resolver el recurso de casación de fs. 2968/2971, de la presente causa nro. 16339 del registro de esta Sala, caratulada: "GIL, Juan José Luis s/recurso de casación"; de la que RESULTA:*

I. Que el Tribunal Oral en lo Criminal Federal de Santa Fe, en la causa Nº 239/10 de su registro, en la sentencia de fecha 10 de septiembre de 2011, cuyos fundamentos se dieron a conocer el día 13 del mismo mes y año, resolvió, en lo que aquí interesa:

1) RECHAZAR el planteo de nulidad efectuado por la defensa técnica del imputado en oportunidad de formular su alegato; y 2) CONDENAR a Juan José Luis GIL como autor penalmente responsable de los delitos de amenazas agravadas (art. 149 bis 1er párrafo del Código Penal) y coacciones agravadas (art. 149 bis 2º párrafo, art. 149 ter inc. 1 y 2 a) del Código Penal, -dos hechos- en concurso real, art. 55 del C.P.), imponiéndole en tal carácter la pena de CINCO AÑOS DE PRISIÓN, inhabilitación absoluta por el mismo tiempo del de la condena, y accesorias legales (arts. 12 y 19 del Código Penal).

II. Que, contra los puntos citados de dicha resolución, los doctores Gonzalo Pablo Miño y Mauricio C. Bonchini, abogados defensores de Juan José Luis GIL, interpusieron recurso de casación a fs. 2968/2971. El recurso fue concedido a fs. 2974/2975 y mantenido a fs. 2986.

III. Que la defensa de Juan José Luis GIL se agravió, en primer término, del rechazo del planteo efectuado en oportunidad de alegar, referido a la nulidad de la prueba recogida en el domicilio de su asistido, por entender que los soportes informáticos secuestrados en dicha ocasión no fueron debidamente conservados mediante el sistema de sellado electrónico, exponiéndolos a posibles contaminaciones. Al respecto, argumentó que en lo atinente al secuestro y peritación de los elementos de autos, no hay ningún informe que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indiquen las fechas y horas en que dicho material fue obtenido por primera vez, ni los métodos informáticos utilizados para evitar la contaminación de la prueba. ***Destacó que al iniciarse la pericia, y en el momento de***

entregar el material a peritar, el juzgado no proveyó la correspondiente documentación respaldatoria del mantenimiento de la cadena de custodia.

Asimismo, la parte recurrente refirió que "[a] simple vista puede observarse que el material recibido del Juzgado no se encontraba adecuadamente protegido para su uso, ya que los puertos de alimentación eléctrica no estaban adecuadamente inhabilitados". *En tal sentido, aseveró que "…en virtud del estado del material a periciar que [les] fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia"; no sólo en lo tocante a la ausencia de fajado en los puertos de alimentación eléctrica, sino también en las circunstancias de lugar, tiempo y modo en que las computadoras secuestradas fueron manipuladas antes de que aquellos peritos las tuvieran a su disposición para estudio. Resaltó que "…la notebook Oliveti Olibook 800 fue peritada en Provincia de Buenos Aires, cuando su secuestro fue en la localidad de Reconquista pcia de Santa Fe"; como así también que "…en la pericial NO se encontraron archivos relacionados a los mails. Solo se encontraron restos de archivos, sin poder identificar los mismos. Lo que llama la atención es que de una computadora con capacidad de 80 G se encontraron 160 G de archivos (fs. 1073)" (énfasis eliminado).*

Por otro lado, la defensa cuestionó la materialidad de los hechos, afirmando que de los mensajes de correo electrónico que sirven de imputación, uno no existe y el otro fue enviado desde la ciudad de Paraná, y no de Reconquista donde reside su asistido. Señaló que "…el primer mail, data del día 26 de marzo de 2009 y obra a fs. 2 a 4 de autos. Sorprendentemente, no existe constancia alguna de este mail, ni de su envío, ni se peritó el mismo, ni se sabe de dónde salió. No sabemos desde que IP se lo envió. No hay registros, no existe". Añadió que "…la testigo Cabas (periodista), en la audiencia del día 9 de agosto de 2012, afirmó haber recibido este mail el día 1º de marzo de 2009, enviado el 28 de febrero de 2009, no sólo 7 días antes de la creación de la cuenta, sino 25 días antes de su primer envío".

Respecto del segundo mail, explicó que "…es del día 20 de mayo de 2009 y obra a fs. 48 a 51 de autos. Este, es el mail peritado y se determina que es enviado desde la IP 190.183.19.79. Para el envío de este mail se utilizó la empresa Gigared S.A., quien a fs. 177/187 y luego copia agregada a fs. 189/199, informa que tal empresa NO brinda servicios en la ciudad de Reconquista (ver oficio Nº 409/09 de fs. 299) y que la IP en cuestión fue asignada a la ciudad de Paraná". Destacó también que "[l]a planilla de Yahoo […] no sólo NO registra movimiento la cuenta negritovega16@yahoo.com.ar el día 26 de marzo de 2009 (fecha de envío del primer mail) sino que el día 20 de mayo de 2009 a dicha cuenta se le asigna una IP 190.183.19.79 que tuvo entrada en la ciudad de Paraná".

La defensa puntualizó, por añadidura, que según surge de la planilla de Yahoo, a la cuenta negritovega16@yaoo.com.ar se ingresó en diferentes días desde diferentes IP, pertenecientes a tres personas distintas, de lo que se sigue en opinión de dicha parte- que las tres personas tenían el nombre de usuario y la clave del mail. Señaló, además, que no puede ser prueba incriminante para

el justiciable que la referida cuenta haya sido creada desde un ciber a pocas cuadras de su casa, ya que cualquiera la pudo crear. Consideró que "[e]n esta afirmación se invierte la carga de la prueba, obligando al justiciable a probar su inocencia".

La parte impugnante resaltó, a su vez, que de todas las presuntas víctimas que declararon como testigos, ninguno recibió directamente los mails presuntamente amenazantes, sino que todos ellos los recibieron mediante reenvíos de amigos y testigos en la causa. Y agregó que "quienes si lo reciben son Viviana Acosta y José Quintana, que, sorprendentemente […] no han declarado en estos autos, ni siquiera fueron citados por la parte acusadora". Cuestionó la verosimilitud asignada a los dichos de los testigos Pietropaolo y Gauna por entender que los comprenden las generales de la ley, ya que en las respectivas audiencias manifestaron claramente su enemistad con GIL.

Finalmente, criticó que se haya tomado como elemento incriminante la circunstancia de que su asistido tuviere fotocopias de la causa 050, destacando que mucha gente –no sólo GIL- tenía copias de dicho expediente, toda vez que "[l]a testigo Pirani, TESTIGO DE LA QUERELLA, en la audiencia del día 9 de agosto de 2012, manifestó que la Asoc. Norte Amplio, el Fiscal Salum y el Dr. Hernández daban conferencias y charlas sobre la causa 050 y que en dichas charlas y conferencia se daban copias de la causa".

Concluyó afirmando que no se alcanzó, a partir de la evidencia colectada en el debate, el estado de certeza requerido para el dictado de una condena. Señaló que "dicha certeza no se satisface con elementos de escaso o nulo valor probatorio, como los presentados a lo largo del debate, insuficientes para desvirtuar las protestas exculpatorias del acusado".

La defensa hizo reserva del caso federal.

IV. Que en el término de oficina, el doctor Javier Augusto De Luca, Fiscal General a cargo de la Fiscalía N° 4 ante esta Cámara Federal de Casación Penal, presentó el dictamen que obra glosado a fs. 2990/2993, en el cual requirió fundadamente el rechazo del recurso de casación deducido por la defensa.

V. Que superada la etapa prevista en los arts. 465, último párrafo y 468 del C.P.P.N., de lo que se dejó constancia en autos (fs. 3033), quedaron las actuaciones en estado de ser votadas. Efectuado el sorteo de ley para que los señores jueces emitan su voto, resultó el siguiente orden sucesivo de votación:

Doctores Mariano Hernán Borinsky, Gustavo M. Hornos y Juan Carlos Gemignani.

El señor juez doctor Mariano Hernán Borinsky dijo:

I. Liminarmente, cabe recordar que según se desprende de los considerandos de la sentencia, el tribunal a quo entendió acreditada (a partir de la prueba producida en el debate oral) "…la existencia y circulación en el ámbito de la ciudad de Reconquista de dos mails de contenido amenazante y coaccionante que fueran enviados desde la cuenta de correo negritovega16@yahoo.com.ar cuya IP de creación es 190.138.170.218, la cual fuera asignada entre las 10:22 y 12:22 horas del día indicado al cliente de Arnet 1601317, cuya cuenta se encontraba otorgada al Señor Juan Carlos Arce con domicilio comercial en el local de Telecabinas ubicado en la dirección mencionada precedentemente (fs. 237). De la misma forma se ha probado, que dicha cuenta fue creada bajo el nombre de fantasía 'Néstor Fernández'"; como así también que "que tales mails que llevaban por título: 'La hermandad avisa entes de hacer algo' en el primer caso (fs. 2/4) de fecha 26 de marzo de 2009; y 'El Misterioso suicidio de un hermano' en el segundo (fs. 48/51), este último de fecha 20 de mayo de 2009, fueron enviados en forma anónima y reenviados a través de interpósitas personas con el objetivo de amenazar y coaccionar a un grupo de personas –en su mayoría- relacionados con el ámbito de defensa de los derechos humanos y con el sistema educativo en el ámbito de la ciudad de Reconquista, como asimismo a testigos, querellantes y funcionarios judiciales que actuaban en el marco de la causa 050/06, en trámite ante el Juzgado Federal de dicha ciudad, en la que se investigaban delitos de lesa humanidad y que tenían como fin esencial, obstaculizar el normal desarrollo de la referida causa".

Los sentenciantes responsabilizaron al imputado Juan José Luis GIL por el envío de los mails amenazantes. En el primero de los mensajes mencionados se hace referencia a una organización denominada "La Hermandad", sobre cuya integración existiría interés por parte de los "corruptos funcionarios federales" responsables de la detención de policías por crímenes de lesa humanidad. Sobre el punto, el mail expresa: "[n]o esperen que les proporcionemos datos logísticos a nuestros enemigos, hoy ha cambiado por completo el escenario del combate, en los 70 ellos nos conocían y sabían quiénes éramos, hoy NO.

Pero lo más interesante es que nosotros SI los conocemos, sabemos donde viven, donde trabajan, cuáles son sus familiares y hasta los hemos infiltrado, no es oro todo lo que reluce". En cuanto a los fines de la organización, se consigna que "…hemos venido a aclarar la situación y hacer justicia, la nuestra por supuesto". Se agrega, asimismo, que la organización tiene "…detalles de las reuniones en la Mutual de los judiciales donde Zanutti, Borsatti, Medina, etc. se reunían en la parte superior antes de que 'copen' el SITRAM, debemos agradecer a Borsatti por facilitarnos la tarea al colocar en sus libros la lista de colaboradores". El mensaje contiene también críticas al accionar de "El juez VALIENTE y su ladero el Fiscal SALUM". Con relación a este último, se afirma que es "…un traidor a su pueblo porque sabe que todo es una mentira sin sustento". Y sobre los testigos en los juicios por delitos de lesa humanidad, se pregunta "¿Harían lo mismo que hicieron con Julio López si alguno duda o no quiere seguir mintiendo". Por añadidura, se incluyen otras frases amenazantes, entre ellas las siguientes: "No es algo práctico hacerse muchas preguntas sobre La Hermandad, es perder el tiempo y en una de esas algo

más"; "Ensañarse con militares y policías viejos es fácil, ahora está La Hermandad.
La cosa cambió".

En el segundo mensaje el autor se dirige al Doctor Gabriel Hernández, afirmando que tiene en su poder "…cierta documentación que lo compromete muy seriamente en el armado de toda (sic) las mentiras de las hermanas Pratto", y advierte que "Su problema es que creyó contar con un paragua protector hasta la eternidad y se ha ensañado con los policías injustamente detenidos, dicho sea de paso lo mismo creyeron Echegoy, Borsatti, Pietropaolo, Medina, Córdoba, Maulín, Nalli, Micheli, Scarpín, Zotelo, Zanuttini, Emilse Deseta, Soledad Zalazar, Jacinto 'el inutil' Esperanza, Marta 'Enculada' Speranza, etc., y ahora ven que todo se termina y ya vendrán los tiempos de revancha y ajuste de cuentas". Por otro lado, se afirma en el mail que "Los ilustrados del juzgado federal y la fiscalía también van a ser tenidos en cuenta en el momento de saldar las cuentitas y hacerles ver que en la vida todo se paga […] por más que Valiente y Salum hoy se hagan los malos, ellos van a tener que dar cuenta de sus actos como así también algunos secretarios, y no hablamos de denuncias o juicios penales, eso es perder el tiempo y nunca se está seguro de nada. Si algo les pasa a los policías detenidos o al hermano de la FAA, ustedes serán ejecutados". El mensaje dice, asimismo: "Para nosotros es claro que la primer muerte de este acto la produjeron Uds., toda la banda, nadie queda fuera del círculo de fuego, sólo falta decidir cuándo será más conveniente comenzar a vengar al Hermano Fleitas. Que en paz descanse, nosotros terminaremos el trabajo".

II. Sentado cuanto precede, se analizará en primer término el agravio de la defensa referido al rechazo del planteo de nulidad efectuado en el debate contra la validez de la prueba informática secuestrada en el domicilio de GIL.

Al resolver sobre el planteo de mención, formulado por la asistencia técnica del imputado en su alegato, el tribunal a quo explicó que "…en el acta de procedimiento que refleja la obtención de la notebook (fs. 315), se describe el modo en que se produjo el secuestro y aseguramiento, rezando la misma: 'Seguidamente se continúa con la habitación denominada ESTUDIO B encontrando un escritorio de madera del cual se secuestra una (1) notebook marca OLIVETTI S/N B2339ah1207240180 con cable de 220 v, acondicionándola dentro de un sobre blanco con la inscripción COMPUTADORA PORTATIL, el cual es cerrado y firmado por los actuantes". Se señaló también que "…dicho secuestro se produjo en presencia de los testigos convocados al efecto, Sres. José Luis Cofré Villagra y Juan José Blanco quienes al deponer durante el debate, fueron contestes en afirmar haber presenciado el secuestro de la notebook la cual reconocieron al serles exhibida, ratificando además el contenido del acta de procedimiento obrante a fs. 313/317 y su firma inserta en la misma".

Asimismo, los sentenciantes valoraron que según se desprende del acta obrante a fs. 333/334vta., "…dichos efectos –secuestrados y asegurados de la forma descripta en el acta de procedimiento- fueron enviados al juzgado

interviniente y controlados en esa sede judicial en presencia del Dr. José Avelino Donatelli y los testigos Andrés Leonardo Alvarez y Cesar Daniel Berlanda, para ser nuevamente resguardados en los mismos sobres, los cuales fueron cerrados, permaneciendo a partir de dicho momento bajo custodia del juzgado de instrucción interviniente". Como así también que "…los referidos efectos, fueron debidamente resguardados en presencia del personal actuante y de los testigos de procedimiento convocados al efecto y en dicha condición fueron entregados al Juzgado Federal de Reconquista, los cuales fueron controlados por el propio Actuario y dos testigos, sin que se haya dejado consignado en dicho instrumento la detección de alguna anormalidad; de esa forma llegaron a poder de la Policía de Seguridad Aeroportuaria para su peritación, consignándose en el informe pericial obrante a fojas 836 vta. –y que lleva la firma del Agente Facundo Ramírez-; que la caja que contenía la notebook marca Olivetti Olibook, fue abierta en presencia de testigos y se procedió a verificar el correcto funcionamiento del Hardware, consignándose expresamente el día y horario de dicho acto, como así también a fojas 840 se menciona que se realizó un 'levantamiento forense de la unidad teniendo como resultado 10 Dvd conteniendo los archivos generados por las herramientas de análisis forense, las cuales se deben guardar como copia original del disco investigado…"". Se afirmó, en consecuencia, que "…en caso de haberse pretendido efectuar otro examen pericial sobre el equipo secuestrado, éste habría sido perfectamente posible […] ya que las pericias se efectuaron sobre copias tomadas del mismo, quedando su contenido intacto".

En base a todo ello, los sentenciantes consideraron que "…nunca se perdió la cadena de custodia de los efectos incautados en el allanamiento efectuado en el domicilio de Juan José Luis Gil desde su secuestro hasta la remisión a [ese] Tribunal, como así también que su contenido permaneció intacto".

Esta conclusión no ha sido rebatida por la parte recurrente, toda vez que de la lectura del recurso de casación en estudio se desprende que la defensa se ha limitado a reditar los términos del planteo formulado en el alegato, sin desvirtuar de modo eficaz a los motivos esgrimidos por el tribunal a quo para rechazar dicho planteo.

En este orden de ideas, corresponde tener presente que la evidencia electrónica puede ser alterada, dañada o destruida si se la manipula o analiza incorrectamente, motivo por el cual es preciso adoptar precauciones especiales a la hora de recolectar, preservar y examinar esta clase de evidencia (Cfr. Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte (Association of Chief Police Officers –APCO-): "Good Practice Guide for Computer-Based Electronic Evidence, 4th Official Release Version, pág. 6). El uso de la evidencia digital o electrónica en el proceso penal requiere, pues, la adopción de medidas tendientes a preservar su integridad, desde que en caso de que una parte de la prueba resulte contaminada, toda ella se torna sospechosa y puede ser invalidada.

En tal contexto, se aprecia que –tal como afirmaron los sentenciantes- el tratamiento dado a los efectos secuestrados en el domicilio del imputado –en

especial la computadora tipo Notebook marca Olivetti- resultó adecuado para proteger la integridad del referido elemento de prueba, de modo tal de salvaguardar la legitimidad y el valor probatorio de la evidencia obtenida a partir de la peritación de su contenido.

Vale destacar, en tal sentido, que la introducción y mantenimiento de la notebook dentro de un sobre sellado –que sólo se cerró y abrió en presencia del actuario y los testigos de actuación- aparece como un medio idóneo para lograr dicho propósito, toda vez que imposibilita el encendido del equipo y/o la introducción o eliminación de los datos almacenados en la memoria del mismo, siendo éste también el objetivo que se busca con el sellado de los puertos de alimentación eléctrica, de los puertos USB y de los puertos de entrada de CD o DVD.

De igual manera, se observa que la cadena de custodia no se vio afectada en ninguna de las etapas que fueron desde el secuestro de la computadora hasta su peritación por parte de los técnicos de la Policía de Seguridad Aeroportuaria, y su posterior remisión al tribunal a quo a los efectos de que sirviese como prueba en el debate oral que culminó con el dictado del decisorio que viene recurrido. Prueba de ello es que en el informe pericial obrante a fs. 835/863 vta. se consigna el correcto funcionamiento del hardware, lo que evidencia que la manipulación de la notebook en los traslados de este elemento de prueba desde Reconquista (provincia de Santa Fe) hasta Buenos Aires (y luego de regreso a Santa Fe) no afectó en modo alguno la integridad del equipo, siendo que –además- la defensa no alegó ni demostró que ello haya ocurrido.

En lo que atañe al peritaje en sí mismo, el principal recaudo exigido a fin de salvaguardar la validez del elemento de prueba informático es que se haga una "imagen de trabajo" de la memoria, a fin de preservar la integridad del original (Cfr. DARAHUGE, María Elena / ARELLANO GONZÁLEZ, Luis E.: Manual de informática forense (Prueba indiciaria informático forense), ERREPAR, Buenos Aires, 2011, pág. 132 y ss.). El análisis del contenido de la memoria se lleva a cabo sobre la "imagen" captada, lo que permite mantener intacto al original, a la vez que garantiza la exactitud de los resultados. Ello así, desde que la "imagen" no es una simple copia de archivos de un disco a otro, sino una duplicación bit a bit del contenido de los discos originales (Cfr. MAUTNER, Nicolás / ARONIN, Lisandro S.: "Procedimientos relacionados a la prueba informática: importancia de la computación forense" en Jurisprudencia Argentina, Buenos Aires, Vol. 2004-II, pág. 1143). Dicho recaudo ha sido adoptado en los presentes actuados, toda vez que en el informe pericial mencionado en el párrafo precedente se consignó que los técnicos de la PSA realizaron una copia de seguridad del contenido de la notebook secuestrada en el domicilio de GIL y llevaron a cabo la pericia a partir del contenido de dicha copia, manteniendo – por consiguiente- intacto el original, de modo tal de permitir que el análisis del equipo pudiese reproducirse en una (hipotética) segunda pericia cuya realización no fue solicitada por la defensa.

De todo lo expuesto se sigue que la parte recurrente no ha logrado demostrar la existencia de falencias en el tratamiento de la prueba de cargo que den pie

a la declaración de nulidad que pretende, como así tampoco que del modo en que se manipuló la referida evidencia se haya derivado un perjuicio concreto al debido proceso o al derecho de defensa en juicio del encausado. Por consiguiente, el agravio en trato no puede tener favorable acogida en la presente instancia.

III. Por otra parte, en lo que atañe a los agravios de la defensa referidos al modo en que el tribunal a quo valoró la evidencia incorporada al debate a efectos de tener por acreditada la materialidad de los hechos, corresponde recordar que la Corte Suprema de Justicia de la Nación ha establecido que lo que constituye causal de arbitrariedad es la ponderación de testimonios, prueba de presunciones e indicios en forma fragmentada y aislada, sin haberse efectuado una visión de conjunto ni una adecuada correlación de los testimonios y de los elementos indiciarios (Fallos 311:621 –énfasis añadido-). En tal contexto, se observa que el tribunal a quo llevó a cabo una valoración global de los referidos elementos de prueba, analizándolos de conformidad con el criterio sentado por el máximo tribunal de la República y a la luz de las reglas de la sana crítica racional, arribando de ese modo al estado de certeza requerido para el dictado de un veredicto condenatorio respecto los hechos reprochados a Juan José Luis GIL. Mientras que, en sentido opuesto, la parte impugnante se apartó de los parámetros sentados por la Corte Suprema de Justicia de la Nación a la hora de valorar los elementos de prueba reunidos en autos, toda vez que no efectuó una evaluación global y concordante de la evidencia, sino que analizó los indicios en forma aislada, sin relacionar unos con otros, lo cual arrojó como resultado una conclusión que no encuentra sustento en el material probatorio incorporado al debate.

En efecto, se observa que la evidencia mencionada por el tribunal a quo en los considerandos de la resolución atacada desvirtúa lo afirmado por la defensa en punto a que el primero de los mensajes de correo electrónico amenazantes "no existe" y que el segundo de ellos "fue enviado desde la ciudad de Paraná".

Ello así desde que en lo que atañe al primero de los mails mencionados, su efectiva existencia surge de los testimonios de Jorge Miceli, Pablo Rolón, Raúl Medina, Héctor Borsatti, Carlos Echegoy, Estela Pietropaolo y Silvina Gauna, que afirmaron en el debate haberlos recibido en sus casillas de correo electrónico, siendo que algunos de ellos –los denunciantes- incluso aportaron las copias del mensaje glosadas a fs. 2/4. Las coincidencias que se verifican en los relatos de todos estos testigos en cuanto al contenido del mensaje permiten, en consecuencia, tener por acreditado que el texto y la fecha del mail en cuestión se corresponden con los que obran agregados a las presentes actuaciones. Mientras que en lo tocante al segundo mensaje, la defensa soslayó considerar otras pruebas que dan cuenta de que –contrariamente a lo afirmado por la defensa- la dirección de IP de origen no estaba asignada a la ciudad de Paraná cuando se creó el mail, sino que se informó ello a partir de un error en el horario consignado al momento de requerir información sobre dicha dirección (se utilizó el horario local, en lugar del horario del Meridiano de Greenwich –GMT- mencionado en el informe de Yahoo obrante a fs. 166/167).

Este mismo defecto lógico (análisis aislado, en vez de global, de los elementos de prueba) se aprecia en otros argumentos esgrimidos por la parte recurrente para sustentar su postura contraria a la adoptada por los sentenciantes. Falencia que se advierte en la aseveración de que -según surge de la planilla de Yahoo obrante a fs. 166/167- a la cuenta negritovega16@yahoo.com.ar se ingresó en diferentes días desde diferentes IP, pertenecientes a tres personas distintas, así como a la afirmación de que se tomó como "prueba incriminante" que la cuenta citada se haya creado en un locutorio cercano al domicilio de GIL, invirtiendo la carga de la prueba. Ello así, desde que en el primer caso se soslayó que –tal como explicó el tribunal a quo en la sentencia atacada- se informaron accesos provenientes de direcciones de IP asignadas a domicilios en Paraná, Rosario y Corrientes como resultado de un error de la P.S.A. al solicitar la información con el horario de nuestro país y no con el horario GTM que figuraba en el informe de Yahoo. Mientras que en el segundo caso, la circunstancia de que el local que tenía asignada la IP desde la cual se creó la cuenta negritovega16@yahoo.com.ar fuera cercano al domicilio de GIL no se valoró por sí solo como dato incriminante, sino conjuntamente con otros elementos de prueba, como el testimonio del dueño que manifestó que GIL concurría habitualmente al lugar, y los informes que dieron cuenta de que el nombrado accedió varias veces a la mencionada cuenta.

A ello cabe agregar que no obstante la constatación (posterior) de que los usuarios residentes en los domicilios informados en Paraná, Rosario y Corrientes no guardaban relación con la cuenta negritovega16@yahoo.com.ar, los citados domicilios fueron allanados en el marco de las presentes actuaciones, no encontrándose en los mismos elementos de interés para la investigación. En sentido opuesto, el allanamiento dispuesto en la vivienda del encausado GIL arrojó como resultado el secuestro de la computadora mencionada supra (en el acápite II del presente voto), en la que se encontraron documentos vinculados a las cuestiones incluidas en los mensajes amenazantes atribuidos al imputado.

De igual manera, cabe señalar que la circunstancia de que GIL tuviese en su poder copias de la causa 050 no fue valorada por los sentenciantes como prueba directa de la responsabilidad del nombrado en el envío de los mails, sino como un indicio de culpabilidad, el cual, al ser analizado en forma global con los restantes indicios, permitió concluir -con el grado de certeza requerido para una condena- que GIL era el autor de los mensajes. Así las cosas, se desprende de la lectura del pronunciamiento puesto en crisis que se cumplieron, en autos, los requisitos para que la prueba de indicios pueda sustentar un veredicto condenatorio: se valoraron elementos conducentes para la dilucidación del hecho investigado; existió una relación de certeza directa entre el hecho investigado y los indicios; se verificó pluralidad de indicios contingentes, a punto de convertirse en determinantes; éstos resultaron verdaderos y no se contradijeron con otras pruebas; y –finalmente- se arribó a partir de ellos a una conclusión libre de dudas (Cfr. ALONSO, Silvina Andrea: "De la prueba de indicios en el delito de lavado de activos", en Revista de Derecho Penal Tributario, Rubinzal-Culzoni, Buenos Aires, Tomo 2010-IV, pág. 635).

Con relación a ello, vale recordar que –según surge de los considerandos de la sentencia atacada- el tribunal a quo sustentó su postura incriminatoria respecto de Juan José Luis GIL en numerosos indicios y elementos de prueba. A saber:

• El informe de Yahoo de fs. 166/167, del que se desprende que la cuenta negritovega16@yahoo.com.ar (de la que partieron los mensajes amenazantes) fue creada el 9 de marzo de 2009 a las 11:22:17 GMT, desde la IP 190.138.170.218, por una persona que se identificó como Néstor Fernández. Se informaron también los números de IP, fechas y horarios (GMT) en las que el usuario se "logueó" en la citada cuenta.

• Que la IP de creación había sido asignada, en la referida fecha y horario, al local de Telecabinas cito en la calle Ludueña 1470 de Reconquista, cercano al domicilio de Juan José Luis GIL (quien residía en Ludueña 1428 de la misma ciudad), a lo que vino a sumarse el testimonio del dueño del mencionado local, quien afirmó en el debate que GIL concurrió al lugar en reiteradas oportunidades.

• El informe de fs. 189/191, del que surge que las IP desde las que se accedió a la cuenta negritovega16@yahoo.com.ar (según la planilla de Yahoo de fs. 166/167) fueron asignadas al usuario de la empresa Arnet identificado como "luisgil", cuyo domicilio de facturación se encontraba en la calle Ludueña 1428 de Reconquista (esto es: el domicilio del imputado).

• El resultado de los peritajes realizados sobre la Notebook Olivetti secuestrada en el domicilio citado precedentemente (fs. 835/863 vta., 1051/1052, 1073, 1087/1313), en los cuales se pudo recuperar información que había sido eliminada por GIL, hallándose menciones a un grupo denominado como "La Hermandad", una "grilla de declaraciones" de testigos en la causa 050, un documento titulado "Intimidaciones a la esposa del Fiscal Candioti" (representante del Ministerio Público Fiscal en la aludida causa 050) y otros documentos vinculados a la causa de mención, coincidentes con datos y comentarios contenidos en los mensajes amenazantes atribuidos a GIL.

• Asimismo, los dichos de los testigos Jorge Miceli, Pablo Rolón, Raúl Medina, Héctor Borsatti, Carlos Echegoy, Estela Pietropaolo y Silvina Gauna, que mencionaron conexiones entre el discurso de Juan José Luis GIL en el ámbito educativo en el que se desempeñaba y –en especial- en el marco de un sumario que se le inició, y que derivó en su suspensión, y el texto de los mails recibidos.

La defensa criticó el valor probatorio asignado por el tribunal a quo a las manifestaciones de los testigos de mención, señalando que ninguno de ellos recibió directamente los mensajes amenazantes (de lo que deriva que el texto originario pudo ser modificado al reenviarse), y que en lo tocante a los últimos dos se aplicaban las generales de la ley dada su manifiesta enemistad con su asistido, Juan José Luis GIL. Al respecto, cabe comenzar recordando lo afirmado por esta Sala IV de la C.F.C.P. en punto a que por aplicación del principio de inmediación, no es posible revisar en esta instancia la credibilidad

de los testigos que depusieron en el debate, sino tan solo el razonamiento desarrollado por los sentenciantes para otorgarle mayor o menor valor probatorio a sus manifestaciones (Cfr., mutatis mutandi, causas Nº 13419 "Fredes, Marcos Ariel y otro s/recurso de casación", Reg. Nº 285/12, rta. el 14/3/2012; Nº 11216 "Baima, Héctor A. s/recurso de casación", reg. Nº 483/12, rta. el 10/4/2012; y Nº 12753 "Alonso, José Luis y otros s/recurso de casación", reg. Nº 697/12, rta. el 7/5/2012; entre otras).

Así las cosas, se desprende de la lectura de los considerandos del pronunciamiento que viene recurrido que los sentenciantes no soslayaron la existencia de una relación de enemistad entre GIL y los testigos Gauna y Pietropaolo, no obstante lo cual consideraron verosímiles sus dichos en atención a que los nombrados se refirieron a "…situaciones reales desarrolladas dentro del ámbito educativo en el que tuvieron que interactuar con Gil", destacando sobre el punto que "[l]a virulencia de la situación creada en razón del sumario administrativo seguido contra el imputado y que derivó en su apartamiento de la tarea docente, sumado a los datos concretos que fueron volcados en los mail y que hacen alusión a cuestiones personales e íntimas de las nombradas y en especial de Pietropaolo, permiten vincular al imputado con los mails amenazantes".

Vale recordar, en tal sentido, que los testigos Estela Pietropaolo, Silvia Gauna, Jorge Domingo Miceli, Pablo César Rolón y Héctor Raúl Borsatti hicieron mención a la existencia de coincidencias en la forma y el contenido del discurso del encausado GIL en el sumario administrativo que se le abrió en el ámbito educativo y el texto de los mensajes objeto de las presentes actuaciones, que los llevaron a sospechar que el nombrado podía ser el autor de los mails. Coincidencias que pudieron ser constatadas por el tribunal merced a la incorporación del referido sumario como prueba documental en el juicio oral, y que –valoradas en forma conjunta y global con el resto de la evidencia permiten tener por acreditado que el propio GIL es quien redactó los mensajes de correo electrónico amenazantes cuyo envió se le reprochó.

De todo lo expuesto hasta aquí se desprende, en consecuencia, que los sentenciantes han demostrado, con fundamentos suficientes, la materialidad del hecho atribuido a Juan José Luis GIL, consistente en el envío en forma anónima de dos mensajes de contenido amenazante "…con el objetivo de amenazar y coaccionar a un grupo de personas –en su mayoría relacionados con el ámbito de defensa de los derechos humanos y con el sistema educativo en el ámbito de la ciudad de Reconquista, como asimismo a testigos, querellantes y funcionarios judiciales que actuaban en el marco de la causa 050/06, en trámite ante el Juzgado Federal de dicha ciudad, en la que se investigaban delitos de lesa humanidad y que tenían como fin esencial, obstaculizar el normal desarrollo de la referida causa". Por consiguiente, corresponde rechazar los agravios formulados por la defensa en orden a esta cuestión.

IV. Por los motivos enunciados precedentemente, y de conformidad con lo propiciado por el Fiscal General ante esta Cámara Federal de Casación Penal,

doctor Javier Augusto De Luca, propongo al acuerdo: RECHAZAR el recurso de casación interpuesto a fs. 2968/2971 por la defensa de Juan José Luis GIL, sin costas (arts. 530 y 531, in fine, del C.P.P.N.). Tener presente la reserva del caso federal.-

El señor juez Gustavo M. Hornos dijo:

I. Inicialmente, debo señalar que el recurso de casación interpuesto es formalmente admisible, toda vez que la sentencia recurrida es de aquellas consideradas definitivas (art. 457 del C.P.P.N.), la parte recurrente se encuentra legitimada para impugnarla (art. 459 del C.P.P.N.), sus planteos se enmarcan dentro de los motivos previstos por el art. 456, incisos 1º y 2º del Código Procesal Penal de la Nación y se han cumplido los requisitos de temporaneidad y de fundamentación requeridos por el art. 463 del citado código procesal.

II. He de indicar que comparto y hago propias las fundamentaciones y conclusiones que fueron extensamente desarrolladas en la ponencia del distinguido colega que me precede en orden votación, lo que en consecuencia me lleva a adherir a su propuesta, por compartir plenamente sus fundamentos.

En efecto, tal como ha explicado el Dr. Borinsky, la defensa no ha logrado poner en evidencia la existencia de descuidos o falencias en el tratamiento de los elementos probatorios secuestrados que fueron objeto de examen pericial.

No ha podido demostrar que la notebook en cuestión haya sido objeto de manipulación o que se haya alterado de algún modo su contenido; de modo que los argumentos brindados por el tribunal de juicio para descartar idéntica pretensión no han sido conmovidos. Y por último, tampoco ha podido revelar que se hubiere concretado algún perjuicio efectivo al debido proceso o al derecho de defensa, teniendo en cuenta el adecuado tratamiento dispensado a los elementos de prueba para resguardar su integridad y preservar la legitimidad del contenido obtenido a partir del examen pericial.

En cuanto al segundo aspecto de la queja, relacionado con la valoración que efectuó el tribunal del debate sobre la evidencia utilizada para concluir que se encontraba configurado el hecho atribuido, debo reiterar que comparto las consideraciones del colega que me antecede.

Los juzgadores han efectuado un examen global y abarcativo de los distintos elementos probatorios disponibles, evitando fragmentarlos, de modo de conservar la visión de conjunto y la correlación que, sin espacio para la duda, han arrojado certeramente los distintos indicadores. Ello, como se ha afirmado en el primer voto, ha permitido al tribunal extraer sus conclusiones a la luz de los criterios de la sana crítica racional.

Con relación a los testigos escuchados en el juicio en particular, también comparto los fundamentos del colega en cuanto rechazó los cuestionamientos

relativos al valor probatorio asignado. Ello pues, ese examen es concordante con los deberes de conocimiento que le corresponden a esta Cámara de Casación para revisar ampliamente la sentencia en virtud de los agravios acercados, incluyendo la fijación de la plataforma fáctica; examen que, a su vez, abarca el control sobre la fundamentación del fallo en ese aspecto, es decir: el paso inductivo entre la apreciación de la prueba y la conclusión de la certeza; y la atribución de significado normativo alcanzado en virtud del establecimiento de los hechos juzgados (tal como ya he sostenido anteriormente en las causas nº 4428, "Lesta, Luis Emilio s/recurso de casación", reg. nº 6049, del 23/09/04; y causa nº 4807: "López, Fernando Daniel s/ recurso de queja", reg. nº 6134, del 15/10/04; y reiterado más recientemente en la causa nº 6946.1 "Tarditi, Matías Esteban s/ recurso de casación" reg. nº 15.457 de la Sala I, del 09/03/2010; entre otras).

Ese alcance amplio del derecho al recurso, referido en los precedentes citados, fue luego reconocido por la Corte Suprema de Justicia de la Nación como el único compatible con los derechos y garantías reconocidos en la Constitución Nacional, los Tratados Internacionales de Derechos Humanos y la aplicación que de éstos han efectuado los diversos organismos y tribunales competentes (C.S.J.N.: c. 1757 XL. "Recurso de hecho, Casal, Matías Eugenio y otro s/robo simple en grado de tentativa", Fallos: 328:3399). Y, luego, entre muchas otras, fue reiterado en el precedente "Reynoso" (Fallos: 329:518), en el que recordó que "la Corte Interamericana de Derechos Humanos, por sentencia de 2 de julio de 2004, en el caso "Herrera Ulloa vs. Costa Rica", indicó que el recurso que contempla el artículo 8, inciso "h" de la citada convención [C.A.D.H.], sea cual fuere su denominación, debe garantizar un examen integral de la decisión recurrida, de todas las cuestiones debatidas y analizadas en el tribunal inferior (parág. 165 y 167)".

Lógicamente, los únicos límites impuestos a la revisión de esta instancia se encuentran determinados por la barrera de aquel conocimiento proveniente de la inmediación, lo cual, si bien en general está representado por la impresión que los testigos puedan causar al tribunal, tal como la propia Corte lo ha explicado en el fallo "Casal" ya citado, debe apreciarse en cada caso.

Ello, por cuanto dichas limitaciones de conocimiento se imponen en el plano de las posibilidades reales, y que sólo han tenido los jueces que han estado presentes como jueces en el juicio oral. Aún cuando, claro está, el tribunal de juicio debe dar cuenta circunstanciada de dicha apreciación, y es en este aspecto que ese juicio plasmado en la sentencia es controlable en casación (cf. mi voto en la causa nº 11.222 "Tavarozzi, Gustavo Sebastián y otro s/recurso de casación"; reg. nº 15.513.4, del 09/09/2011; entre otros).

Como anticipé, en el voto del colega que me antecede se ha plasmado acabadamente que el proceder del tribunal anterior se adecuó a las pautas recién reseñadas; en tanto llevó adelante una evaluación de los testimonios de modo global y conjunto con el resto de la evidencia rendida en el debate de modo de obtener una conclusión certera acerca de la comprobación de la

materialidad del hecho atribuido y la responsabilidad que le cupo en él a Juan José Luis Gil.

En suma, corresponde rechazar el recurso interpuesto por la defensa, sin costas, por haberse efectuado un razonable ejercicio del derecho al recurso (arts. 8.2. h, C.A.D.H., y arts. 530 y 531, C.P.P.N.) y tener presente la reserva del caso federal. El señor Juan Carlos Gemignani dijo: Que por coincidir en lo sustancial con el desarrollo efectuado por mis colegas, adhiero a la solución allí propuesta. Tal es mi voto. Por ello, en mérito del acuerdo que antecede, el tribunal, ***RESUELVE:*** *I. RECHAZAR el recurso de casación interpuesto a fs. 2968/2971 por la defensa de Juan José Luis GIL, sin costas (arts. 530 y 531 in fine del C.P.P.N.). II. TENER PRESENTE la reserva del caso federal efectuada. Regístrese, notifíquese y remítase al tribunal de origen, quién deberá notificar personalmente lo resuelto al imputado, sirviendo la presente de atenta nota de envío.-JUAN CARLOS GEMIGNANI- MARIANO HERNÁN BORINSKY - GUSTAVO*
M. HORNOS

CAPITULO 5. CONCLUSIONES. APORTES

5.1.- Conclusiones

En el marco del aporte que realiza la presente tesis en relación a un protocolo para aplicar en las pericias informáticas, incluyendo la actividad forense, se alcanzaron los siguientes resultados:

- ✓ Desarrollo de un protocolo forense informático, posible de aplicar en los distintos fueros de la Justicia Nacional.
  Esto permitirá aportar mayor claridad en el desarrollo del período de prueba, acortar los tiempos procesales en los juicios y permitir a los jueces contar con mejores elementos al momento de valoración de la prueba y producir un fallo o sentencia con mejores fundamentos técnicos.
- ✓ Ordenamiento y normalización de procedimientos periciales en informática, que hoy día, ante un mismo problema, se aplican en forma diferente según la fuerza de seguridad interviniente (Policía Federal Argentina, Gendarmería Nacional Argentina, Policía Metropolitana, Prefectura Nacional Argentina y policías Judiciales)
- ✓ Base procedimental para aplicar en los casos que la Justicia Argentina designe peritos de oficio ad-hoc, los que son sorteados desde una lista oficial que las Cámaras de los distintos fueros poseen. Esto permite generar un estándar de trabajo técnico que facilitará resolver de la misma manera, siempre que se presente el mismo problema técnico.
- ✓ Desarrollo de un protocolo base, que puede ser adoptado por las empresas privadas, con el objetivo de pre-constituir prueba informática de manera confiable e indubitable, al momento de aportar elementos de juicio al juzgado. Esto permitirá ahorrar tiempos y costos para las distintas partes del pleito (actora y demandada) y para el propio Juez.

5.2.- Futuras líneas de investigación para esta tesis

La problemática de la “nube” o “Cloud Computing” presenta nuevos desafíos, los que pueden ser abordados basándonos en el protocolo propuesto en el presente trabajo. Pues, por ejemplo, en el marco del CyberCrimen, ya es posible considerar las siguientes estadísticas:

- La piratería informática, obtiene aproximadamente desde U$S 1 billones hasta U$S16 billones al año (Fuente: McAfee)
- El tráfico de drogas genera una fuente de ingresos de aproximadamente U$S 600 billones al año (Fuente: UNODC)
- Mientras que las actividades dedicadas al CyberCrimen, generan aproximadamente alrededor de U$S300 billones hasta $1 trillón al año (Fuente: varias)

Sobre este tema, Juan Carlos Vázquez (consultor en seguridad de McAfee) opina que *"La ciberdelincuencia ya puede ser considerada como un servicio, es decir, resulta redituable y los hackers ya se encargan de hacer la infraestructura necesaria para los ataques y venderla o rentarla",* **(***08/2013)*

Esta actividad delictiva se encuentra en mayor expansión y en consecuencia con atractivas ganancias, en Europa del Este, principalmente en Ucrania y Rusia, mientras que en América Latina México, Brasil y Colombia son los mercados más exitosos para este delitos (Fuente McAfee).

Por lo tanto, es fundamental atacar en forma organizada y con un adecuado protocolo estas potenciales necesidades, con el objetivo de responder en forma inmediata y efectiva a la problemática que nos propondrán estos futuros planteos, que a modo de ejemplo se describen como:

- ¿Es posible aplicar un protocolo para cadena de custodia de la evidencia informática? Para ello, es necesario considerar en el mismo, los siguientes aspectos:
    - Entender el esquema de trabajo y funcionamientos de las redes en general, y en particular en la WEB y en la DeepWeb. A esta última se le conoce informalmente como Internet profunda o Internet invisible, y consiste en no utilizar direcciones de Internet, sino códigos y aplicar el concepto de pseudodominio de nivel superior (red .onion, la cual fue creada por la Armada de los Estados Unidos como una prueba, pero que ahora es aprovechada por delincuentes cibernéticos.)
    - Acceder a las redes y capturar el tráfico de la misma. En general, en Argentina, es necesario que se realice esta actividad sobre la base de un oficio judicial, para que tenga validez como prueba.
    - Identificar los CyberEventos
    - Poseer la habilidad para identificar, captura y analizar archivos del tipo log, obtenidos desde la navegación por las redes
    - Entender como asegurar este tipo de pruebas, debido a su innegable volatilidad
    - También es importante, dentro de estos aspectos a tener en cuenta, evaluar la posibilidad de incluir en el análisis en cuestión, los posible dispositivos que se encuentren conectados en la red, en el momento de la investigación
    - Desplegar métodos para investigar accesos y tráfico de redes remotas
- ¿Es posible considerar en ese protocolo la menor cantidad de agentes implicados en la manipulación, análisis de evidencia y generación de reportes para la valoración de quienes deben impartir justicia?
- ¿Es posible asegurar trazabilidad de la prueba informática, identificando tiempos y responsables?
- ¿Es posible obtener pruebas válidas desde la Nube?
- ¿Es posible contemplar problemas de jurisdicciones, ante la obtención de evidencias?

- Teniendo en cuenta una adecuado protocolo de trabajo, es posible dar respuesta al interrogante es lo mismo “la falta de evidencia” a la evidencia de la falta”?
- ¿Es posible identificar las personas implicadas en el proceso, desde la obtención de la prueba, hasta la valoración de la misma por la Justicia, incluyendo las etapas de forensia y pericial informática?
- ¿Es posible asegurar la inviolabilidad de la evidencia informática?
- ¿Es posible definir procedimientos que permitan almacenar y asegurar inviolabilidad de la prueba informática, antes eventuales repeticiones o ampliaciones de la pericia, producto de nuevas investigaciones?

La respuesta afirmativa a los interrogantes mencionados anteriormente, para la cadena de custodia, permite proteger y dar inmutabilidad a la evidencia, al tener conocimiento de quién obtuvo la evidencia, dónde y cuándo fue obtenida, quién la protegió y quién ha tenido acceso a la evidencia, y en qué condiciones.

- Por otra parte, la constante evolución del delito, nos permite agregar otro tipo de inquietudes, las que guardan relación por ejemplo con el siguiente interrogante: ¿Es posible que los continuos intentos de violentar cifrados como el RSA 4096, tengan éxito? Esto puede impactar en distinto aspectos, que pueden ir desde un intento de violación en la seguridad en los datos con el objetivo de cometer un delito, hasta la inquietud desde un Tribunal de Justicia de conocer si esto es posible o puede haber pasado en alguna circunstancia judicial que se denuncie.

  Sobre este punto, debemos avanzar sobre nuevos desafíos como cuando se plantea que:

  “… *La seguridad que ofrece el sistema de claves RSA 4096 es uno de los más “potentes” y, hasta el momento, se han dispensado advertencias por Internet alertando de vulnerabilidades sobre el avanzado sistema de criptografía. La herramienta Phuctor que busca módulos duplicados en los*

servidores PGP de claves públicas, desde Loper-OS expresan haber ***conseguido "romper" el sistema de cifrado.***"

Se afirma que: "…*Las claves que han sido descifradas, se señala que corresponden a errores de seguridad por problemas de red, fallos en el disco duro o errores de software*."

http://www.adslzone.net/2015/05/18/rompen-por-error-el-cifrado-mas-seguro-del-mundo/

- Es fundamental además considerar las nuevas alternativas y problemática que genera "Cloud Computing". Esta nueva preocupación se centra en:
  - ✓ El debido conocimiento y control de la gestión en la nube
  - ✓ El cumplimiento contractual entre el prestador y el cliente
  - ✓ La disponibilidad del servicio en la nube
  - ✓ La confiabilidad, seguridad y confidencialidad sobre los servicios

  Sin duda, esto dispara nuevos problemas legales, que van a exigir de un perito informático la preparación y conocimiento adecuado de varios aspectos técnicos hoy día no habituales en el tratamiento de la informática. [PUB002] Consideraciones legales relativas a la privacidad en proyectos de Cloud Computing en el exterior del país – Mg. Darío Piccirilli – Ing. Juan Cruz González Allonca - relais-v2-n1-77-90

- Finalmente, a la luz del nuevo Código Procesal Penal, y teniendo en cuenta que a criterio del suscripto se plantea un nuevo paradigma legal sobre las pericias en general, y en particular sobre las de carácter informático, se hace necesario cubrir la actual falencia en los procedimientos vigentes (que no existen o no se encuentran normalizados) y además de cubrir la necesidad de **contar con un protocolo actualizado**

y debidamente formalizado para poder afrontar los desafíos técnicos derivados de las nuevas tecnologías en informática, asistiendo en forma a la Justicia, en forma efectiva al momento de dictar sentencia.

Pues, se debe tener en cuenta que en la Ley 27.063 – Título IV: Peritajes. **Artículos 161**, se plantea lo siguiente:

> "… *Artículo 161.- Procedencia. Si para conocer o apreciar un hecho resultaran necesarios conocimientos especiales en alguna ciencia, arte o técnica, las partes podrán presentar informes elaborados por peritos de su confianza en cuyo caso deberán acompañar los elementos que acrediten la idoneidad profesional de aquéllos*."

> **<u>Comentario</u>:**
>
> En esta parte de la ley, **no se hace referencia a la necesidad de contar con un perito de oficio designado oficialmente por el juez**, como hasta ahora viene sucediendo con el actual Código Procesal Penal.

Luego en el **Artículo 164,** se plantea:

> *"… Artículo 164.- Dictamen pericial. El dictamen será fundado y contendrá, de manera clara y precisa, una relación detallada de las operaciones practicadas y sus resultados, las observaciones de las partes o de sus consultores técnicos y las conclusiones que se formulen respecto de cada tema estudiado.*
>
> *Los peritos podrán dictaminar por separado en caso de que exista diversidad de opiniones entre ellos. El dictamen se presentará por escrito firmado y fechado, sin perjuicio de la declaración en las audiencias."*

Comentario:

Tampoco aquí aparece la figura del perito de oficio designado por el juez actuante en la causa. Esto significa que las partes que intervienen en el pleito judicial, podrán nombrar sus propios peritos, quienes actuaran en forma conjunta o separada, **aplicando sus propios protocolos para practicar la forensia informática**, **el procedimiento pericial en la preservación de la prueba y el mantenimiento de la cadena de custodia para la pericia informática.**

Aquí queda claro que es posible que aparezca una diversidad de situaciones técnicas, basadas en distintas experiencia y conocimientos de los peritos, lo que podría producir dictámenes muy distintos sobre la misma causa. Esto traería confusión y podría complicar la situación técnica, al momento que el Juez deba valorar las pruebas y dictar sentencia.

Hoy día, la figura del perito de oficio es la que representando al juez, define los procedimientos científicos a aplicar, dirige la pericia y asiste directamente al juez, en forma totalmente objetiva e imparcial.

Pero por otra parte, quedan planteados los siguientes interrogantes:

- Existe entonces la posibilidad que quien pueda contratar el mejor perito del mercado (o estudio pericial), tendrá mejores posibilidades en la resolución técnica del conflicto?
- Se pierde la igualdad de posibilidades, basadas en la objetividad e imparcialidad del perito de oficio, nombrado por el Juez.

Finalmente, en el **Artículo 165** de la misma ley, se plantea:

> *"… Artículo 165.- Instituciones. Si el peritaje se encomendara a una institución científica o técnica y en las operaciones debieran intervenir distintos peritos o equipos de trabajo, se podrá elaborar un único informe bajo la responsabilidad de quien dirija los trabajos conjuntos, el que será suscripto por todos los intervinientes."*

Comentario:

En esta parte de la norma, se abre la posibilidad de dar intervención a una institución científica o técnica, por ejemplo una Universidad. Esto podría mejorar la situación de disponibilidad de peritos adecuados, pero seguiría vigente lo planteado en el comentario al Art. Anterior.

5.3.- Aportes – Propuestas

5.3.1.- **Órgano asesor en la Justicia Nacional**

Se propone crear un órgano asesor técnico informático pericial, en el ámbito de la Corte Suprema de Justicia de la Nación, que tomando como base los puntos técnicos planteados en la presente Tesis, pueda optimizar los mismos a través de un refinamiento y profundización de los aspectos detallados en el punto 5.1.- Conclusiones – Futuras líneas de investigación.

Esto permitiría tener un equipo técnicamente especializado en el tema pericial informático, que pueda cubrir en forma multidisciplinaria todas las aristas que tiene una pericia informática, basada o no en la forensia informática, asegurando amplia experiencia y conocimientos actualizados.

De esta manera, a través del órgano asesor (que en base el nuevo Código procesal Penal no sería vinculante), se podría ayudar a las

partes de un conflicto a contar con protocolos adecuados para dirimir un planteo técnico en informática, y por otra parte, contribuiría a definir pautas claras basadas en las buenas prácticas, facilitando así el fallo de un Juez.

5.3.2.- **Instituciones Científicas – Universidades Nacionales.**

Fomentar en las Instituciones Científicas, Universidades Nacionales, Institutos y similares, **la creación de entes u órganos técnicos específicos, con el fin de asesorar a la Justicia Nacional y otro tipo de entidades u organizaciones** que necesiten realizar tareas periciales en el ámbito de la informática.

Potenciar los centros de investigación forense y periciales en informática ya existentes en algunas entidades, como la Universidad Nacional de La Plata, permitiendo así un aprovechamiento de las experiencias e investigaciones realizadas hasta el momento, generando una base para profundizar en forma inmediata, apuntando a la excelencia profesional y permitiendo formar nuevos recursos humanos en el tema.

Ello, con la finalidad de contribuir a la adecuada solución de problemas informáticos en un litigio, asegurando la aplicación de las buenas prácticas periciales, propendiendo a generar dictámenes técnicos justos, equitativos, imparciales, objetivos y técnicamente correctos, en el marco de la mejor calidad profesional.

Es fundamental tener en cuenta que **hoy día la informática es trasversal a todas las situaciones y disciplinas**, manteniendo puntos de contacto (y por ende, potenciales puntos de conflicto) en todas los aspectos de la vida cotidiana.

Sin duda, esto permitirá cubrir de la mejor manera posible el “vacío¨ que hoy existe y **que se profundizará a partir del año 2016**, con la aplicación del nuevo Código Procesal Penal, generando así condiciones adecuadas para quienes deban impartir justicia considerando y valorando las pruebas informáticas para dirimir pleitos.

Pues, a criterio del suscripto, desaparece conceptualmente el perito de oficio, o al menos desaparecería la asistencia de las fuerzas de seguridad (Policía Federal Argentina, Gendarmería Nacional Argentina, Policía Metropolitana y Prefectura Nacional Argentina) en la función de peritos de oficio, con todo lo que ello implica.

Se va a generar la necesidad de contar de manera urgente con peritos informáticos, que tal vez no posean la experiencia, especialidad y herramientas necesarias para la complejidad de tareas que se presenten, haciéndose necesario contar con órganos serios y capaces de asistir tanto a la Justicia Nacional Argentina como a las partes que intervengan (personas físicas, empresas, industrias, organismos estatales, organizaciones sociales, organizaciones educativas, fundaciones, ONG, etc.)

CAPITULO 6. BIBLIOGRAFÍA – REFERENCIAS[1]

6.1.- BIBLIOGRAFÍA – REFERENCIAS BASE

Libros

Gatesi, M y Creus, D. (2012). *El cibercrimen y las guerras de ro-bots: Search & Destroy*.
[CIBER01]

Miró Linares, F. (2012). *El Cibercrimen: Fenomenología y Criminología de la Delincuencia en el Ciberespacio.* Ediciones Jurídicas y Sociales S.A., 1ra. Edición. Pág. 237, 250 y 261
[CIBER02]

Glenny, M. (2013). *El lado oscuro de la Red, el CiberCrimen, la Ciberguerra y TU*. España, Madrid: Alcaná Libros. Pág. 220 a 233
[CIBER03]

Vacca, J. (2010). *System Forensics, Investigation, and Response.* Jones & Editorial: Barlett Publishers
[FoEx07]

McKenzie Marshall, A. (2008). *Digital Forensics: Digital Evidence in Criminal Investigations. Editorial:* Wiley-Blackwell
[FoEx08]

Revistas

Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. (2011). Academic Press - Elsevier Inc. 3ra. Edición
[Casey04]

Guidelines for Evidence Collection and Archiving. (2002) – RFC 3227. Network Working Group.
[GUID001]

[1] Para las citas de las referencias bibliográficas se ha tenido en cuenta la normativa ISO 690:2013 aplicada por la Universidad Politécnica de Valencia

Ponencias de congresos

Sáenz, R. (2014). "*Situación en Argentina a 5 años de la sanción de la ley de Delitos Informáticos". Tercer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática".* Mar del Plata, Buenos Aires, Argentina

[**ANTE 02**]

Evelyn Salas, O. Ramírez García, A. y Núñez Mori, O. (2011). *"Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana*". Pontificia UNIVERSIDAD CATÓLICA del Perú Lima, Perú.
[**PROPER**]

López, O. Amaya, H. y León, R. (2002). "*Informática forense: generalidades, aspectos técnicos y herramientas"*. Primer Congreso Iberoamericano de Seguridad Informática CIBSI '02. Morelia, México.
[INCFOR02]

Piccirilli, D. (2014). "*La Forensia como Herramienta en la Pericia Informática*". Revista Latinoamericana de Ingeniería de Software 1(6) - relais-v1-n6-237-240
[PUB001]

Piccirilli, D. y González Allonca, J. (2014). *"Consideraciones legales relativas a la privacidad en proyectos de Cloud Computing en el exterior del país*". Revista Latinoamericana de Ingeniería de Software 2(1) - relais-v2-n1-77-90
[PUB002]

Páginas WEB

Agencia Española de Protección de Datos. (2001). Convenio sobre la CIBERDELINCUENCIA - Budapest, 23.XI. <https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf> [Consulta: 13 de enero de 2015] [**CONV01**]

FBINoblett, M (2000). Recovering and Examining Computer Forensic Evidence. <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm> [Consulta: 24 de noviembre de 2014] **[ReEx01]**

Scientific Working Group on Digital Evidence (SWGDE) (2000).Digital Evidence: Standards and Principles. <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm> [Consulta: 12 de Febrero de 2015] **[ScWo01]**

UNIANDES. (2005). *Evidencia Digital: contexto, situación e implicaciones nacionales*. <http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf> [Consulta: 10 de abril de 2015] [**EviDig05**]

IOCE, International Organization of Computer Evidence. <http://www.ioce.org> [Consultado: 30 de octubre de 2014] [**IOCE06**]

UNODC. (2010). *Guía para el desarrollo de la capacidad de examen forense.* <http://www.unodc.org/documents/scientific/FDE_Guide_S_Ebook.pdf> [Consultado: 30 de octubre de 2014] **[GUID002]**

Department of Justice Office of Justice Programs National Institute of Justice Electronic Crime Scene Investigation – U.S. (2008). *A Guide for First Responders.* <www.ojp.usdoj.gov/nij> [Consulta: 01 de febrero de 2015] **[GUI003]**

NIST. *Examination of Digital Evidence: A Guide for Law Enforcement*. (2015)
<http://www.nist.gov/oles/forensics/digital_evidence.cfm>
[Consulta: 29/01/2015]
[**GUI004**]

National Criminal Justice Reference Service. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* NCJ 199408
<https://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx>
[Consulta: 3 de junio de 2015]
[GUI005]

United Nations Public Administration Network. (2003). *Guidelines for the Management of IT Evidence.*
<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf>
Consulta: 6 de junio de 2015
[GUI006]

United Nations Public Administration Network. (2004). *Guidelines for the Management of IT Evidence.*
http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf
[Consulta: 30 de enero de 2015)
[COFO003]

Institute for Socio-Financial Studies. (2009). Computer *Forensics – Part 2: Best Practices - Information Security and Forensic Society.*
<http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf>
[Consulta: 31 de enero de 2015]
[COFO001]

Association of Chief Police Officers. (1996). *Good Practice Guide for Computer-Based Electronic Evidence - Official release version*
<http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf>
[Consulta: 6 de febrero de 2015]
[COFO002]

McAfee. (2014). *Forensic Investigation - Hunting Down The Source of Your Attack.*
<http://www.mcafee.com/in/resources/data-sheets/foundstone/ds-forensic-investigation.pdf>
[Consulta: 12 de mayo de 2015]
[INCFOR01]

US DEPARTMENT OF JUSTICE. (2004*). Forensic examination of digital evidence. A guide for law enforcement. Special Report.*
<https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
[Consulta: 12 de mayo de 2015
[FoEx04]

OIPC-INTERPOL. Quai Charles de Gaulle -69006 Lyon – Francia. (2008). *Informe Forense de Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia.*

<http://www.interpol.int/es/Centro-de-prensa/Noticias/2008/PR017>
[Consulta: 10 de diciembre de 2014]
[ANTE01]

US Department of Justice. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.*
<https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>
[Consulta: 26 de junio de 2015]
[GUI007]

ISSUU. (2006). Introducción a la Informática Forense.
<http://issuu.com/gilbertcs/docs/dos>
[Consulta: 1 de julio de 2015]
[GUI008]

ACCESSDATA. (2015). *Forensic Toolkit*
<http://www.accessdata.com/products/utk>
[Consulta: 16 de diciembre de 2014]
[FoEx05]

X-Ways Software Technology AG. (2015). *WinHex*
<http://www.x-ways.net/forensics/index-m.html>
[Consulta: 20 de diciembre de 2014]
[FoEx06]

Legislación – Fallos judiciales

Argentina. Código Procesal Penal de la Nación Argentina.

Argentina. Nuevo Código Procesal Penal de la Nación Argentina. Ley 27.063, sancionado 4 de diciembre de 2014, promulgado 9 de diciembre de 2014.

Argentina. Código Procesal Civil y Comercial de la Nación Argentina

Argentina. La Cámara Federal Confirmó anulación de Peritaje sobre mails - Causa Nro. 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial" - Jdo. Fed. n° 7 - Sec. N° 14 Buenos Aires, 24 de mayo de 2012 **[FALLO1]**

Argentina. Cámara Federal de Casación Penal - Causa Nro. 16339 -Sala IV– C.F.C.P. "GIL, Juan José Luis s/ rec. de casación". 22 de marzo de 2013. REGISTRO Nro: 337/13 **[FALLO2]**

Argentina: Ley 25.036 Propiedad. Intelectual, 15 de noviembre de 2008.

Argentina: Ley 26.388 Delitos Informáticos, 24 de junio de 2008.

Argentina: Artículo 44 Código Contravencional de la Ciudad Autónoma de Buenos Aires, 23 de Septiembre de 2004

Argentina: Ley 25.930 Modificación Código Penal / Incluye Inc. 15 Art. 173 y Modificación Art. 285, 17 de septiembre de 2004

Argentina: Ley 25.891 Servicio de Comunicaciones Móviles, 25 de mayo de 2004.

Argentina: Ley 25.236 Habeas Data, 2 de noviembre de 2000.

Argentina: Ley 24.766 de Confidencialidad, 30 de diciembre de 1996.

Argentina: Ley 24.769 Penal Tributaria, 15 de enero de 1997.

GLOSARIO

CC: Cadena de Custodia

CD-ROM: Disco compactos, de solo lectura, utilizado para grabar y guardar información

CLOUD COMPUTING: La computación en la nube, conocido también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos

CPU: Unidad Central de Procesamiento. Término utilizado normalmente para identificar una computadora personal del tipo PC. En realidad es una de las partes principales que integran un equipo computador

CVP: Ciclo de Vida Pericial. Término creado y aplicado por el Mg. Darío A. Piccirilli, para explicar las distintas etapas que intervienen durante una pericia informática, desde su inicio hasta su final (incluye las etapas de impugnaciones y aclaraciones solicitadas por el Juez, hasta el cobro de honorarios)

ED: evidencia digital

DeepWeb: Se le conoce informalmente como Internet profunda o Internet invisible. Se estima que es una porción presumiblemente muy grande de Internet y que es difícil o casi imposible de rastrear y deliberadamente (Proyecto Tor)

DONGLE: Término aplicado a un soporte para almacenamiento de datos en forma externa (tipo pendrive o similar), que generalmente se conecta vía USB y se aplica para autenticar software (por ejemplo, para validar licencias de software)

DVD: Digital Versatile Disk. Es similar en apariencia a un CD, pero con mayor capacidad de almacenamiento.

FCCI: Formulario de Cadena de Custodia Informática

FORENSIA: también llamado computación forense o análisis forense digital. Es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

FREE SPACE: espacios que se encuentran en un disco rígido o medio de almacenamiento de datos, que fueron previamente “usados” (es decir grabados)

y luego borrados o “liberados” por el sistema operativo, pero que no se encuentran nuevamente grabados o “pisados”.
En estos casos, son partes o “fragmentos” de archivos pre existentes, que pueden ser utilizados por expertos en forensia informática, para encontrar evidencia digital.

IMAGEN FORENSE: Es el proceso de obtener una copia de datos almacenados en un medio óptico o magnético. Es de aclarar que la copia resultante permite realizar un análisis de datos para investigar sobre la misma, como si fuera la información original (y permite de esta manera preservar la prueba informática en su estado fuente o de origen).

IMEI: International Mobile Equipment Identifier. Es un número de serie único de 15 dígitos, que sirve para identificar un teléfono o dispositivo celular o GSM.

INGENIERIA SOCIAL: Se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros, generalmente con fines delictivos.

MD5: es un algoritmo de reducción criptográfico de 128 bits ampliamente usado en el mercado informático, para identificar información sin alteraciones

PASSWORD: una frase o palabra o combinación de letras números y/o signos, de conocimiento reservado, que es aplicado como medida de seguridad para accede a los sistemas de informática.

RAM Random Access Memory. Unidad para almacenar informático dentro de un computador. Es de alta velocidad y es volátil (es decir, cuando el computador se apaga, se pierde su contenido)

SANITIZAR: expresión en castellano que se aplica para indicar la acción de limpiar un elemento

SLACK SPACE: Cuando un programa de una computadora requiere grabar datos en bloques físicos de las unidades de almacenamientos de información, estos bloques se asignan en partes, así el programa va usando cada trozo hasta completarlo y luego seguir con el siguiente. Cuando se genera un programa por primera vez, generalmente estas partes son contiguas. Con el tiempo y con el uso o procesamiento, estas partes contiguas se fragmentan en áreas más pequeños. Cuando se borra un datos o programa, es posible que queden restos de estas partes (fragmentos) que no poseed ninguna estructura lógica (por ejemplo de un archivo), pero que sí puede contener algún “vestigio” de información que puede ser aprovechado durante una investigación (ello, aunque no tenga un significado “lógico”)

SO: Sistema Operativo es un programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware en un equipo computador, y provee servicios o interactúa con los programas de aplicación. Son por ejemplo

Windows NT, Windows 2000, XP o Vista. También puede ser UNIX, y sus variantes Linux, HP-UX, Solaris y Apple's Mac OSX.

USB STORAGE DEVICES: dispositivos para pequeños volúmenes de almacenamientos de datos. Son conectados a las computadoras por ports o puertos preparados para ello (del tipo USB), pueden ser fácilmente removidos y transportados.

WINDOWS: sistema operativo del tipo propietario, perteneciente a la empresa Microsoft Corporation.
Ejemplos del mismo son: MS-DOS, Windows, Windows 3.0, Windows 95, Windows 98, Office XP, Windows XP, Windows NT, Windows Vista, Windows 8, Windows 10, Windows Server.

WIPEAR: limpiar, borrar en forma segura, de forma tal que no queden datos residuales que puedan contaminar una copia forense para la posterior etapa de búsqueda

ZIP DRIVE Dispositivo de 3.5 pulgadas, del tipo removible, producido ir la empresa Iomega. Este dispositivo puede almacenar información en discos del tipo "ZIP", con un formato de compresión de datos especial y propietario de la marca. El archivo generado bajo este formato, tiene una "extensión" identificado como "ZIP".

FIGURAS