Universidad Siglo 21

Trabajo Final de Graduación

Investigación Aplicada

La Ciencia Informática Forense como auxiliar del proceso judicial. Estudio y análisis de su inserción en la investigación de delitos de índole federal.

Alumno: Caamaño, Ezequiel Alejandro

Año: 2013

Índice

Resumen

En los últimos años se ha verificado un incremento exponencial en el uso de las tecnologías de la información en todos los ámbitos de la vida cotidiana. Este incremento produjo a su vez un aumento en la incidencia de estas herramientas tecnológicas en las distintas actividades delictivas, ya sea como objeto mismo de delito o como productor o contenedor de pruebas criminales. En este ámbito surje la informática forense como herramienta innovadora en el proceso judicial. La hipotesis planteada es que el desarrollo de esta área no fue acompañado de la conveniente difusión y conocimiento hacia los distintos actores del proceso y que consecuentemente su potencial se encuentra acotado, debiendose implementar mecanismos que permitan explotar todas sus posibilidades y aumentar el valor de sus aportes durante el proceso. Se busca arribar a un plan de actuación para mejorar la interacción entre los ámbitos de la justicia, las fuerzas policiales, y los grupos técnicos específicos.

Palabras claves Informática forense, evidencia digital, criminalística, pericia informática

Abstract

In recent years there has been an exponential increase in the use of information technologies in all areas of daily life. This increase was in turn an increase in the incidence of these technological tools in various criminal activities, either as an object of crime or as a producer or container of criminal evidence. In this area arises computer forensics as innovative tool in the judicial process. The hypothesis is that the development of this area was not accompanied by the appropriate dissemination and knowledge toward the various actors in the process and consequently its potential is limited, and should implement mechanisms to exploit all the possibilities and increase the value of their contributions during the process. It seeks to reach an action plan to improve the interaction between the fields of justice, police forces, and the specific technical groups.

Key words: Computer forensics, digital evidence, criminalistics science, computing expertise

B. Presentación del Trabajo Final de Graduación

B.1.1 Título: La Ciencia Informática Forense como auxiliar del proceso judicial. Estudio y análisis de su inserción en la investigación de delitos de índole federal en la Argentina.

B.1.2. Introducción a la temática

En la actualidad es innegable la inserción de la Informática en todos los ámbitos humanos. La informática se incorpora en todos los aspectos de la vida diaria de la mayoría de las sociedades humanas modernas, afectando la vida de todos los habitantes del mundo, de una u otra manera con diversos grados de intensidad.

Dicho proceso se dio también en el ámbito del derecho. Si bien la Informática Jurídica tuvo adelantos en sus aspectos documentales y de gestión, sigue atrasada en el ámbito decisorio.

La incorporación de los sistemas informáticos a la vida cotidiana y su enorme potencial como herramientas multipropósito trajo aparejado que pudieran utilizarse también para cometer delitos o para contener indicios de actos ilícitos cometidos en cualquier ámbito, naciendo de este modo la necesidad de un experto capacitado en una ciencia a la que hasta el momento el procesal judicial no había apelado.

De esta manera surge una nueva especialidad de la Criminalística que en los últimos años se ha vuelto indispensable en el procedimiento judicial, y que requiere de un profundo conocimiento de los elementos técnicos materiales e inmateriales, ingenio para extraer de ellos la información requerida, una cuidadosa revisión de las condiciones que permitan preservar el valor probatorio de esa información y un certero modo de vincular toda esa actividad con las necesidades legales del proceso que las requiera.

Dicha especialidad es la Informática Forense, objeto principal de estudio de este Trabajo Final de Graduación.

Específicamente se estudió el desarrollo actual de la especialidad en el ámbito judicial federal, y su inserción en el área pericial de una fuerza de seguridad.

B.1.3. Planteamiento del problema y su justificación

Para poder desarrollar su actividad de manera profesional, el perito informático forense debe unificar una serie de perfiles mínimos pretendidos, que deben incluir, un Marco Científico, Criminalístico, Informático General y Específico, así como también un marco legal abarcativo de las distintas actividades periciales a desarrollar.

Sin embargo, si bien se puede contar con un conjunto de tecnologías y herramientas acordes con las tareas a desarrollar, dicha capacidad técnica se enfrenta a distintas dificultades, entre las que se pueden contar el desconocimiento por parte de los actores decisorios en el proceso judicial de las posibilidades reales que la Informática Forense tiene, habida cuenta de lo novedoso del campo específico. A esto se puede sumar la escasa jurisprudencia, la falta de antecedentes en ocasiones e incluso, en algunos aspectos, el vacío legal existente en torno al tema, y lo extremadamente tradicionales y ortodoxos que suelen ser los ámbitos de las investigaciones judiciales y sus actores.

Ante esta realidad se consideró sumamente pertinente un estudio profundo del sistema informático pericial, que sirva no solo como acercamiento a un campo específico del conocimiento científico tecnológico, sino también desarrollar recomendaciones que tengan por objeto mejorar la sinergia propia del sistema.

B.1.4. Hipótesis

Como describiéramos anteriormente, es innegable la fuerte inserción de las denominadas Tecnologías de la Información en todos los ámbitos de la vida en sociedad, el crecimiento exponencial de su utilización en la mayoría de las actividades, y su práctica ubicuidad.

Sin embargo, estas tecnologías que determinan incluso nuevas formas de establecer vínculos interpersonales, se basan en desarrollos tecnológicos y científicos demasiado profundos para las personas ajenas a esa área del conocimiento.

En relación a lo antes referido, es inevitable el aumento de la presencia de sistemas informáticos y electrónicos en la comisión de delitos comunes. Asimismo, y como consecuencia de esta evolución hacia la utilización de tecnologías digitales, surgen nuevas formas delictivas asociadas y, a su vez, con características particulares muy distintivas y a la vez innovadoras, que se constituyen en un nuevo desafío para los investigadores de los fueros judiciales penales, que por un lado requieren de profesionales capacitados que les sirvan de soporte científicos a la hora de valorar los hechos, pero que además manejen una temática altamente especializada.

Frente a esta situación, se plantearon las siguientes hipótesis

- La informática forense se encuentra cada vez más presente en la investigación criminal.
- Sin embargo, existe un fuerte desconocimiento de las partes no técnicas involucradas en el proceso penal, de todas aquellas posibilidades que brinda la informática forense en la sustanciación de una causa judicial, acotando sus potencialidades.

B.1.5. Objetivos Generales

Realizar un acercamiento a esta especialidad tan compleja y específica dentro del campo de estudio de la Informática y del desarrollo de la misma en el ámbito jurídico pericial en la actualidad nacional, a través del análisis de distintas fuentes de información existentes, y del trabajo de campo en áreas específicas dedicadas a la aplicación directa de las técnicas periciales informáticas.

B.1.6 Objetivos Específicos

1) Realizar una investigación por medio de distintas fuentes que permita:

    - Identificar la utilidad que proporciona un análisis forense informático.
    - Identificar las herramientas disponibles para realizar un análisis forense informático.
    - Analizar el marco jurídico tecnológico existente en la actualidad en el país relacionado con la actividad pericial informática.

2) Analizar la estructura del área criminalística pericial informática de una fuerza de seguridad policial y su relación como auxiliar de la justicia.

3) Definir un plan de actuación para mejorar la interacción entre los ámbitos de la justicia, las fuerzas policiales, y los grupos técnicos.

B.2. Metodología

B.2.1. Metodología y estructura teórica

Metodología a Aplicar

a) Elección del tema:

Motivos:

-Trabajo en el área.

-Si bien el tema de investigación fue tratado con anterioridad, el mismo presenta particularidades que varían acorde al ámbito jurisdiccional y legal de aplicación.

-Es de interés para el investigador.

-Se considera cada vez más presente elementos y conductas relacionadas con el uso de las tecnologías de la información en la vida diaria, y por ende en relación con la comisión de delitos.

b) Tipo de investigación:

-Antes de plantear las hipótesis se realizó una revisión del material documental existente.

-La investigación fue mixta, es decir, documental y de campo.

-Se recurrió a fuentes directas e indirectas.

-Se buscó arribar a conclusiones cuya aplicación sirva para mejorar la interacción entre los ámbitos científico-periciales y procesal legal.

c) Limites de la investigación:

- La presente investigación se llevó a cabo tomando como ámbito de estudio el área pericial y de investigaciones de los denominados delitos informáticos de la Policía Federal Argentina, y su interacción con el fuero penal federal, por lo que sus interpretaciones sólo podrán aplicarse a dicho ámbito.

- Sus resultados no podrán aplicarse a la investigación en el ámbito de la justicia ordinaria.

Metodología

El presente trabajo se dividió en diferentes capítulos donde se llevó a cabo una introducción a la temática y su surgimiento, se describió el Marco Criminalístico, con la incorporación de la Informática Forense en la ciencia Criminalística, y en el ámbito judicial, donde se describieron los conceptos de Delito Informático y el Lugar del Hecho. Seguidamente se introdujo el concepto de Prueba Documental Informática y su valor probatorio. Posteriormente se enumeraron los principios y reglas que rigen la actividad, introduciéndonos en el marco tecnológico propiamente dicho con la enumeración de herramientas habituales de uso, para finalizar describiendo las actividades periciales complementarias.

Por otro lado, se realizó el análisis del área pericial de una Fuerza de Seguridad Federal (la Policía Federal Argentina), y más en profundidad de las actividades periciales informáticas, a través del empleo de entrevistas con personal en actividad de la misma y el análisis de la información obrante en los registros de la fuerza. Asimismo se apuntó a obtener testimonios de funcionarios judiciales del área de la investigación del delito para poder evaluar la utilidad del uso de esta herramienta en la prosecución de causas criminales.

Del estudio y análisis de la información obtenida se arribóa una propuesta de posibles caminos a seguir para lograr un mejor uso de esta herramienta de las Tecnologías de la Información para la prosecución de las causas penales, extrayéndose las pertinentes conclusiones del estudio.

B.2.2. Fundamentación Teórica

Capítulo Nº 1: Introducción a la Informática Forense. Surgimiento.

Como se ha mencionado al inicio del presente trabajo, el desarrollo de los medios de procesamiento digital y su integración con las redes de datos ha trascendido los ámbitos académicos, científicos y comerciales, incorporándose a distintas actividades diarias, influyendo cada vez más no solo en las relaciones interpersonales sino también en la manera en que se vincula la gente con el medio, desde el consumo hasta la educación.

No obstante, de la misma forma en que surgen potencialidades que facilitan el intercambio de bienes y servicios de una manera positiva, también el uso de la informática favoreció el anonimato para la comisión de ilícitos de distinta índole, utilizándose, por ejemplo, la red para adquirir drogas, armas y pornografía infantil.

Como ha sucedido a lo largo de la historia, todo avance de la tecnología puede ser utilizado tanto para beneficio de los hombres, como así también como herramientas en la ejecución de actividades reñidas con la ley y la ética. A esto hay que sumarle el presunto anonimato que otorga el uso de redes de comunicaciones como Internet.

Relacionado con lo antedicho, y con la naturaleza disociada entre la tecnología, la ética y el estado de derecho, requiere, como en toda investigación de índole científico tecnológico, tener una visión estrictamente profesional y técnica, a la hora de llevar a cabo una diligencia pericial, independiente de la especificidad de la actividad forense de que se trate.

En este sentido es fundamental referir que los especialistas forenses en todas sus especialidades actúan frente a la autoridad judicial que ha solicitado su asistencia, como testigos idóneos, debiéndose hacer hincapié en las tareas técnicas específicas y los conocimientos científicos propios del área, dejando de lado cualquier tipo de prejuicio u opinión personal en torno al caso de estudio.

El surgimiento de la Informática Forense

Como se mencionara anteriormente, la Informática Forense se desprende principalmente de una serie de sucesos que han afectado a la sociedad globalizada e informatizada de fin de siglo XX y principios del XXI (Darahuge y Orellano González, 2011):

- La aparición de conductas compatibles con figuras delictuales, utilizando sistemas de información, evolucionando en lo que posteriormente se calificaría como delitos informáticos propios e impropios.
- La capacidad que poseen estas conductas de interactuar directa o indirectamente con gran parte de la normativa penal vigente.
- La escasez de legislación específica vigente, configurando una zona gris legal, e incluso a veces un vacío, aunque se analizan distintas implementaciones.
- La inexistencia de mecanismos de acción contra delitos de informáticos o llevados a cabo por medios computacionales dentro de la Legislación de forma (Códigos de procedimiento), por lo que en ocasiones se producirían conflictos entre los derechos a la verdad material, al debido proceso y a la privacidad, al momento de secuestrar y preservar pruebas informáticas.
- La existencia en la actualidad de escasa jurisprudencia, dependiendo más de la opinión, la formación profesional y la buena voluntad del juez, que de un accionar legislativo consensuado y fundamentado científicamente en un entorno multidisciplinario.

Lo antes mencionado ha sido acompañado de un incremento constante en estas modalidades delictivas, y de las herramientas informáticas en la comisión de otras actividades tipificadas en el Código Penal de la Nación, afectándose transversalmente distintas áreas de a sociedad.

Esto ha generado la necesidad de que desde las distintas áreas comprometidas con dicha problemática (Informática, Derecho, Criminalística), surjan acciones tendientes a desarrollar desde un punto de vista interdisciplinario métodos de abordaje, mecanismos y

técnicas, que permitan conformar un protocolo de acción frente a este tipo de diligencias.

Asimismo, se considera de interés para el profesional tener un conocimiento cabal del alcance, desarrollo y evolución de la Informática Forense, lo que redundará en la conformación de una visión abarcadora y a la vez precisa que permita fundamentar las tareas llevadas a cabo.

Esto permitirá no solo el correcto desarrollo de su actividad profesional, sino además mejorar la interacción con otras disciplinas forenses, en vista de la naturaleza multidimensional de toda actividad humana en general y de las acciones de índole delictual en particular, permitiendo el desarrollo a su vez de normativas y metodologías de abordaje efectivas y eficaces en el análisis del delito informático y sus consecuencias.

Como se refiriera anteriormente, el surgimiento, crecimiento y difusión de las tecnologías de la información en general, y la incorporación de la utilización de los servicios de redes de datos en particular, ha generado importantes aportes a la humanidad, que van desde lo tecnológico a lo cultural, pasando por los mecanismos de relación interpersonal. Ligado con esta interacción no puede eludirse el advenimiento de formas de utilización de estos medios tecnológicos en la comisión de hechos delictuales o actividades relacionadas con delitos.

Como se mencionara precedentemente, las computadoras o sistemas computacionales pueden ser utilizadas como herramientas en la comisión del delito, o incluso convertirse en objeto del delito propiamente dicho. Estas tipologías pueden variar tanto como las simples amenazas a través de mensajes correo electrónico, robo o copia no autorizada de software hasta casos de fraudes electrónicos o pornografía infantil, pasando por todo un abanico de posibilidades en lo que respecta a la utilización de medios digitales.

Dichas circunstancias determinan la necesidad de implementar diversas e incontables herramientas para la investigación de evidencia sospechada, tales como búsqueda de palabras claves específicas, análisis de registros de eventos para verificar qué ocurrió en determinado horario y fecha y del análisis de información almacenada en dispositivos volátiles o no

volátiles.

Por su parte, las vulnerabilidades propias de los sistemas operativos, aplicaciones y servicios de red, convierten a los equipos informáticos en victimas ideales para distintos tipos de ataques o fraudes tecnológicos, como los ataques de forma remota a través de redes de datos, como Internet. Frente a esto, han surgido distintas iniciativas para conformar equipos de respuestas a incidentes. Entre ellos se pueden destacar el CERT (Coordination Center), el Forum of Incident Response And Security Teams (www.first.org), el AR-CERT-Coordinación en Emergencias en Redes Teleinformáticas (www.arcert.gov.ar).

Capítulo Nº 2: Ciencia Criminalística. Implantación Pericial Criminalística

La Informática Forense, como disciplina particular inserta dentro de la Ciencia Criminalística, mantiene caracteres y particularidades propias de esta disciplina madre, por lo que se hace necesario una revisión de esta última.

Podemos mencionar que la Criminalística es la disciplina que se encarga de brindar apoyo al proceso judicial, aportando criterios científicos, tecnológicos y técnicos al análisis a posteriori de los hechos criminales. Desde el punto de vista de la ciencia del derecho, se orienta al área penal.

Su surgimiento permite obtener una respuesta científico-racional para la valoración de los indicios que surgen en torno a la comisión de los delitos, permitiendo suplantar métodos probatorios clásicos de dudosa validez objetiva e incompatibles con un estado de derecho moderno y la filosofía imperante en el sistema legal argentino. En este sentido, permiten descartar desde la histórica prueba divina, las pruebas corporales y sus sucesores, la prueba confesional y la prueba testimonial con sus problemas de subjetividad, configurando un nuevo tipo de prueba denominada "prueba indiciaria".

Su base se centra en el estudio de los indicios, denominados por esta especialidad como "testigos mudos", que permanecen en el lugar del hecho y que permitirían realizar la reconstrucción del mismo.

Para esto se requiere la identificación, recolección, certificación y resguardo de la citada prueba indiciaria por parte de los distintos profesionales forenses.

Podríamos definir a la Criminalística como "disciplina auxiliar de la investigación judicial que aplica los conocimientos, métodos y técnicas de la investigación de las ciencias naturales en el examen del material sensible significativo relacionado con un presunto hecho delictivo o no, con el fin de determinar su existencia, o bien reconstruirlo, para señalar y precisar la intervención de uno o varios sujetos, llegando así a la verdad histórica o material del hecho. Su objeto de estudio es la prueba indiciaria."

Asimismo, resulta de interés para su análisis el estudio de los objetivos específicos que pueden vislumbrarse en esta actividad:

- Investigar técnicamente y demostrar científicamente la existencia de un hecho en particular que probablemente sea delictivo.
- Reconstruir los hechos acaecidos, determinando los fenómenos ocurridos y los mecanismos utilizados, señalando los instrumentos u objetos de ejecución sus manifestaciones y las acciones que se pusieron en juego para realizarlo.
- Aportar las evidencias, coordinar técnicas y sistemas para la identificación de la víctima.
- Aportar evidencias para la identificación del o los presuntos autores.
- Aportar pruebas indiciarias para probar el grado de participación del o los presuntos autores y demás involucrados.

Asimismo, Darahuge y Orellano González (2011), identifican una serie de características destacables de la disciplina que nos permiten arribar a un concepto más completo de la misma:

- Indicios (Testigos Mudos): Se consideran como tales a todo objeto, instrumento, huella, marca, rastro, señal o vestigio, que tiene su origen en la ejecución de un hecho, independientemente de su naturaleza y condiciones particulares. El análisis de los mismos permitirá establecer relaciones y determinar la sucesión de acontecimientos que lo generó, los instrumentos utilizados y/o los actores involucrados, aunque los mismos puedan o no corresponderse con actos ilegítimos o ilegales. Por su parte, es dable destacar que un indicio está formado de signos y en algunos casos de símbolos, cuyo sentido o interpretación dependerán del entorno y el objetivo de la labor pericial reconstructiva. Como se mencionara anteriormente, dicha labor reconstructiva puede considerarse en definitiva el fin último de la actividad pericial.
- Identidad: Este principio es basal del análisis pericial y considera que un indicio es idéntico a sí mismo y diferenciable de sus copias y modelos representativos.

- Intercambio: Es el que se encuentra presente por la propia interacción entre los distintos actores (autor y víctima) y el lugar del hecho o escena del crimen, como resultado de los hechos ocurridos.
- Correspondencia o identificación comparativa: Fundamental en todo análisis forense ya que es la que relaciona indicios entre sí y causísticamente con los posibles autores del hecho investigado. Ejemplo de esto es la correspondencia de huellas dactilares halladas con una persona, o la asociación de proyectiles con el arma mediante la cual fueron disparados, a través del uso de comparadores balísticos.
- Reconstrucción de hechos: Como resultado de las distintas actividades periciales y a partir del análisis de los indicios en la escena del crimen se debería poder deducir, generar y proponer una secuencia de ejecución de acciones, y una situación resultado, coherente, metodológica y lógicamente válida, sustentada en las distintas medidas llevadas a cabo durante la investigación pericial y con los respectivos fundamentos científicos, tecnológicos y técnicos de validez reconocida y reproducción asegurada, que permitan establecer la sucesión de eventos que conforman el hecho delictivo investigado y su correspondientes circunstancias que lo rodean.
- Probabilidad: Del análisis científico pericial y de los elementos observados y verificados durante la investigación del hecho en si mismos, se debe poder determinar la probabilidad de ocurrencia del evento, partiendo desde un grado muy bajo de probabilidad hasta la certeza metodológica, lógica e instrumental, resultando dicha probabilidad de importancia trascendente en la sustanciación de la investigación judicial.

Cabe destacar que, existen diversas maneras de clasificar a los indicios de acuerdo con su naturaleza y demás características. Algunas de estas clasificaciones son las siguientes:

- Indicios determinados o indeterminados
- Indicios asociativos o no asociativos.
- Indicios microscópicos o macroscópicos.
- Indicios trasladables o no trasladables.

- Indicios virtuales

Lo referido precedentemente, podrían hacer suponer que la utilización de la Criminalística como soporte del proceso judicial brinda una certeza acabada a la hora del análisis de los hechos por los distintos estamentos del sistema procesal penal. Sin embargo, en la práctica la metodología propia de la disciplina termina comparando objetos con otros objetos, distintos elementos de la prueba indiciara, y si bien aporta muchísimos elementos de juicio para los organismos judiciales, en pocas ocasiones se puede relacionar dichos indicios de manera directa con el autor de los hechos. No obstante, el desarrollo tecnológico permite en muchos casos establecer vinculaciones sin probabilidad de duda, como en el caso de los análisis de ADN, que permiten establecer la vinculación directa del autor con el hecho y la escena del crimen.

En última instancia, siempre es el juez quien debe evaluar la pertinencia de la prueba indiciaria, dentro del marco de la normativa procesal vigente y a partir de su propia concepción e interpretación, como elemento pertinente y conducente en la investigación del hecho particular que debe analizar, juzgar y sentenciar.

En relación con las distintas disciplinas que engloba la Criminalística en su conjunto, se pueden mencionar a la Medicina Forense, Toxicología, Dactiloscopia, Balística, Documentología, entre otras, denominadas genéricamente Ciencias Forenses.

Dentro de estas Ciencias Forenses, y como resultado de los cambios tecnológicos y su vinculación sociocultural, aparece la Informática Forense. No obstante lo novedoso de la especialidad, como rama de la Criminalística se sustenta en las premisas científicas, metodológicas, criminalísticas y probatoria judicial, de esta Ciencia madre. Además, por el propio carácter transversal de la Informática misma, viene y se integra, complementa y es complementada por las restantes Ciencias Forenses, convirtiéndose en herramienta de análisis de todas ellas y se relaciona de manera similar con todos los métodos probatorios aceptados por el Derecho Procesal.

Al igual que en la Criminalística clásica su objeto era la prueba indiciaria, en el caso

particular de la Informática o Computación Forense, su objeto es la prueba indiciaria informática, es decir, los testigos mudos que quedan como resultado de operaciones lícitas e ilícitas sobre activos informáticos, con fines reconstructivos orientados en particular, pero no exclusivamente, a la investigación judicial.

Capítulo Nº 3: Concepto de Informática Forense. Su implantación en la Criminalística.

A la hora de establecer una definición en torno a la Informática Forense, se observa que los distintos autores que tratan la problemática establecen múltiples definiciones. Dentro de esta multiplicidad de conceptos (Cano, 2009), surgen alguno como computación forense, digital forensics (forensia digital), network forensics (forensia en redes), entre otros.

El primero de los conceptos, computación forense, lo describe de dos maneras complementarias no excluyentes, como:

- Disciplina de las ciencias forenses que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular hipótesis relacionadas con el caso; y
- Disciplina científica y especializada que, entendiendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos.

Por su parte, cuando se refieren a network forensics (forensia en redes), se plantea un escenario más complejo, ya que deben incorporarse el conocimiento de sistemas operativos,, protocolos, configuraciones e infraestructura de comunicaciones específicas.

Por último, digital forensics (forensia digital), plantea un acercamiento más globalizador de la especialidad, refiriéndose a una forma de aplicar conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en la investigación de delitos.

Todos estos conceptos apuntan a aspectos generales y específicos que convergen en la identificación, la preservación, la extracción, el análisis, la interpretación, la documentación y la presentación de evidencia digital, entendiéndose como tal a cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático, para sustentar las hipótesis sobre hechos que se hayan formulado.

Si bien los conceptos vertidos anteriormente nos permiten realizar un acercamiento a la definición de Informática Forense, el autor del presente trabajo considera más cercano y compatible con la jurisprudencia y evolución de la doctrina del derecho argentino, al análisis de Darahuge y Arellano González (2011), quienes establecen varios aspectos del concepto de Informática Forense:

1) La informática Forense es un método probatorio consistente en la revisión científica, tecnológica y técnica, con fines periciales, de una colección de evidencias digitalizadas para fines de investigación y legales.
2) Cada caso específico debe ser analizado como si fuera un juicio, de esa manera cualquier investigación en Informática Forense puede soportar un escrutinio legal.

Se puede concluir que entendemos por Informática Forense "al conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática" (Darahuge y Arellano González; 2011; p. 9).

En este sentido, cabe aclarar que en Criminalística se considera como prueba indiciaria al conjunto de huellas (testigos mudos), de cualquier tipo y naturaleza, que se haya producido como resultado de una acción cualquiera y que al ser metodológicamente investigados, permitan reconstruir los hechos acaecidos. En general, pero no en forma excluyente, se relacionan con actos delictivos, equiparándose con el concepto descripto en la bibliografía internacional especializada como "evidencia digital".

Además de las características que le corresponden por tratarse de una especialidad de la Criminalística, cuenta con particularidades propias de la especialidad forense, que justifican su diferenciación inclusiva en las mismas. En tal sentido se puede afirmar que forma parte de la Informática en general y de la Seguridad Informática en particular.

Sus características particulares se enumeran a continuación:

Objeto: la prueba indiciaria informática.

Método: desarrollar mecanismos de análisis criminalístico, con soporte científico, tecnológico y técnico, sobre la prueba indiciaria informática.

Tipicidad: Aunque se trata de una construcción transdisciplinaria, posee características propias derivadas de sus diferencias conceptuales con las restantes ciencias forenses.

Especificidad: Su empleo, desde el punto de vista metodológico, puede clasificarse en:

- Análisis Pericial de la Prueba Indiciaria Informática
- Gestión Integral de la Prueba Documental Informática
- Auditoría Informática Forense.

Implantación Informática

La implantación de la disciplina forense informática, al igual que sucede con el surgimiento de toda área del conocimiento innovadora, al intentar insertarse dentro de las demás, presentó en sus inicios ciertas dificultades en relación a la definición de su objeto, sus métodos y los límites de su accionar.

A esto se suma una característica inherente a las ciencias informáticas o de la computación, que deriva de la gran variedad de formaciones académicas y profesionales con sus distintos títulos de pregrado y grado, y sus denominaciones.

Al analizar otras disciplinas forenses se puede observar que dichas cuestiones se encuentran mucho más definidas, tanto por la antigüedad de su implantación, como por las características propias de la especialidad. Ejemplo de esto es la Medicina Forense, para cuya

práctica se requiere título profesional claramente determinado (Médico), matricula habilitante otorgada por organismo responsable (Colegio Médico o Ministerio de Salud), y títulos de especialidad.

Cuando por su parte, analizamos lo que ocurre con la Informática Forense, nos encontramos con la existencia de un sinnúmero de títulos habilitantes para realizar pericias, tanto de grado como de pregrado, los que incluyen:

- Ingenieros y Licenciados en Informática (Carreras de Grado).
- Técnicos Superiores y Analistas de Sistemas (Carreras terciarias y universitarias de pregrado).
- Carreras de Postgrado (especializaciones, maestrías y doctorados específicos).
- Incumbencias de otras disciplinas (por ejemplo, la carrera de ingeniero electrónico o industrial, etc.)

Obviamente, esta diversidad de formaciones académicas y listados, genera un ambiente de confusión y desorden.

Este clima de confusión, se suma al escaso conocimiento que se registra en el ámbito del derecho tanto de la Criminalística en general, como de la Informática Forense en particular, debido a la prácticamente nula o escasa incorporación en los programas de formación formal de grado de los profesionales de la Abogacía, lo que conlleva a la necesidad imperiosa de la asesoría especializada por parte de un experto en temas de informática y criminalística.

En este sentido, resulta interesante para ayudar a aclarar un poco el panorama al profano la descripción de las distintas Disciplinas Informáticas, pudiendo encuadrar a la Informática como la disciplina principal, formando parte constitutiva, pero no excluyente, la Computación y los Sistemas de Información, pudiendo dividir sus especializaciones principales en:

- Computación:

  - Equipos Informáticos
  - Métodos de Computo.
  - Servicios de generación, almacenamiento, procesamiento y análisis estadístico de datos.
  - Herramientas de apoyo (oficina virtual, soporte a la decisión)

- Sistemas de Información
  - Análisis y diseño de sistemas de información.
  - Programación.
  - Gestión de Sistemas Operativos.
  - Gestión de Aplicaciones.
  - Gestión de Bases de Datos.

- Redes de datos:
  - Diseño e implementación de redes.
  - De área local (LAN).
  - De área metropolitana (MAN).
  - De área ampliada (WAN).
  - Gestión de operaciones y servicios remotos (Internet, transferencia de activos, comercio electrónico).
  - Aplicaciones interactivas de comunicaciones (Correo Electrónico, conversaciones en línea, videoconferencia).
  - Aplicaciones educativas (Educación no presencial, local y/o a distancia).

- Seguridad Informática:
  - Protección de activos informáticos.
  - Auditoría Informática.
  - Ingeniería Inversa (Técnica y social).
  - Guerra Informática (“Warfare”).
  - Informática Forense.

Esta última especialización se puede considerar como crítica, ya que es transdisciplinaria en por lo menos dos sentidos principales:

- En sentido intrínseco, porque abarca métodos y técnicas de todas las otras divisiones de la informática (desde la simulación y análisis de redes físicas o virtuales, hasta la ingeniería inversa).
- En sentido extrínseco, complementa, suplementa y se nutre de diversas áreas del Derecho y de la Criminalística.

A partir de lo antes mencionado, y del análisis de las subespecialidades precedentemente mencionadas, se puede arribar a una definición más acabada de la Informática Forense como el conjunto multidisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación de la prueba indiciaria informática (Darahuge y Arellano González, 2011).

A partir de este punto, se puede efectuar una comparación de la relación y la distinción con respecto a otras especialidades informáticas conexas:

- La auditoría informática: Se puede considerar que la informática forense actúa en soporte de dicha auditoría, pero ésta trasciende a la primera, ya que las herramientas informático forenses brindarán los elementos necesarios para su ejecución práctica, pero no aportarán datos referidos a la legalidad o legitimidad de los resultados obtenidos. En síntesis, la Informática forense aporta herramientas técnicas al auditor para que este realice el análisis de los activos informáticos y sus relaciones, exclusivamente.
- La Informática Forense, como instrumento de análisis de la realidad: Por su propia naturaleza, la Informática Forense tiende a generar un modelo de comportamiento racional con soporte científico y técnico respecto de la prueba indiciaria disponible en un determinado lugar. Este modelo de comportamiento, incluyendo sus consideraciones sociales, criminológicas y criminalísticas, instrumentado por medios idóneos, como, por ejemplo, la realidad virtual, se constituye en una reconstrucción del hecho virtual. De ahí que su utilidad se expanda más allá del

ámbito jurídico y judicial. Es una forma particular y específica de analizar, reconstruir y modelar la realidad. En definitiva puede ser utilizada en toda circunstancia que lo requiera, tanto en los distintos fueros judiciales, como en la labor diaria de organismos oficiales y privados y hasta en ámbitos particulares propios de una persona determinada y su grupo de pertenencia.

Capítulo Nº 4: Concepto de Prueba Documental Informática. Incorporación en el ámbito judicial. Valor probatorio.

A la hora de intentar definir el concepto de Prueba Documental Informática, y más aún, al intentar aprehender su verdadera naturaleza, puede servirnos de medio acercarnos a dicho concepto empezando por el estudio de la Prueba Documental Clásica, de la cual deriva.

Dicha prueba documental fue durante mucho tiempo el principal elemento de la investigación judicial y el objeto de estudio de la Ciencia Criminalística, actuando durante decenas de años como respaldo de la mayoría de los procesos, incluso después de la incorporación de la oralidad procedimental.

Esta tipo de elemento probatorio, ha sido incorporado al proceso judicial hace decenios, por lo que se la conoce, emplea y valora de acuerdo a su pertinencia y a su carácter conducente en el desarrollo del proceso, sin mayores complicaciones, relacionándola directa o indirectamente con los hechos investigados.

Por su parte, admite una clasificación en bibliográfica; foliográfica y pictográfica, acorde con la naturaleza del soporte de la misma.

En relación con lo antes referido, al tratar de describir el concepto de Prueba Documental Informática, se podría indicar que, en principio, difiere solamente en su soporte. Esto se puede efectuar equiparando, por ejemplo, el término de documento con el vocablo más técnico de archivo. En este sentido es dable destacar que desde la óptica de la Informática, toda información es información almacenada, ya sea que se encuentre en soporte físico, en procesamiento o en tránsito.

Por lo tanto, se puede establecer una analogía en el tratamiento de la Prueba Documental Informática, con el tratamiento de la Prueba Documental Clásica, y utilizar mecanismos o protocolos que aseguren su validez.

Resumiendo, se puede incorporar a la clasificación de la prueba documental clásica

una especie más, además de la bibliográfica, foliográfica y pictográfica, incorporando la prueba documental informática con las características propias de la diferencia en el soporte de la misma.

En este caso, es dable destacar que se vuelve trascendental la utilización de una prueba de informes para confirmar los resultados.

Asimismo, debido a la propia naturaleza de la prueba, su especificidad y sus peculiaridades relacionadas con su origen informático, la misma debe ser validada a través de una pericia informática que permita eliminar cualquier controversia que pueda surgir en torno a ella.

Relaciones con otras disciplinas

- Medicina Legal: le brinda soporte informático a la misma, a través del mantenimiento de Historias Clínicas, interconsultas remotas, etcétera.
- Criminología: Al momento de la reconstrucción virtual del hecho, se constituye en soporte fundamental, para intentar aprehender cuestiones vinculadas con el factor humano de la situación.
- Criminalística: Mantiene con la Informática Forense una estricta relación de género a especie.
- Disciplinas periciales integradoras: Se constituyen en soporte mutuo e instrumento de cada disciplina específica.

Puestos a analizar la incorporación en el ámbito del proceso judicial penal, de la prueba documental informática, no se puede negar que la misma es un medio probatorio, tan válido como cualquier otro. Desde la perspectiva de la legalidad, se encuadra en el marco general de la prueba documental clásica, difiriendo de esta solo en el soporte (papel en la clásica, digital en la Informática). Su tratamiento es analógico de la antes citada, con algunas características propias y se encuentra respaldada por el artículo 378 del Código Civil y Comercial de la Nación. (*"...Los medios de prueba no previstos se diligenciarán aplicando por analogía las disposiciones de los que sean semejantes o, en su defecto, en la forma que*

establezca el juez").

La primera consideración respecto de su pertinencia y ubicación entre los mecanismos probatorios judiciales, se refiere a la naturaleza complementaria de ésta. Como ya se refiriera, los resultados obtenidos deben ser convalidados con la respectiva pericia informática y la prueba de informes de la misma.

Resumiendo, toda documental informática es una prueba indiciaria, pero no toda prueba indiciaria informática es una prueba documental. Esta característica debe ser tenida especialmente en cuenta por el operador del derecho, a la hora de establecer los puntos de pericia, ya que los mismos pueden incluirse en la documental informática o no y seguramente la trascienden a la hora de formularlos.

Valor Probatorio de la Prueba Informático Forense.

La Prueba documental informática se asimila en nuestro sistema legal a la prueba documental clásica, que se encuentra regulada en los distintos Códigos de Procedimiento y aceptada en forma homogénea.

Como se refiriera anteriormente, se podría decir que la prueba documental informática solo se diferencia de la anterior en el soporte, por lo que debe ser tratada en el Derecho Procesal de igual manera, ya que se considera que:

- Se trata de archivos (en papel o digitales, pero conteniendo texto y/o gráficos).
- Se pueden reproducir sin restricciones.
- Son adulterables mediante maniobras de modificación remotas.
- Pueden ser firmadas y certificadas.
- Constituyen elementos probatorios de similar valor decisivo.
- Difieren solamente en dos puntos principales: I) mientras los documentos en papel adhieren al principio de identidad criminalística, los digitales no; y II) los documentos digitales son fácilmente modificables por medios remotos, lo que no ocurre con los documentos bibliográficos o foliográficos.

Asimismo, cabe mencionar que la prueba documental informática puede ser utilizada en igual forma que la documental clásica, ya que es susceptible de certificación por medios digitales (autoridad certificante y firma digital), por medios de certificación tradicional y acorde a su nivel de certificación y clasificación de seguridad su solidez probatoria es equivalente a la documental clásica.

Resumiendo lo antedicho, y en virtud de la similitud entre la prueba documental clásica y la informática, se puede considerar su pertinencia como equivalente. Ejemplo de esto es la jurisprudencia existente en la que se asimila el correo electrónico con la correspondencia epistolar.

Sin embargo, es importante mencionar que dependerá la pertinencia de la correcta interpretación de sus características particulares al solicitarla, implementarla y al evaluarla. En este sentido, es interesante observar los fundamentes de un fallo en el que la Cámara Nacional de Apelaciones en lo Comercial, Sala "D", acepta el valor probatorio de un mensaje de correo electrónico que no ha sido firmado digitalmente, en el que expresa: *"En el valor probatorio de correo electrónico ocupan un lugar preeminente a partir de la vigencia de la Ley 25.506 los documentos con firma digital, en tanto su valor probatorio es equiparable al de los instrumentos privados, y se presume su autoría e integridad del mensaje... Aun cuando en este caso se trata de documentos que carecen de firma digital a los que no puede otorgarse un valor de convicción preeminente por no cumplir con los requisitos de los arts. 2 y 5 de la ley 25.506... no existe elemento a mi juicio para que se los ofrezca como medio de prueba (C.P.C. 378:2), considerándoselos principios de prueba por escrito como había aceptado la doctrina antes de la sanción de la citada ley... Tal valor probatorio se sustenta en las normas del C.C. 1190, 1191,1192, pues aunque por no estar firmados no alcancen la categoría de documento privado es admisible su presentación en juicio para probar un contrato siempre que emanen del adversario, hagan verosímil el hecho litigioso y que las restantes pruebas examinadas a la luz de la sana crítica corroboren su autenticidad. Por lo tanto, es decisiva la prueba complementaria que se produzca merituada conforme los criterios de la sana crítica y conjuntamente con las restantes pruebas del proceso".*

De esta manera se asimila el documento digital al documento sin firma y se le reconoce el valor de Principio de Prueba Por Escrito, aunque en este caso en particular se recalca la necesidad de ser corroborados por otros elementos de prueba y no resultar contrarios o contradictorios con los mismos (Darahuge y Arellano González, 2011).

Si bien, lo antes referido corresponde a la jurisprudencia y doctrina procesal imperante en la actualidad, al valorar la prueba informática en la Argentina resulta interesante revisar la postura de Vázquez Rojas (2008), al analizar la prueba informática desde la Teoría Racional de la Prueba, que considera a las pruebas como elementos de conocimiento, interesándose más en cómo el juzgador conoce o debe conocer determinado medio probatorio. En este sentido refiere que "la adopción de la teoría racional no implica negar la discrecionalidad del juez en el contexto de la reglas jurídicas que establecen el principio de libre apreciación de la prueba sino que este efectúe sus valoraciones por las reglas de la ciencia, la lógica y de la argumentación racional".

Asimismo, considera el grado de similitud existente entre la prueba indiciaria informática y las pruebas científicas, ya que ambas aluden a circunstancias que para ser establecidas o valoradas es necesario recurrir a ámbitos especializados del saber, y que por esto mismo la autoridad judicial debe apelar a expertos para adquirir las nociones técnico-científicas que le sirvan para auxiliarlo a la hora de juzgar.

Además, hace hincapié en la importancia de asegurar que el experto puede proveer información confiable, para lo cual se requeriría: a) la controlabilidad de la teoría científica sobre la que se funda la prueba; b) la determinación del porcentaje de error relativo a la técnica empleada; c) de la existencia de un control ejercido por otros expertos; d) de la existencia de un consenso en la comunidad científica de referencia.

Capítulo Nº 5: Delito Informático y lugar del hecho.

Al momento de tratar de definir el concepto de "Delito Informático" o de alta tecnología, la doctrina, tanto nacional como internacional, no se ha podido poner de acuerdo para arribar a una definición concreta.

Por un lado, la doctrina internacional no considera posible arribar a una definición propia de delito informático. No obstante, se considera que abarca por un lado la esfera privada del ciudadano, mediante la acumulación, archivo, asociación y divulgación de datos obtenidos mediante computadoras, y, por otra parte, delitos patrimoniales por el abuso de datos procesados automáticamente. Se centran por un lado en conductas que utilizan herramientas tecnológicas y en conductas que recaen en estos medios como tales.

Durante mucho tiempo se consideró que se trataba de delitos comunes que se diferenciaban por el tipo de herramienta utilizada o por los objetos que vulneraban. Dicha definición resultaba lo suficientemente acotada como para dejar de lado y no contemplar otras conductas que difícilmente se podían tipificar a través de las figuras penales existentes.

De esta manera surgieron algunos intentos de definir a los Delitos Informáticos como "aquel que se da con la ayuda de la informática o de técnicas anexas", o como "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena", o bien "cualquier conducta criminal que en su realización se hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin". Incluso el Departamento de Justicia de los Estados Unidos de América confeccionó su propia definición de delito informático como "cualquier acto ilegal que requiera el conocimiento de tecnología informática para su perpetración, investigación o persecución".

A partir de dichas definiciones, Tobares Catalá y Castro Argüello (2010, p. 29) rescatan los elementos comunes y conceptualizan la figura delictiva de una manera que se considera bastante certera al definir a los delitos informáticos como "aquellas conductas

ilícitas susceptibles de reproche y pasibles de sanción por el derecho penal, en las cuales se utilizan de manera indebida cualquier medio, mecanismo y/o sistema informático, ya sea como fin en si mismo o como medio para la comisión de otro delito".

Previo a la sanción de la Ley Nacional Nº 26.388, que modifica el Código Penal e incorpora la figura del delito informático, tipificándolo en nuestra normativa, existieron varias clasificaciones que pueden resultar de interés.

Una de ellas es la expresada por Julio Tellez Valdés (México, 2008), que realiza una división entre dos criterios: como instrumento o medio, y como fin u objetivo.

Como instrumento o medio, como su denominación lo indica, engloba esas conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documento vía computarizada (tarjetas de crédito, cheques)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, fraude).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos, tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema, introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objeto, se compone de las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a los dispositivos de almacenamiento.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje.

Otras clasificaciones, dividen a los delitos informáticos en tres categorias, de acuerdo a cómo usan la tecnología:

- Como método: cuando se utilizan métodos electrónicos para llegar a un resultado ilícito.
- Como medio: cuando se utiliza una computadora como medio o símbolo.
- Como fin: conductas delictivas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Otra clasificación digna de mención es la elaborada por Jorge Pacheco Klein, que los divide en:

- Internos: como por ejemplo, el sabotaje de programas:
- A través de las telecomunicaciones.
- Manipulación de computadoras: apropiación indebida, peculado y fraudes informáticos
- Utilizando computadoras en apoyo de empresas criminales, como el lavado de dinero y la distribución de drogas.
- Robos de software: piratería.

Finalmente, incluso organismos como la Organización para las Naciones Unidas cuentan con una clasificación en la que reconoce tres categorías, según sean cometidos mediante:

- Fraudes por manipulación de computadoras: manipulación de datos de entrada, abarcando a la sustracción o apoderamiento de datos, la manipulación de programas, la manipulación de datos de salida, y el fraude por manipulación informática.
- Por falsificación: el documento describe conductas de adulteración de la información contenida en forma de datos, como la alteración de documentos almacenados en los sistemas.
- Por daño o alteración de sistemas, se clasifica a acciones como el sabotaje informático, envio de virus, gusanos, bombas lógicas, accesos no autorizados, reproducción no autorizada de programas, etc.

Incluso se propone una clasificación según las actividades delictivas graves que tienen como epicentro a la web, entre las que se mencionan:

- Terrorismo
- Narcotráfico
- Espionaje
- Espionaje industrial
- Tráfico de armas
- Proselitismo de sectas
- Propaganda de grupos extremistas
- Pornografía infantil

Existen varias clasificaciones más, pero el panorama antes descripto nos permite hacernos una idea de la complejidad del tema a la hora de abordarlo y tratar de encuadrar estas conductas que nacen y se gestan con el advenimiento de las nuevas tecnologías.

En la Argentina, los esfuerzos de legislar sobre esta temática dieron como resultado la sanción en junio del año 2008 de la Ley Nº 26.388 de Reformas al Código Penal, incluyendo de esta manera en su normativa las conductas que denominamos "Delitos Informáticos".

Es importante destacar que no se generó con la mencionada reforma un cuerpo legal autónomo del Código Penal, con figuras determinadas, clasificaciones y definiciones propias, sino que se incorporaron, sustituyeron, modificaron y agregaron a las figuras típicas existente, nuevos conceptos. En este sentido, coincidimos con algunos autores en que probablemente hubiera sido más conveniente generar una norma específica, por tratarse de un bien jurídico novedoso como en el caso de otras conductas delictivas, como la Ley de Estupefacientes, por ejemplo.

La ley 26.388, tipifica los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (Art. 128 C.P.)
- Violación, apoderamiento y desvió de comunicación electrónica (Art. 153, párrafo 1º C.P.)
- Interceptación o captación de comunicaciones electrónicas o telecomunicaciones (Art. 153, párrafo 2º C.P.)
- Acceso a un sistema o dato informático (Art. 153 bis C.P.)
- Publicación de una comunicación electrónica (Art. 155 C.P.)
- Acceso a un banco de datos personales (Art. 157 bis, párrafo 1º C.P.)
- Revelación de información registrada en un banco de datos personales (Art. 157 bis, párrafo 2º C.P.)
- Inserción de datos falsos en un archivo de datos personales (Art. 157 bis, párrafo 2º C.P.)
- Fraude informático (Art. 173, inc. 16 C.P.)
- Daño y sabotaje informático (Art. 183 y 184, incs. 5 y 6 C.P.)

Asimismo, incorpora una serie de terminología en la normativa de fondo, términos que se agregan como últimos párrafos del art. 77 del mencionado cuerpo legal:

- Documento: comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Firma y suscripción: comprende la firma digital, la creación de una firma digital o firmar digitalmente.
- Instrumento privado y certificado: comprenden el documento firmado digitalmente.

El Delito informático propio e impropio

Independientemente de las clasificaciones referidas en el presente capítulo, al enfocarnos en el análisis del elemento informático en la producción de delitos, nos encontramos ante dos situaciones distintas que debemos destacar, y que revisten una importancia vital desde el punto de vista del profesional forense:

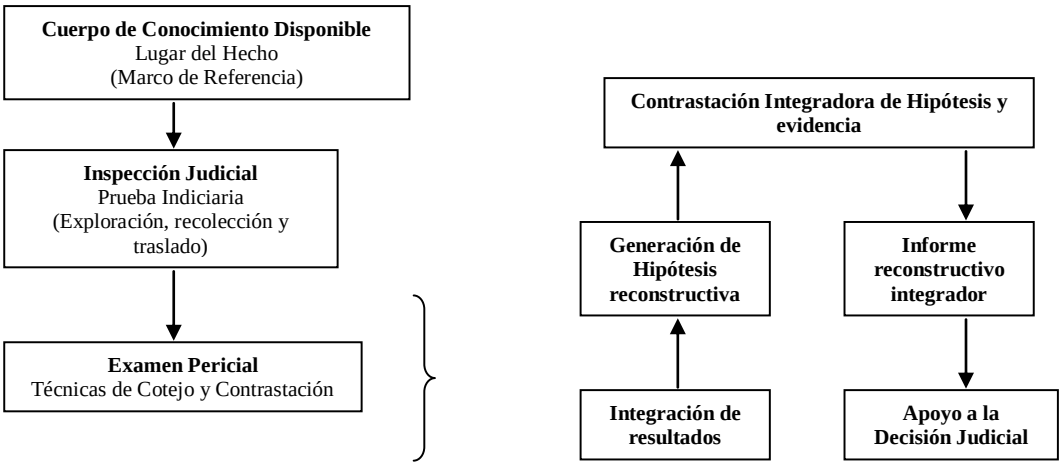
- Delitos informáticos propios: Son aquellos delitos que atentan contra un bien protegido específico: "la información". En general afectan al derecho a la privacidad.
- Delitos informáticos impropios: Son los que se producen mediante la violación de normas jurídicas ya establecidas, con anterioridad al empleo de esta modalidad, por ejemplo daño, estafa, utilizando para cometerlos herramientas informáticas.

Como toda clasificación, admite formas mixtas De ahí que algunas figuras gocen de ambas particularidades, por ejemplo, en la sustitución de identidad, se procuran datos filiatorios (sensibles) propios de la persona a sustituir y luego mediante esta información se realizan todo tipo de actividades lícitas e ilícitas en su nombre y por su cuenta.

Cabe destacar que toda prueba indiciaria tiene como fin principal o subsidiario contribuir a la reconstrucción de los hechos acaecidos en un momento espacio temporal histórico. Esta reconstrucción metodológicamente hablando, consiste en el desarrollo de un guión factible, a partir de la prueba indiciaria recolectada.

La tarea de reconstrucción de los hechos ocurridos se realiza a partir de un marco de

referencias, soportado por el marco teórico de quien la efectúa y a partir de las variables involucradas (situación original → hechos → nueva situación). No escapa al marco general de una investigación formal, a partir de cualquier disciplina del conocimiento.



Darahuge y Orellano González, 2011, Pág. 27

El punto de partida es el lugar del hecho a partir del cual se realizan las tareas reconstructivas y de cuya integridad dependen los resultados posteriores.

Lugar del hecho Virtual propio o impropio

Se suele identificar a la Criminalística con la investigación del lugar del hecho (se trate de una escena criminal, delictiva o no). Lo que percibimos y complica bastante el tema es que el lugar del hecho real (el lugar físico donde ocurrieron los hechos investigados) en general estaba restringido a un espacio físico limitado y que, con escasas excepciones (las aeronaves, las embajadas, los océanos, las vía navegables internacionales), podía circunscribirse, delimitarse y establecer con claridad la jurisdicción y competencias correspondientes (de esto dependerá el derecho procesal a aplicar y la validez e inserción legal de la prueba pericial a implementar). Pero con el auge de las comunicaciones las circunstancias han cambiado, se producen delitos informáticos propios (ataque a la información) e impropios (delitos comunes utilizando herramientas y métodos informáticos), pero en un entorno geográficamente distribuido y no siempre posible de delimitar.

A partir de ahí derivamos la concepción y representación de un lugar del hecho virtual (propio cuando se trata de delitos realizados por medios informáticos distribuidos geográficamente e impropio, cuando solo se emplea para modelar mediante herramientas de simulación, inteligencia artificial y redes neuronales, un lugar del hecho real clásico). Este lugar del hecho virtual no deja de ser un lugar del hecho con características particulares. Es un lugar delimitado o delimitable, donde ha ocurrido un hecho o un conjunto de hechos íntimamente relacionados, que deben ser utilizados para comprender e integrar la trama investigada. No debemos olvidar que la reconstrucción del hecho no es otra cosa que la representación posible del orden sucesivo en que se supone ocurrieron los acontecimientos cuestionados, a partir de los "testigos mudos"; obrantes en la escena analizada, una especie de trama con soporte argumental lógico y respaldo científico, tecnológico y técnico específicos.

A mediados del siglo pasado, el lugar del hecho se evidenciaba como un lugar físico geográficamente determinado. A partir del surgimiento de la computación, aparece el criterio de virtualidad. La virtualidad no es otra cosa que un modelo representativo de una realidad contrastable o meramente imaginaria.

Del surgimiento del delito informático propio e impropio se construye una nueva forma de interpretar la realidad reconstructiva y aparece el lugar del hecho virtual. Este modelo adquiere por lo menos dos formas distintas:

- Lugar del Hecho Virtual Impropio: Consiste en el modelo virtual, realizado por medios informáticos, del Lugar del Hecho Real. Por supuesto es contrastable con la realidad y cuenta con el soporte tecnológico de la Realidad Virtual y la Inteligencia Artificial. Es básicamente una simulación interactiva, que pretende ofrecer alternativas consistentes a partir de las cuales realizar una reconstrucción de los hechos sucedidos.
- Lugar del Hecho Virtual Propio: En este caso no existe el Lugar del Hecho Real. Se trata de reconstruir situaciones puramente virtuales a partir de la prueba indiciaria informática. En este caso el lugar del hecho no es estrictamente determinable y puede llegar a abarcar diversas situaciones geográficas, jurisdicciones y competencias.

La confección de modelos a partir del Lugar del Hecho Real, no trae grandes dificultades, es nada más que una herramienta puesta al servicio de la investigación judicial. Herramienta sumamente útil, porque facilita el intercambio de información entre los participantes que pueden

interactuar por medios virtuales, adecuar sus tiempos a las necesidades particulares de cada actor y evitar las complicaciones derivadas de la concurrencia en un momento y lugar determinado de la totalidad de los actores necesarios para realizar una inspección judicial. Por otra parte admite las posibilidades de revisión, reconsideración y reformulación de propuestas. Una inspección judicial normalmente trae aparejadas una serie de tareas complementarias en las que los artífices de la misma deben reunirse para intercambiar información, lo cual se vuelve innecesario utilizando medios reconstructivos a partir de un modelo virtual de lugar del hecho.

Por otra parte surge con la informática y las redes de comunicaciones la posibilidad de interactuar por medios virtuales con personas físicas y jurídicas distribuidas en todo el mundo, y estas relaciones son factibles de derivar en conflictos jurídicos, que requieran intervención jurisdiccional. Establecer la misma se vuelve sumamente complejo, no solo a la hora de lograr el cumplimiento efectivo de la sentencia judicial recaída, sino a partir del momento de seleccionar (de ser esto posible) la jurisdicción ante la cual presentar la acción legal.

En lo que se refiere al Lugar del Hecho Virtual Propio, la problemática está aún lejos de ser comprendida en su totalidad, ya que en su consideración intervienen factores extraños a la ciencia y a la tecnología, relacionados con la situación política de un país determinado y sus normas de Derecho Internacional, como ser:

- Tratados Internacionales de Integración.
- Relaciones Internacionales Bilaterales.

Capítulo Nº 6: Principios y reglas de la Informática Forense

La informática Forense requiere de ciertos principios que constituyan un marco de referencia y variables normativas, que a su vez nos van a servir de basamento para fijar protocolos de acción determinados y aceptados, que permitan arribar a un principio de estandarización procedimental.

- Principio de entidad pericial propia: El empleo de los medios informáticos como instrumentos de conformación de la prueba indiciaria informático forense. Se integra con metodología propia, que permite asegurar la detección, identificación, documentación, preservación y traslado de la evidencia obtenida, con técnicas e instrumentos propios e inéditos para las Ciencias Criminalísticas.
- Principio de protección y preservación: Cadena de custodia estricta y con certificación unívoca comprobable.
- Principio de identidad impropio (de Copias): Del original, ya que cuando se duplica un archivo informático la copia no es igual a la original sino idéntica (un bit no difiere de otro bit y entre sí son inidentificables unívocamente).
- Principio tecnológico transdisciplinario: Se requieren conocimientos específicos por parte de todos los involucrados en la prueba indiciaria informático forense.
- Principio de oportunidad: Debido a su facilidad de destrucción normalmente requiere de tareas complementarias que aseguren su recolección (medidas preliminares, inspecciones o reconocimientos judiciales, órdenes de allanamiento o de intercepción judiciales).
- Principio de compatibilización legislativa internacional: Gran parte de los contratos particulares celebrados en el marco del Derecho Internacional Privado se realizan mediante comunicaciones digitales. Estas actividades no solo devienen en demandas civiles, comerciales y laborales internacionales, sino que en muchas oportunidades constituyen delitos tipificados en la legislación de fondo de cada país.
- Principio de vinculación estricta: La prueba indiciaria informático forense puede estar relacionada con múltiples actividades delictivas dentro de la legislación internacional o el derecho interno, algo que si bien es propio de la prueba pericial, se vuelve crítico respecto de esta disciplina por su relación vinculante con diversos ámbitos.

Estos principios también son expuestos en la bibliografía clásica de la Informática Forense como referencia y guía de actuación, enumerándolos en cuatro reglas básicas de actuación (Airala y Rapetti; 2008):

Regla 1: Minimizar el Manejo del Original: La aplicación del proceso de la informática forense durante el examen de los datos originales se deberá reducir al mínimo posible. Esto se puede considerarse como la regla más importante en la informática forense. Cualquier análisis debe dirigirse de manera tal que minimice la probabilidad de alteración, esto se logra copiando el original y examinando luego los datos duplicados.

La duplicación de evidencia tiene varias ventajas:

- Asegurar que el original no será alterado en caso de un uso incorrecto o inapropiado del proceso que se aplique.
- Permitir al examinador aplicar diferentes técnicas en casos dónde el mejor resultado no está claro. Si durante tales ensayos los datos se alteran o se destruyen, simplemente se recurre a otra copia.
- Permite a varios especialistas de informática forense trabajar en los mismos datos, o en partes de los datos, al mismo tiempo.
- Asegurar que el original se ha preservado en el mejor estado posible para la presentación en un juzgado.

Aunque hay ventajas al duplicar la evidencia, hay también desventajas:

- La duplicación de evidencia debe realizarse de la mejor manera y con herramientas, que aseguren que el duplicado es una copia perfecta del original. El fracaso para autenticar el duplicado apropiadamente, producirá un cuestionamiento sobre su integridad, lo que lleva inevitablemente a preguntar por la exactitud y fiabilidad del proceso del examen y los resultados logrados.
- Duplicando el original, se está agregando un paso adicional en el proceso forense, a más de que la recreación de este ambiente se torna un tanto difícil. Esto implica que se requieren más recursos y tiempo extra para facilitar el proceso de duplicación, y la metodología empleada debe extenderse para incluir el proceso de la duplicación.

Regla 2: Documentar los cambios: Cuando ocurren cambios ya sea en la evidencia original o duplicados durante un examen forense, la naturaleza, magnitud y razón para ellos debe documentarse apropiadamente, esto se aplica tanto a nivel físico como lógico. Adicionalmente, el perito debe ser capaz de identificar correctamente la magnitud de cualquier cambio y dar una explicación detallada de por qué era necesario el mismo, este proceso depende directamente de las habilidades y conocimiento del investigador forense.

Durante el examen forense este punto puede parecer insignificante, pero se vuelve un problema crítico cuando el examinador está presentando sus resultados en un juicio. Aunque la evidencia puede ser legítima, las preguntas acerca de las habilidades del examinador y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado. Con una duda razonable, los resultados del proceso forense, en el peor de los casos, se consideraran inaceptables. Aunque la necesidad de alterar los datos ocurre pocas veces, hay casos dónde al examinador se le exige el cambio para facilitar el proceso del examen forense.

Regla 3: Cumplir con las Reglas de Evidencia: Para la aplicación o el desarrollo de herramientas y técnicas forenses se deben tener en cuenta las normas pertinentes de evidencia. Asegurar que el uso de herramientas y técnicas no disminuye la admisibilidad del producto final.

Presentar la información de una manera que sea tan representativa del original como sea posible. Es decir, el método de presentación no debe alterar el significado de la evidencia.

Regla 4: No exceda su conocimiento: El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad. Es esencial que el perito sea consciente del límite de su conocimiento y habilidad. Llegado este punto, dispone de las siguientes opciones:

- Detener cualquier examen y buscar la ayuda de personal más experimentado.
- Realizar la investigación necesaria para mejorar su propio conocimiento, para que le permita continuar el examen y se alcance a obtener lo que se busca.

Es indispensable que el examinador forense puede describir correctamente los procesos empleados durante un examen y explicar de la mejor manera la metodología seguida para ese

proceso. El fracaso para explicar competentemente y con precisión, la aplicación de un proceso puede producir cuestionamientos sobre el conocimiento y credibilidad del examinador.

Los análisis complejos deben ser emprendidos por personal calificado y experimentado que posea un apropiado nivel de entrenamiento. Adicionalmente, dado que la tecnología está avanzando continuamente, es importante que el examinador reciba entrenamiento continuo.

De todo esto se puede desprender que la prueba pericial informático forense se vincula transdisciplinariamente, por pertenecer simultáneamente al Derecho (por incluirse entre los métodos probatorios procesalmente aceptados); a la Informática (constituyendo una especie de está en si misma); y a la Criminalística.

Capítulo Nº 7: Marco Tecnológico Pericial

A la hora de analizar la pericia desde la práctica, lo primero a considerar por el perito informático forense es el conjunto de elementos que conformarán sus herramientas de trabajos fundamentales, tanto de hardware como de software.

Antes de iniciar la descripción de algunas de ellas, es de importancia señalar que el profesional debe estar compenetrado con su utilización, realizando prácticas previas en laboratorio de las tareas que deba desarrollar en la actividad pericial propiamente dicha. Esto le permitirá por un lado adquirir familiaridad con las herramientas, lo que evitara demoras y posibles errores por impericia, negligencia o desconocimiento; y por el otro lado le permitirá realizar una verificación previa de su correcto funcionamiento.

En lo que respecta a las herramientas de hardware, es conveniente contar con equipos fijos en el laboratorio y una unidad de informática forense móvil. En este sentido cabe destacar que existen a nivel global empresas que comercializan equipos armados específicamente para las prácticas forenses, tanto fijos como móviles, que incluyen software de Informática Forense y herramientas para distintos sistemas operativos. No obstante, es factible armar equipamiento personalizado con las opciones presentes en el mercado, apuntando siempre a sumar la mayor cantidad de características técnicas que permitan obtener versatilidad y potencialidad a la hora de desarrollar la actividad (como por ejemplo, contando con diferentes puertos de conexiones diversas, cableado vario, tanto de datos como de corriente, etcétera).

En lo que respecta a las herramientas de software, se cuenta con herramientas específicas para alguna tarea, otras que reúnen varias funcionalidades, e incluso conjuntos de herramientas integradas en un solo paquete. A su vez, estás pueden ser de tipo comercial o distribuidas con licencias de software libre.

Es de destacar que el perito informático debe contar con profundos conocimientos, de distintas áreas de la informática para poder realizar una correcta selección y aplicación de las herramientas pertinentes, y esta formación debe incluir, entre otras, software de base (sistemas operativos), arquitectura, lenguajes de programación, redes de computadoras (topologías, protocolos, gestión de equipos), etcétera.

A continuación se detallarán algunas herramientas de software de uso habitual en Informática Forense:

Conjunto de herramientas integradas en un solo paquete de arranque en vivo disponibles para CD, DVD, Pendrive (Software Libre):

- **Centrux**: basado en Debian; herramientas para Informática Forense y Respuesta a Incidentes, desarrollado por Marcos Pablo Russo.
- **Caine**, Computer Aided Investigative Environment: Distribución Linux conteniendo un amplio conjunto de herramientas de Informática Forense.
- **The Penguin Sleuth Kit**, de Ernest Baca, basada en la distribución Linux Knoppix. Presenta una interfaz gráfica y se pueden ejecutar las herramientas como root desde la línea de comando. Contiene Herramientas para examinar archivos, directorios, unidades de datos y metadatos de imágenes de dispositivos, herramientas para la recuperación de archivos eliminados en varios Sistemas Operativos, de indexación y búsqueda, para duplicación y borrado seguro de dispositivos de almacenamiento, monitores de red, detección de intrusiones, auditoria de red y test de penetración, inspección de servidores, herramientas gráficas de inspección de red y de seguridad, conexión remota, encriptación, exploración de vulnerabilidades de TCP/IP, paquetes de conexión Secure Socket Layer (SSL), consultas de servidores de nombres de dominios, etcétera.
- **Smart Linux:** basado en Slackware Linux, diseñado para análisis informático forense.
- **Snarl:** basado en FreeBSD.
- **Open Computer Forensics Architecture (OCFA):** de la Agencia Nacional Policial Alemana.
- **Forensix:** creada por Dr. Fred Cohen, experto en código malicioso, es un conjunto de herramientas para la recolección y análisis de datos basado en Linux. Reconoce una gran variedad de hardware. Genera la imagen a partir de cualquier dispositivo de almacenamiento, realiza la verificación de la integridad de los datos con MD5 y crea un registro en la base de datos del caso. Esta herramienta al estar basada en Linux, reconoce diferentes tipos de sistemas de archivos, montando la imagen o dispositivos en distintos sistemas de archivos en modo solo lectura para prevenir cualquier tipo de modificación de la evidencia. Permite efectuar busqueda de cadenas de caracteres o aplicar operaciones booleanas para busquedas acotadas y una herramienta para la busqueda de

imágenes y mostrar bitmaps. La mayoría de las aplicaciones son accedidas por medio de una interfaz gráfica.

- **Helix:** conjunto de herramientas integradas para inicio en vivo para los sistemas operativos Linux, Unix, Mac y Windows.
- **LNX4N6:** del sitio belga de informática forense, basado en Debian.
- **GRML:** Herramienta para administración de sistemas, detección de hardware, rescate, análisis de sistemas de archivo. Basada en Debian.
- **The Autopsy Forensic Browser:** herramienta de gestión de pericias informáticas desarrollada por Brian Carrier bajo licencia GNU General Public License. Su navegador es una interfaz gráfica para la ejecución de los comandos de las herramientas forenses y estándar de las utilidades de Unix. Permite realizar el análisis de volúmenes y sistemas de archivos sobre los sistemas operativos Unix y Windows.

Conjunto de herramientas integradas en un solo paquete Comerciales:

- **EnCase:** de Guidance Software. Es una herramienta basada en Windows. El entorno gráfico facilita la actividad de investigación. Realiza funciones de Duplicación de dispositivos de escritura bit a bit, certificación matemática (hash), vista previa de un volumen, búsqueda de expresiones para filtrado, visualización de discos y volúmenes, apertura de casos, generación de archivos de evidencia, resguardo del caso, generación de informes. Utiliza la metodología de casos para el análisis de cualquiera de los dispositivos o discos que se relacionan con la misma investigación, trabajando con una imagen generada como el archivo de evidencia. Es posible agregar todos los archivos de evidencias y efectuar busquedas en multiples computadoras y en pilas de disquetes. Al crear un nuevo caso el programa solicita información relevante acerca de éste para ser incluida posteriormente en el informe pericial. Durante el análisis se pueden marcar elementos de interés y efectuar comentarios en el área de texto y volver a estas marcas en otro instante de la investigación. Estas indicaciones sirven para ser agregadas al informe y facilitar la tarea del perito informático forense señalando los aspectos relevantes de la investigación a medida que se esta realizando el análisis. Al finalizar se puede exportar el archivo en un formato .RTF, lo que permite su edición en cualquier procesador de textos.
- **New Technologies Incorporated (NTI)**: El software está basado en aplicaciones de

línea de comando.

- **WinHex:** editor de hexadecimal y herramienta de análisis forense que se ejecuta bajo Windows. Se basa en un programa hexadecimal y editor de discos. Posee herramientas para duplicación de discos, visualización y descarga de RAM física y de la memoria virtual de procesos en ejecución, técnicas de recuperación de datos, limpieza del disco duro, poderosas capacidades de búsqueda física y lógica de palabras claves, duplicación de la estructura de registro de archivo, etc.
- **F-Response:** Provee acceso de lectura a los discos de cualquier computadora en red y a la memoria Ram de la mayoría de los sistemas operativos de Microsoft. Permite realizar tareas de Informática Forense a través de redes ip.

Herramientas individuales e integradas en paquetes de funciones específicas:

- **http:/www2.opensourceforensics.org/**, herramientas variadas para Informática Forense, respuesta a incidentes, se aplican a la mayoría de las tareas requeridas en la recolección y análisis de datos, así como también presenta una serie de procedimientos para la verificación de las funcionalidad de las herramientas con el fin de que el perito determine si la herramienta reúne las capacidades esperadas para su labor pericial. Además de las herramientas y procedimientos se encuentran artículos relacionados con la Informática Forense y un conjunto de archivos de imágenes de discos para efectuar las pruebas de las aplicaciones. El conjunto de herramientas que ofrece este sitio aparece en las siguientes categorías, tanto para los sistemas operativos Linux como para Windows:
  - Ambientes de inicio o arranque automático: para iniciar el sistema dubitado en modo seguro o confiable.
  - Obtención o adquisición de datos: para la recolección de información a partir de un equipo apagado o encendido.
  - Particiones del sistema: para examinar la estructura de organización de los datos en los dispositivos de almacenamiento secundario, tal como tablas de particiones y etiquetas de los discos.
  - Sistema de archivos: para examinar sistemas de archivos o imágenes de discos y mostrar el contenido de los archivos y cualquier otra meta data o información de la estructura del mismo.
  - Aplicaciones: para analizar los contenidos de un archivo a nivel de la capa de

aplicaciones.

- Red: para analizar paquetes y tráfico de red. No incluye los registros de eventos de los dispositivos de red.
- Memoria: para analizar la información de la memoria volátil.
- Entornos de programación: para construir herramientas de Informática Forense personalizadas.

- **The Coroner's Toolkit (TCT):** de Dan Farmer y Wietse Venema, http://www.porcupine.org/forensics/tct.html, conjunto de herramientas variadas de análisis forense para Unix, incorporada en la mayoría de paquetes integrados de software de arranque en vivo. Recolecta información específica que requiere de conocimientos avanzados del sistema operativo por parte del perito y además debe ser ejecutada en la computadora vulnerada. La característica relevante es que permite capturar el estado actual de la información que resultaría casi imposible realizarlo de forma manual. La información que se almacena en dispositivos de memoria volátil posee datos relevantes para la obtención de evidencia y detección de actividades no permitidas. Incluye herramientas para recuperar archivos borrados en Unix, para reconstruir datos coherentes a partir de un flujo de bits. Ejemplo de estas herramientas son:
  - grave.-robber: recolecta información de los procesos activos, conexiones de red y contenidos de los dispositivos de almacenamiento no volátil. Herramienta sumamente útil, ya que comienza a relevar datos por orden de volatilidad. Esta puede ser lenta y tardar horas. Lo ideal es recolectar los datos volátiles en un sistema activo, apagar la computadora, crear una imagen del disco y ejecutar la herramienta sobre la copia del sistema de archivo.
  - Mac: puede ser utilizada junto con grave-robber o en forma aislada y permite recolectar una lista ordenada cronológicamente de las modificaciones, accesos y cambios de cada inodo, junto con su nombre de archivo. Esto facilita la correlación de datos en el análisis de las actividades efectuadas en el sistema de archivos. Se puede utilizar en cualquier sistema operativo.
  - Unrm: permite generar un solo objeto conteniendo todo lo que se encuentra en los espacios no asignados en un sistema de archivo, lo cual puede ser de un tamaño considerable. No se debe efectuar la recolección de los datos en el disco que se está analizando, porque sobrescribirá los propios datos de la investigación. Cuanto mayor

sea espacio libre, mayor será la cantidad de información.

- **The Autopsy Forensic Browser,** para analizar discos y sistemas de archivos de Windows, Unix, Linux. Es un sistema con licencia GNU General Publc License. La ejecución de Autopsy requiere la instalación previa del conjunto de herramientas Sleuth Kit. El navegador del tipo web de Autopsy es una interfaz gráfica para la ejecución de los comandos de las herramientas forenses y estándar de las utilidades Unix. Permite realizar el análisis de volúmenes y sistemas de archivos sobre los sistemas operativos Unix y Windows. Los datos se almacenan en un directorio dentro del "Evidence Locker", el cual se especifica en el momento de la instalación o al ejecutar el programa. En el modo normal, Autopsy importa un archivo de una imagen de un disco o partición. En el modo "en vivo", Autopsy puede analizar un sistema en ejecución y no almacena ningún dato en el disco rígido local. Autopsy puede generar informes o reportes de cada uno de los análisis que se efectúen, brindando información con diferentes niveles de detalle. Esta herramienta aparece también en la mayoría de los paquetes de código abierto y con software de base Linux que se ejecutan en el modo de arranque en vivo.

Herramientas de funciones específicas:

Hash – Verificación o comprobación matemática

- **Md5summer**: herramienta de código abierto con interfaz gráfica.
- **Fsum Frontend**: es una herramienta de código abierto para efectuar cálculo del hash o digesto, efectuar checksums y HMAC para archivos de texto y cadenas de caracteres.
- **DiskSig y CRCMD5:** herramienta comercial. Se incluyen un conjunto de herramientas de Informática Forense pero pueden también ser adquiridas individualmente. CRCMD5 muestra si el valor Hash se mantuvo igual o si en el caso que sea diferente, muestra los archivos que fueron modificados.
- **Md5sum.** Es un algoritmo creado por Ro Rivest, del Instituto Tecnológico de Massachussett. Consiste en un algoritmo de verificación de 128 bits. Existen aplicaciones Unix, Linux y Windows.

Borrado Seguro, limpieza y desinfección:

- **Comando dd**. Del sistema operativo Unix y versiones dd.exe para Windows.

- **Active@ KillDisk**: producto comercial que responde a los requisitos del Departamento de Defensa de los Estados Unidos e incluye el método de destrucción de Peter Gutmann, de 35 pasadas.
- **DiskScrub:** producto comercial que responde al estándar del Departamento de Defensa de los Estados Unidos de América.
- **Steganos Privacy Suite.** Contiene la herramienta Shredder, producto comercial, disponible que responde al estándar del DoD 522-22-M/NISPOM8-306 y permite seleccionar la opción de borrado de Peter Gutmann de 35 pasadas y la del borrado profundo, es decir, el borrado de los datos que pudieron almacenarse en operaciones de eliminación y escritura anterior en los espacios libres, destruyendo todos los espacios libres de la unidad.

Duplicación de discos

- **FTKImager, Forensic Toolkit Imager** crea y certifica imágenes de diferentes dispositivos.
- **Safeback**: Producto comercial, efectúa la duplicación bit a bit y genera un hash del tipo SHA 256.
- **SnapBack DatArrest**: Producto comercial que responde al estándar del NIST.
- **Ghost:** producto comercial.
- **Comando dd,** responde al estándar del National Institute of Standards and Technology.
- **AIR – Automated Image and Restore:** es una interfaz gráfica del comando dd, diseñada para la creación fácil de imágenes en informática forense.

Duplicación en forma remota

- **Netcat:** con características similares a las antes referidas pero para realizar la operación de manera remota.
- **RDA**

Manejo de particiones

- **Partition Magic:** La aplicación genera un informe del contenido de la tabla de particiones y permite examinar las particiones de un disco.
- **Gparted:** es un editor gráfico de código abierto para el manejo de particiones del dispositivo de almacenamiento.

Red

- **Network Miner.** Network Forensic Analysis Tool (NFAT) para windows.
- **Xplico:** herramienta que trabaja sobre sistemas UNIX.
- **Wireshark:** Herramienta de análisis de protocolos de red, probablemente la más utilizada al momento de la redacción del presente trabajo, por su potencialidad y facilidad de uso.

Recuperación de archivos eliminados

- **Foremost:** herramienta de línea de comando, diseñada por Jess Kornblum y Kris Kendall, graduados del MIT. Para funcionar correctamente requiere de almacenamiento externo. Permite recuperar archivos perdidos en los sistemas operativos Linux, Unix y Windows.
- **Falback:** Permite recuperar archivos en sistemas de archivos FAT12, FAT16 y FAT32. Se utiliza en sistemas operativos Linux o Unix.

Recuperación de archivos con claves

- **ElcomSoft Distributed Password Recovery:** recupera las claves de una gran variedad de aplicaciones de oficina de Microsoft, OpenOffice, PGP, Adobe pdf, claves del sistema de resguardo de Iphone, Ipad, Blackberry.

Recuperación de archivos de la papelera de reciclaje

- **Rifiuti:** permite obtener toda la información del archivo INFO2 en forma automática.
- **Debugfs:** poderosa herramienta para la recuperación de archivos eliminados.

Telefonía, celulares, PDA, GPS

- **Bitpin:** visualiza y administra información de teléfonos LG, Sansung, etc. (licencia GPL).
- **Chip IT**
- **SIMfill:** herramienta para la validación experimental de celulares.
- **Oxygen Forensic Suite** (herramienta comercial)
- **UFED Cellebrite:** herramienta comercial para la extracción de datos, análisis físico y lógico.

- **Device Seizure**: herramienta comercial para análisis de celulares, PDA y GPS

Herramienta para consulta de pertenencias de dominios

- www.lacnic.org: Registro de direcciones de internet para América Latina y el Caribe. Utilizada para establecer pertenencias de direcciones de dominios web.

Es de hacer notar que además de los equipos informáticos tradicionales (pc de escritorio, portátiles, dispositivos de almacenamiento), también los requerimientos judiciales abarcan en ocasiones el análisis sobre aparatos de telefonía celular, lo que comprende el análisis del equipo, memoria, periféricos, etc., por lo cual se han incluido algunas herramientas de mención.

Por otra parte, el incremento del uso de los servicios de las redes sociales y de servicios web como el correo electrónico gratuito, determina que habitualmente se deba requerir información relativa a datos de registración, logs de conexión e incluso solicitar copia de los mensajes, a las empresas responsables de los mismos, para poder llevar a cabo la actividad pericial.

Etapas a desarrollar durante la aplicación del Marco Tecnológico Pericial

Es importante considerar una primer etapa previa a la pericia propiamente dicha que se lleva a cabo en el Laboratorio Pericial que consiste en efectuar una preparación y comprobación de las herramientas de software y hardware a utilizar.

Esto incluirá una comprobación matemática de las herramientas de software, para lo cual se generará el hash correspondiente, guardando el resultado, para posteriormente verificar la integridad de la herramienta.

Asimismo se realizará una comprobación de los dispositivos físicos de almacenamiento, rotulando discos, limpiando y desinfectando dispositivos, y el control del resto de herramientas a utilizar.

La práctica pericial informática ante la requisitoria de una autoridad judicial, incluye una serie de etapas:

1) Acceso a los recursos informáticos sospechados, es decir el acceso al lugar físico del hecho, en donde se realizará la recolección de evidencia, o al material propiamente dicho.
2) Identificación y registro de cada uno de los elementos de la escena del peritaje, desde el ingreso al área hasta el arribo al elemento específico dubitado.
3) Autenticación, duplicación y resguardo de la prueba, que incluye la certificación matemática de la evidencia.
4) Detección, recolección, registro de indicios probatorios y cadena de custodia: en esta etapa el perito informático forense accede a la evidencia específicamente y efectúa todas las tareas relacionadas con la detección de los ilícitos, la recolección de elementos probatorios y la documentación de los formularios pertinentes de la evidencia obtenida. En esta etapa el perito informático forense determinará si el abordaje a la evidencia digital se efectuará con el equipo encendido, en tiempo real o con el equipo apagado, en el lugar del hecho o en el laboratorio.
5) Análisis e interpretación de los indicios probatorios: acorde a las circunstancias, estas actividades se realizarán en el lugar del hecho o en el laboratorio. Se utilizaran todas aquellas herramientas que permiten el análisis de la evidencia recolectada y su posterior interpretación. La reconstrucción y/o simulación del incidente se efectuará preferentemente en el laboratorio. Los datos obtenidos se documentarán.
6) Cotejo, correlación de datos y conclusiones: según la requisitoria pericial, se podrá realizar en el lugar del hecho o en el laboratorio. Se efectuaran las tareas necesarias para obtener las conclusiones que comprueben o no la concurrencia del delito, ilícito o incidente, a través de comparaciones, correlaciones y verificaciones de la integridad de los datos obtenidos. En esta etapa el perito informático forense deberá utilizar el criterio, el sentido común y los conocimientos académicos para generar conclusiones coherentes y contundentes.
7) Resguardo de herramientas de hardware y software utilizadas en la elaboración de la pericia. En esta etapa se deberá documentar todos los elementos utilizados en la pericia informática forense, resguardando el material en sitios de acceso restringido y adecuadamente protegidos.
8) Generación de informe pericial: en esta etapa el perito informático forense concluye la pericia, efectuando las acciones de revisión del escrito y comprobación de posibles errores, evitando de esta forma la omisión de datos relevantes o la inclusión de datos

superfluos o equívocos. Asimismo, de acuerdo con la naturaleza de la requisitoria judicial, el perito informático forense podrá elaborar un conjunto de medidas de respuesta a incidentes o recomendaciones.

Capítulo Nº 8: Actividades Periciales Complementarias a la realización de la pericia

En el caso de estudio que nos ocupa, el perito es llamado como perito oficial por pertenecer a una estructura que lo designa en este sentido y que normalmente está relacionada con Fuerzas de Seguridad, Policías Judiciales u organismos forenses dependientes del Poder Judicial. En este supuesto, la actividad inicial e inexcusable es la Aceptación del cargo de perito.

A diferencia de los peritos de parte, esta diligencia prácticamente no se requiere, ya que la propia actividad profesional y el cargo implican que una solicitud pericial tiene carácter de mandato y es irrenunciable (salvo en casos excepcionales), aunque en ocasiones se plasma la diligencia en un acta pertinente, y su relación estará regida por las normas administrativas del organismo del cual depende.

Finalizadas las actividades técnicas específicas, el perito debe confeccionar el informe pericial del caso, utilizándose habitualmente modelos de informes periciales clásicos. El mismo debería incluir:

- Párrafo de presentación.
- Objeto de la Pericia.
- Elementos ofrecidos o material a peritar.
- Observaciones y operaciones realizadas.
- Conclusiones
- Párrafo de cierre, elevación y recibo de devolución.

Asimismo, en el cumplimiento del mandato judicial, puede ser necesario llevar a cabo otras actividades complementarias como la realización de croquis ilustrativos, dibujos auxiliares, obtención de vistas fotográficas, etcétera.

Capítulo Nº 9: Estructura Orgánica del área Pericial de la Policía Federal Argentina. Análisis de su estructura y funcionamiento. Área Pericial Informática

La Policía Federal Argentina (PFA) es una de las principales fuerza de seguridad de la República Argentina. Fue creada el 24 de diciembre de 1943, mediante el Decreto número 17.750 sobre las bases de la antigua Policía de la Capital, que operó en el ámbito de la Ciudad de Buenos Aires desde 1880 hasta ese año y entro en funciones el 1 de enero de 1945. Como Institución de derecho que es en sí misma, en ella descansa el ejercicio de la fuerza pública del Gobierno de la Nación.

Toda su organización, despliegue, procedimientos y servicios se cumplen de conformidad de las leyes y reglamentos que regulan su existencia, las que se dictan conforme el esquema jurídico legal que tiene la Constitución Nacional y las leyes de fondo de la Nación como único marco de referencia.

Para desarrollar su labor como Auxiliar del proceso judicial, cuenta con una estructura orgánica que incluye como una de sus áreas más importantes la encargada de la actividad pericial propiamente dicha organizada bajo la denominada Superintendencia de Policía Científica.

La misma cuenta con dos Direcciones Generales: la Dirección General de Antecedentes, encargada del registro de documentos y antecedentes penales de la población; y la Dirección General de Pericias, órgano técnico científico específico.

Depende de la Dirección General de Pericias el Departamento Scopométrico, del que a su vez dependen todas las Divisiones periciales específicas: División Scopometría; División Rastros; División Medicina Legal; División Laboratorio Químico; División Ingeniería Vial Forense; División Fotografía Policial; División Balística y la División Investigación y Desarrollo Pericial, todas con asiento en la Ciudad Autónoma de Buenos Aires.

Cada una de estas se encarga de un área científico pericial específica, respondiendo a requerimientos de autoridades judiciales de distintos fueros, tanto de la Justicia Federal como de la Justicia ordinaria del ámbito metropolitano y de la provincia de Buenos Aires.

Por su parte de la División Investigación y Desarrollo Pericial dependen un total de trece

Gabinetes Científicos Periciales, distribuidos en todo el territorio de la República Argentina. Específicamente se trata de los Gabinetes Científicos Córdoba, Tucumán, Posadas, Resistencia, Jujuy, Salta, Bahía Blanca, Mendoza, Rosario, Neuquén, Comodoro Rivadavia, Concepción del Uruguay y Mar del Plata.

Dichos Gabinetes Científico Periciales fueron creados alrededor del año 1990, con el objeto de acercar a los fueros judiciales del interior del país distintas especialidades científicas para atender sus requerimientos específicos, habiendo nacido en su mayoría como Laboratorios Químicos, para posteriormente ir adquiriendo el carácter de Gabinetes Periciales Integrales, al incorporar otras áreas forenses.

En este sentido, es de destacar que el promedio de requerimientos judiciales (solicitud de asistencia en investigaciones en calidad de peritos) ronda en algunos de ellos las quinientas unidades anuales, siendo en su mayoría requeridas pericias físicas y/o químicas para coadyuvar al esclarecimiento de delitos de índole federal como, por ejemplo, el tráfico ilícito de estupefacientes.

Sin embargo, con el auge que tomó en los últimos tiempos el uso de las Tecnologías de la Información en todos los aspectos de la vida diaria y la utilización de medios digitales en la comisión de delitos, impulsaron la paulatina incorporación de personal capacitado como Peritos Informáticos en las dependencias mencionadas.

No obstante lo antes referido, la inclusión de cuadros formados en las técnicas de la Informática Forense o incluso con conocimientos ad hoc se ha efectuado de manera muy lenta, generalmente motivado en el interés propio del personal en el tema y no como un programa organizado y con continuidad en el tiempo, salvo una excepción.

Fue el caso de la conformación entre los años 2003 y 2005 de la División *Delitos en Tecnologías y Análisis Criminal* del Departamento *Técnico y Análisis para la Investigación Criminal* dependiente de la Superintendencia de Investigaciones Federales de la Policía Federal Argentina, cuando se impulsó formalmente la incorporación de personal que revistaba en otros destinos de la fuerza, pero que contase con algún grado de formación académica en áreas afines a la Informática (programadores, analistas de sistemas, licenciados, etcétera).

En la actualidad dicha dependencia realiza no solo pericias informáticas, sino que incluso

lleva a cabo investigaciones complejas en torno a Delitos Tecnológicos, a requerimiento de autoridades judiciales tanto federales como de la justicia ordinaria de la Ciudad Autónoma de Buenos Aires y de la provincia que la circunda, prestando asistencia ante probables requerimientos efectuados por jueces del interior del país.

Huelga decir que la extensión geográfica de la República Argentina, la escasez de medios y la burocracia existente, dificultan el desplazamiento de personal idóneo y redunda en mayores demoras en la sustanciación de las causas en que se requiere su asistencia.

Por otro lado, es de destacar que en concordancia con la incorporación y el ingente desarrollo de la informática en la vida diaria, el número de requerimientos originados en autoridades judiciales en relación a esta temática se ha incrementado en los últimos años. Si bien en primera instancia se pensaría que no es extendida la utilización de lo que el común de la población asume como equipos informáticos en la comisión de ilícitos, ya sea como herramienta delictiva u objeto del mismo, dicha afirmación pierde valor al analizar la utilización de un equipo tecnológico cuyo uso se encuentra altamente difundido, y el cual es pasible de peritar: el teléfono celular.

Acorde con lo informado por los registros de la Comisión Nacional de Comunicaciones, en mayo de 2012 se encontraban en uso 57.911.800 líneas de telefonía celular móvil, manteniéndose las cifras aproximadas del año anterior. Si consideramos que el censo nacional del año 2010 arrojo una población de 40.117.096 habitantes, estamos frente a una penetración tecnológica de 144,36%.

Mes de Mayo	Cantidad en miles	Variación porcentual		
		mes anterior	igual mes del año anterior	del acumulado respecto a igual período del año anterior
2011	57.860,5	0,0	5,9	7,8
2012	57.911,8	0,0	0,1	0,1

Fuente: CNC. Comisión Nacional de Comunicaciones

e: Valor estimado sujeto a rectificaciones según informes de CNC.

Servicio Telefónico Móvil Celular. Teléfonos en uso

Si bien el número de líneas en uso no se ha incrementado, la cantidad de llamadas efectuadas a sufrido un aumento de más del 20%, y el uso de mensajes SMS, un 27,5 %, en el periodo de un año, convirtiendo al uso de la telefonía móvil celular en el servicio público con mayor crecimiento y difusión.

Mes de Mayo	Cantidad en miles	Variación porcentual		
		mes anterior	igual mes del año anterior	del acumulado respecto a igual período del año anterior
2011	5.880,6	1,2	25,0	24,5
2012	7.096,1	1,5	20,7	20,8

Fuente: CNC. Comisión Nacional de Comunicaciones

Servicio Telefónico Móvil Celular. Llamadas realizadas

Mes de Mayo	Cantidad en miles	Variación porcentual		
		mes anterior	igual mes del año anterior	del acumulado respecto a igual período del año anterior
2011	7.568,7	2,7	25,4	24,0
2012	10.013,9	2,2	32,3	27,5

Fuente: CNC. Comisión Nacional de Comunicaciones

Servicio Telefónico Móvil Celular. Mensajes Cortos SMS

Obviamente, esta tendencia se mantiene e incluso aumenta a la hora de evaluar los métodos de comunicación utilizados en la comisión de delitos, debido a varios factores, entre los que se cuentan la facilidad con que se pueden adquirir tarjetas SIM en el mercado local, sin el debido control de los datos reales del presunto titular de la línea, y a la creencia extendida de que la intervención y registro de las comunicaciones móviles es mucho más compleja que la de la telefonía fija.

Consultadas fuentes de las distintas dependencias dedicadas al área pericial informática antes mencionadas, todas coinciden en referir que entre el 65 y 75 % de los requerimientos judiciales recibidos en los últimos años consisten en peritar aparatos de telefonía celular que pudieron estar implicados en la comisión de delitos de índole federal (tráfico ilícito de estupefacientes, contrabando, etcétera).

Siguiendo con esta línea de análisis se ha podido observar que los primeros meses luego de la incorporación de la especialidad de pericias en los Gabinetes Científicos del interior del país, y efectuadas las comunicaciones de rigor informando de dicha circunstancia a las autoridades judiciales federales locales, las mismas efectuaron un número pequeño de requerimientos. Con el transcurso de los meses dicho guarismo aumento considerablemente pasando de un promedio de 2,5 solicitudes por mes al iniciarse la especialidad a un promedio de 27 luego de pasados tres años.

No se descarta que dicha tendencia siga en aumento, basándonos en el Informe de Mercado de Informática y Telecomunicaciones del año 2011, publicado por la Cámara de Informática y

Telecomunicaciones de la República Argentina (CICOMRA), que indica un constante incremento en todos los tópicos analizados. Estos incluyen, entre otros, ventas de computadoras, usuarios de telefonía móvil y fija, usuarios y clientes de internet y banda ancha, registrándose en estos últimos el aumento más marcado.

Evolución Mercado TIC

2001-2011

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Mercado TIC Total	14.500	11.520	13.645	18.960	23.290	28.600	36.055	44.450	50200	60.626	80.586
Mercado TI	3.690	3.970	4.760	5.900	7.630	9.500	12.000	14.850	17.200	21.545	28.321
Mercado Telec.	10.810	7.550	8.885	13.060	15.660	19.100	24.055	29.600	33.000	39.081	52.265

Fuente:CICOMRA

Mercado TI por rubro

2000 - 2011

Rubro	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
	M $	M $	M $	M $	M $	M $	M $	M $	M $	M $	M $	M $
Hardware	1610	1100	720	1240	2100	3140	3850	5100	6267	7193	8775	11906
Software	790	680	1100	1190	1230	1400	1750	2110	2628	3044	3714	4679
Servicios	1510	1590	1800	1920	2110	2480	3090	3800	4722	5556	7223	9390
Insumos	310	320	350	410	460	610	810	990	1233	1410	1833	2346
Total	**4220**	**3690**	**3970**	**4760**	**5900**	**7630**	**9500**	**12000**	**14850**	**17200**	**21545**	**28321**

Fuente:CICOMRA

Venta de PC´s

2001-2011

AÑO	Venta de PC´s
2001	661.000
2002	110.000
2003	420.000
2004	675.000
2005	1.200.000
2006	1.400.000
2007	1.750.000
2008	1.850.000
2009	2.300.000
2010	2.800.000
2011	4.100.000

Fuente: CICOMRA

Indicadores Tecnológicos en la Argentina

2001-2011

Sector	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
INTERNET											
Clientes	1.350.000	1.430.000	1.600.000	2.045.000	2.300.000	2.800.000	3.100.000	3.900.000	4.400.000	5.000.000	5.800.000
Clientes Banda Ancha	97.000	125.000	240.000	475.000	880.000	1.590.000	2.750.000	3.300.000	3.900.000	4.700.000	5.800.000
Usuarios	3.650.000	4.100.000	5.700.000	7.560.000	10.000.000	13.000.000	16.000.000	20.000.000	23.000.000	27.000.000	31.000.000
Banda ancha móvil	-	-	-	-	-	-	-	-	-	-	1.600.000
TI											
PC´s Parque Total	3.860.000	3.800.000	4.030.000	4.400.000	5.200.000	6.000.000	7.000.000	8.200.000	9.700.000	11.500.000	15.500.000
MERCADO TIC											
Mercado TI en millones de $	3.690	3.970	4.760	5.900	7.630	9.500	12.000	14.850	17.200	21.545	28.321
Mercado Telecomunicaciones en millones de $	10.810	7.550	8.885	13.060	15.660	19.100	24.055	29.600	33.000	39.081	52.565

Fuente: CICOMRA

A esto se suma en el último año el desarrollo por parte de las operadoras de telefonía celular del mercado de la banda ancha móvil, que se está extendiendo masivamente entre los usuarios de equipos de gama media y alta, de la mano de la aparición de terminales del tipo denominado smartphone a precios accesibles. Estos últimos, son verdaderos equipos informáticos, con todas las características de computadoras, que incluso operan Sistemas Operativos que se utilizan en otros equipos como tablets y PC's, lo que aumenta su versatilidad a niveles impensables.

Asimismo, se ve incrementada la potencialidad de los mismos para ser utilizados en la comisión de ilícitos o para asegurar sus resultados, y en igual medida aumenta la necesidad de personal especializado para la prosecución de las investigaciones.

Por su parte, al consultar con funcionarios de la Justicia Federal en relación a la utilización de los servicios de especialistas en Informática Forense en las investigaciones judiciales, refirieron que en un principio no tenían un concepto acabado del campo de acción criminalística de la especialidad y de las medidas que se podían solicitar. No obstante, luego de transcurrido el tiempo y de observar los distintos informes que les remitían y los aportes que representaban en las causas que instruían empezaron a solicitar más asiduamente su incorporación como un elemento de juicio más para incorporar a la instrucción del proceso judicial.

Por su parte destacaron el incremento constante de investigaciones por infracción a la Ley Nº 26.388 de Delitos Informáticos, aguijoneadas por el impulso que cobraron en los últimos tiempos las denominadas Redes Sociales (Facebook, Hi5, Twitter), destacando que en estos casos,

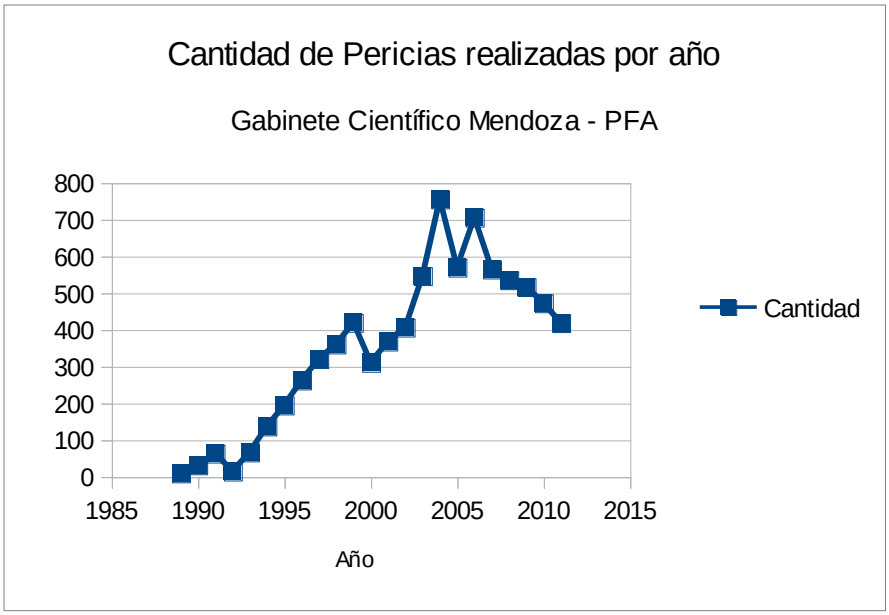
más allá de las pericias sobre equipos propiamente dicha, el auxilio de los peritos informáticos a lo largo de todo el desarrollo de la investigación se vuelve ineludible.

Cabe destacar que, se puede hacer un análisis de lo ocurrido al momento de la creación de los Gabinetes Científicos distribuidos en el interior del País en relación a los requerimientos de pericias efectuados en los primeros años de su instalación, cuando surgieron como laboratorios de pericias químicas. Haciendo las salvedades del caso, hay que tener en cuenta que la actividad de los mismos como auxiliares del sistema judicial federal principalmente se basaba en la realización de análisis de sustancias secuestradas en procedimientos policiales, para determinar si se tratan de estupefacientes.

Dicha actividad pericial es sumamente conocida por los instructores de causa federales, contando con prestigio, análisis, procedimientos y protocolos estandarizados y bien definidos.

No obstante, si estudiamos el número de pericias solicitadas, por ejemplo, al Gabinete Científico Mendoza, desde su creación, en el año 1989 hasta el año 2011, se observa que los primeros años los requerimientos eran escasos, produciéndose un incremento importante y constante con el transcurso del tiempo, para alcanzar picos de setecientos cincuenta y seis requerimientos en el año 2004, y estabilizándose la tendencia en torno a las cuatrocientas pericias anuales.

Año	Cantidad
1989	10
1990	32
1991	64
1992	15
1993	67
1994	138
1995	195
1996	263
1997	321
1998	361
1999	420
2000	311
2001	369
2002	407
2003	547
2004	756
2005	570
2006	706
2007	565
2008	536
2009	517



Si bien dicha variación podría ser la resultante de diversos factores, entre los que puede incluirse un aumento en índices delictivos y de las políticas de combate de ilícitos, también se debe incluir el afianzamiento del conocimiento y la consideración que adquieren las áreas periciales en los ámbitos judiciales, como consecuencia del nivel científico de su actividad.

Esto permite traspolar la experiencia al ámbito de la Informática Forense, y considerar que con el transcurso del tiempo la especialidad pericial adquirirá otra dimensión en los ámbitos locales.

Capítulo Nº 10: Caso de estudio. Infracción a la Ley 26.388 (Delitos Informáticos)

En este capítulo se va a describir el desarrollo de una investigación en torno a una infracción a la Ley Nº 26.388 de Delitos Informáticos, por considerarse que la misma puede ayudar a describir situaciones varias en las que el auxilio de la Informática Forense fue crucial para la resolución de la causa y la identificación positiva del presunto responsable del hecho. Si bien en primera instancia puede no parecer un hecho delictivo de trascendencia, la manera en que afectó a la víctima del mismo, tanto en su salud psíquica como en su vida laboral y personal eran de consideración.

En el mes de Febrero del 2012 es citado a comparecer en la Secretaría Penal de un Juzgado Federal del interior del país el perito informático de la dependencia de la Policía Federal Argentina con asiento en esa provincia, juntamente con personal de la brigada de investigaciones de la misma. El motivo de la citación era interiorizarlo de los pormenores de una investigación que llevaba a cabo dicho juzgado, pero que hasta el momento no había arrojado resultados significativos.

Al presentarse a la repartición judicial, el Secretario del Juzgado le informa que la causa que motiva la citación se inicia cinco años atrás cuando una persona de sexo femenino, profesional y docente secundaria, radica una denuncia en la que refiere que ha recibido llamados, mensajes de texto en su celular y en su casilla de correo personal de distintos hombres que referían comunicarse por haber tomado contacto con ella a través de distintas páginas de avisos de contactos sexuales, en las que según la denunciante nunca había publicado nada.

Asimismo, la denunciante refiere advertir que alguien, además de ella, accedía a sus cuentas de correo electrónico y de redes sociales y que enviaban mensajes de correo con fotos trucadas de ella y le endilgaban relaciones sentimentales con esposos de sus amigas.

Por otro lado, distintos contactos de ella recibieron mensajes de correo electrónico en los cuales se la acusaba de ser corruptora de menores, incluso con alumnos de ella (lo que le valio la no renovación de un contrato laboral, entre otras cosas), o denuncias de delitos ante la Administración Federal de Ingresos Públicos, lo que originó varias investigaciones e inspecciones en su hogar, siendo su profesión la de Contadora Pública.

Atento a lo expuesto, se realizó una compulsa del expediente en sede tribunalicia, al tiempo que se solicitó autorización al Juzgado Interventor para entrevistar a la víctima del hecho, para que

aporte los detalles que pudieran resultar de interés para la sustanciación de la investigación.

A continuación se realizarán unas breves reseñas de los informes periciales elevados al juzgado durante el desarrollo de la investigación en los que se pueden apreciar las medidas llevadas a cabo, los resultados obtenidos y las recomendaciones efectuadas para la prosecución de los actuados.

Primer Informe Pericial enviado

PERICIA N°: XXXX.-

MENDOZA, de 2.012.-

SR. JUEZ:

El que suscribe, xxxxxxxxxxxxx, eleva el Informe Pericial solicitado por el SR. JUEZ, Secretaría Penal de, en relación a Autos N°: xxxxx, caratulados: "Fiscal S/ Av. Inf. Ley 26.388".-

OBJETO DE LA PERICIA:

1) Constatar la existencia o no de las publicaciones en Internet que dieran origen a la presente causa.-

2) Determinar el origen de las mismas.

3) Informar las medidas necesarias para el esclarecimiento del hecho.

MATERIAL DE LA PERICIA:

Compulsa del expediente y citación de la denunciante, xxxxxxxxxxxxx, a la sede de xxxxxxxxxxxxxx de la Policía Federal Argentina.

OBSERVACIONES Y OPERACIONES EFECTUADAS:

1)- Con relación al perfil identificado como "xxxxxx", del sitio web www.contactossex.com

a)- Se coteja la existencia del mencionado anuncio, no hallándose activo en el servidor

correspondiente.

2)- Con relación al perfil identificado como “xxxxxxx2”, del sitio web www.contactossex.com

a)- Se coteja la existencia del mencionado anuncio, no hallándose activo en el servidor correspondiente.

3)- Con relación a las tareas investigativas tendientes a esclarecer el hecho, se solicitó al instructor:

- Solicite por nota a la empresa Yahoo Argentina, solicitado logs de conexión, direcciones IP de las últimas conexiones y datos de registración de las cuentas xxxx@yahoo.com.ar, yyyyyy@yahoo.com.ar y zzzzzz@yahoo.com.ar.
- Con respecto a la primera de las mencionadas, la citada xxxx@yahoo.com.ar posee como dirección IP de registración xxx.xx.xx.xx, el día 08 de Noviembre de 2011 a la 01:02:11 GMT, la cual estaría asignada acorde con el Registro de Direcciones de Internet para América Latina y el Caribe a la firma XXXXXXXXXXXXX S.A., empresa dedicada a la provisión de servicios de internet. (Anexos I y II)
- Posteriormente la instrucción elevó nota a la citada firma para que comunique que abonado de la misma usufructuó la mentada dirección en dicha fecha, informando que la misma estaba asignada a un comercio de tipo Cyber a nombre de xxxxxxxxxXXXX xxx, ubicado en calle xxxxx xxx, local 41, de la ciudad de xxxxx. (Anexo III)
- Asimismo, se solicitó a la instrucción, solicite oficios dirigidos a las firmas Google Inc. y Facebook Inc., para requerir logs de conexión, direcciones IP de las últimas conexiones y datos de registración de las cuentas, iiiiii@gmail.com, jjjjjjj@gmail.com, jjjj@gmail.com, y posteriormente de las cuentas kkkk@gmail.com, y llll@gmail.com.
- En relación al punto d) se recibió respuesta en relación a las primeras tres cuentas, la que se agrega como anexo IV.

CONCLUSIONES:

I)- Los anuncios que dieran origen a los actuados no se encuentran activos a la fecha del presente informe.

II) En relación a la investigación propiamente dicha, hasta el momento no se han podido observar coincidencias ni patrones comunes en la información recibida relativa a direcciones de internet, por lo que se consideraría oportuno mantener vigentes las cuentas de correo y perfiles de la red social Facebook obrantes en la causa, hasta tanto se reciba y analice la información pendiente de recepción, y se evalúen nuevas medidas a solicitar para la sustanciación de la causa.

Segundo Informe Pericial elevado

AMPLIACION PERICIA N°: XXXX.-

MENDOZA, de 2.012.-

SR. JUEZ:

El que suscribe, xxxxxxxxxxxxx, eleva el Informe Pericial solicitado por el SR. JUEZ, Secretaría Penal de , en relación a Autos N°: xxxxx, caratulados: "Fiscal S/ Av. Inf. Ley 26.388".-

OBJETO DE LA PERICIA:

1) Establecer el lugar desde donde se realizan las conexiones a internet investigadas en la causa.

2) Informar las medidas necesarias para el esclarecimiento del hecho.

MATERIAL DE LA PERICIA:

4) Informes remitidos por la firma Google Inc. con datos de registración e historial y logs de conexión de las casillas de correo iiii@gmail.com; jjjj@gmail.com; kkkk@ gmail.com y llll@gmail.com.
5) Informes remitidos por la firma Facebook Inc. con datos de registración e historial y logs de conexión de los perfiles http://www.facebook.com/xyz, y http://www.facebook.com/ ijk.
6) Encabezado de mensaje de correo electrónico recibido en la casilla hhhh@hotmail.com, el pasado 15 de Mayo de 2012
7) Informe remitido por la firma Informática y Telecomunicaciones S.A.

OBSERVACIONES Y OPERACIONES EFECTUADAS:

- Con relación al informe recibido de la firma Facebook Inc. se observó que se accedió al perfil de la página http://www.facebook.com/xyz el pasado 13 de Abril de 2012, a las 20:10:16 UTC, desde la dirección IP x.y.z.a, la cual estaría asignada acorde con el Registro de Direcciones de Internet para América Latina y el Caribe a la firma xxxxxxXXXXXXX S.A., empresa dedicada a la provisión de servicios de internet. (Anexo I y II)

- Asimismo, se recibió llamado telefónico por parte de la denunciante, quien informó que una amiga de ella, la señora , habría recibido el pasado 16 de Mayo de 2012, un mensaje de correo electrónico procedente de la casilla de correo xxxx@gmail.com, simulando haber sido enviado por la denunciante, por lo que es

citada a la sede de la Policía Federal Argentina, a fin de proceder con su consentimiento a la apertura de su casilla de correo electrónico.

- El día 21 de Mayo a las 10,30’ horas se presenta la Sra. , en la sede de la Policía Federal Argentina, procediéndose a la apertura de su casilla de correo electrónico hhhh@hotmail.com, y extrayendo el encabezado de un mensaje de correo electrónico recibido el día 16 de Mayo de 2012, observándose que el mencionado mensaje fue remitido desde la IP x.y.z.h. la cual estaría asignada acorde con el Registro de Direcciones de Internet para América Latina y el Caribe a la firma Google Inc., utilizando la casilla de correo xxxx**@gmail.com.** (Anexo III y IV)

- Asimismo, se efectuó observación del perfil http://www.facebook.com/xyz apreciando que el mismo día, horas 17,31’ se realizó una entrada en la sección denominada muro, en la cual publican, textualmente **“Todos contra la AFIP”.** (Anexo V)

- Posteriormente, se coteja información remitida por la firma Google Inc. en la que comunica que el pasado 16 de Mayo a las 20:45:20 UTC se realizó un ingreso a la cuenta xxxx@gmail.com, realizando la desconexión de la misma a las 20:50:51 UTC, desde la dirección IP a.b.c.d. (Anexo VI)

- Dicha dirección IP (a.b.c.d.) estaría asignada acorde con el Registro de Direcciones de Internet para América Latina y el Caribe a la firma xxxxxxxxxxXX S.A., empresa dedicada a la provisión de servicios de internet. (Anexo VII)

- Posteriormente la instrucción elevó nota a la citada firma para que comunique que abonado de la misma usufructuó la mentada dirección en dicha fecha, informando que la misma estaba asignada a la Concesionaria de una Terminal de Ómnibus. (Anexo VIII)

- Atento a lo expuesto, el pasado 24 de Mayo, horas 08,30' se mantuvo una entrevista con el Sr. , designado por el gobierno provincial como administrador de la Terminal, luego de la finalización de la concesión que mantuviera la firma antes mencionada, a quien se le consulta al tenor del uso de la infraestructura de red de la mencionada terminal de ómnibus, quien refiere que de dicha área se encarga el Sr. Mariano , quien se encontraba ausente, indicando que el mismo se comunicaría con el personal a efectos de aportar todos los datos que puedan resultar de interés para la causa.

- Posteriormente se mantiene entrevista telefónica con el Sr. Mariano, quien refire que la dirección IP a.b.c.d. es usufructuada de manera exclusiva por el comercio de Cyber existente en la terminal. Consultado al tenor del sistema de circuito cerrado de televisión y cámaras que se observaran en el predio de la estación terminal, refiere que incluso existen grabaciones en el interior del mismo comercio, por lo que se le solicita informe acerca de la posibilidad de obtener las grabaciones de video registradas por dicho sistema. Ante esto, refiere que las grabaciones solicitadas se encuentran en unos equipos que fueron reasignados a otras tareas unos días antes de la entrevista, por lo que se ofrece a realizar las gestiones necesarias para acceder a las mismas. Es así que el mismo día, aproximadamente a las 14,30' horas informa

que se puede acceder a las mismas, solicitándolas oficialmente al Sr. , representante de la firma concesionaria anterior.

- En relación a lo comunicado en informe pericial nro. xxxx de fecha de 2012, donde se comunicara que la dirección IP x.x.x.x sería usufructuada por un comercio de Ciber a nombre de , ubicado en calle , local 41, de la ciudad de , se efectuó inspección ocular en el comercio y alrededores observándose que si bien en el local no existe sistema de registro de usuarios ni de videograbación, aproximadamente a unos 30 metros de la puerta del mismo en dirección norte, más precisamente en la ochava sudeste de la intersección de calle y , se ubica una de las cámaras tipo domo utilizadas por el Centro Estratégico Operativo (C.E.O.) de la Policía local, por lo que se entabló contacto telefónico con el Comisario , de dicha dependencia, quien informara que las grabaciones del sistema de videovigilancia se mantienen por 15 días, luego de lo cual son borradas.

CONCLUSIONES:

I) En relación a la investigación propiamente dicha, se considera oportuno librar oficio dirigido al Sr. , representante de la firma concesionaria solicitando aporte al personal de la Policía Federal Argentina, las grabaciones registradas en video en el local de Ciber que utilizara el pasado 16 de Mayo de 2012, entre las 17,00' y 18,30' horas, la dirección IP a fin de compulsar las mismas en presencia de la denunciante, a efectos de determinar si en el horario referido ingresa al local alguna persona de su conocimiento que pudiera tener acceso a sus cuentas de correo y perfil de Facebook.

Tercer Informe Pericial elevado

AMPLIACION PERICIA N°: XXXX.-

MENDOZA, de de 2.012.-

SR. JUEZ:

El que suscribe, xxxxxxxxxxxxx , eleva el Informe Pericial solicitado por el SR. JUEZ , Secretaría Penal de , en relación a Autos N°: xxxxx, caratulados: “Fiscal S/ Av. Inf. Ley 26.388”.-

OBJETO DE LA PERICIA:

1) Establecer el lugar desde donde se realizan las conexiones a internet investigadas en la causa.

2) Informar las medidas necesarias para el esclarecimiento del hecho.

MATERIAL DE LA PERICIA:

8) Archivo de video con filmación obtenida por cámara de seguridad de local de ciber ubicado en correspondiente a registro de video del día 16 de Mayo de 2012 entre la hora 16:31:37 y las 19:03:08, entregado el día 04 de Junio de 2012 por el Sr. Mariano en la sede de las oficinas de la (Archivo File20120516163137.Avi). Cabe destacar que el mismo fue obtenido del Sistema de captura de video "Geo Vision 600", instalado en un servidor de la firma.

OBSERVACIONES Y OPERACIONES EFECTUADAS:

- El pasado 08 de Junio a las 14,20' horas se hace presente en la sede , la denunciante, Sra. , con el objeto de proceder a reproducir el video objeto de la pericia y consultarle si observa la presencia de alguna persona de su conocimiento.
- En determinado momento la denunciante refiere observar el ingreso al local a una persona de su conocimiento, tratándose de , titular del D.N.I. Nº , a la hora 17:18:56, acorde con el horario registrado por el sistema de video vigilancia, vistiendo camisa blanca, pantalón de jean azul y calzado color marrón, quien intercambia unas palabras con el encargado del local, para posteriormente dirigirse a la parte trasera del mismo.
- Posteriormente, la denunciante observa que siendo la hora 17:54:30 la misma persona se retira del lugar.

CONCLUSIONES:

I) En relación a la investigación propiamente dicha, se considera oportuno librar oficio dirigido al Sr. , representante de la Terminal del Sol, solicitando aporte al personal de la Policía Federal Argentina, las grabaciones registradas en video de la totalidad de las cámaras que se encontraban instaladas en la Terminal de Omnibus el pasado 16 de Mayo de 2012, en los periodos comprendidos entre las 17,00' y 17,18' horas, y las 17,54' y 18,05' horas a fin de obtener mayores registros de la persona sindicada por la denunciante, .

II) Asimismo se considera librar oficio dirigido a la empresa Facebook Inc., (sin otro aditamento) en el que se solicite informe: historial y logs de conexión del perfil correspondiente a la url **http://www.facebook.com/xyz,** desde el día 15 de Mayo de 2012 a la fecha.

Con posterioridad a lo antes referido, el Sr. Mariano informó que al acceder al sistema para obtener las grabaciones solicitadas, el mismo realizó una limpieza de registros antiguos, por los que las video filmaciones del día de interés habían sido borradas, aportando el disco rígido de la computadora en la que se encontraba el mencionado sistema a efectos de efectuar los procedimientos de recuperación de datos pertinentes.

Con el respeto de los protocolos del caso, se lleva a cabo la medida, obteniéndose otras filmaciones en las que se observa la presencia y los movimientos en el lugar de la persona referida por la denunciante, identificándola positivamente, lo que habilitó a las autoridades judiciales intervinientes a iniciar las imputaciones correspondientes.

Esto es solo una muestra de como la Informática Forense permitió arribar a un resultado favorable en la faz judicial en beneficio de una persona que se encontraba seriamente afectada por la comisión de un delito.

Capítulo Nº 11: Conclusiones y Recomendaciones

En este trabajo se ha buscado acercarnos a una temática compleja y específica dentro del campo de estudio de la Informática, como la Informática Forense y el desarrollo de la misma en el ámbito jurídico pericial en la actualidad nacional.

De esta manera se efectuó una introducción, analizando su surgimiento y desarrollo histórico, refiriendo los acontecimientos que fomentaron su evolución. Posteriormente, se realizó un análisis de su implantación en la Criminalística, y su incorporación al ámbito judicial, describiendo conceptos fundamentales de la temática como Delito Informático, lugar del hecho y Prueba Documental Informática, profundizando el análisis de esta última e indicando el valor probatorio de la misma y su vínculo con la Teoría Racional de la Prueba.

A continuación se procedió a describir los principios y reglas generales que deben regir el ejercicio de la práctica de la especialidad, para posteriormente realizar la descripción del marco tecnológico pericial, con la enumeración de las principales herramientas con que se cuenta para trabajar.

Finalmente se esbozó la estructura del área pericial informática de la Policía Federal Argentina y se realizó un análisis de su vinculación en la actividad de la Justicia Federal en lo Criminal, y su progresiva incorporación como fuente de consulta.

De todo lo expuesto se puede concluir:

- La Informática Forense es una herramienta muy importante en el desarrollo de las investigaciones de hechos ilícitos, no solo de las figuras delictivas específicas (Delitos Informáticos), sino de la generalidad de las investigaciones, como consecuencia del incremento de la utilización de las Tecnologías de la Información en la vida diaria, y del aumento asociado del uso de los servicios de comunicación digitales.
- No obstante, existe cierto desconocimiento de las potencialidades de esta herramienta criminalística por parte de las autoridades del Poder Judicial y del Ministerio Público Fiscal, razón por la cual la implantación de la misma en las distintas jurisdicciones sufre demoras, debiendo transcurrir un periodo de tiempo para que los distintos funcionarios comiencen a tomar contacto con el uso de esta herramienta y a conocer las ventajas de su

funcionalidad.

- Por otra parte, se considera que, de mantenerse la tendencia creciente en la utilización de Tecnologías de la Información, en pocos años la cantidad de recursos humanos disponibles y preparados en áreas de Informática Forense serán escasos y podría volverse dificultoso cubrir la demanda de los requerimientos que pudieran surgir.

Atento a lo expuesto, se considera oportuno intentar buscar posibles caminos de acción para paliar las dificultades antes mencionadas, en el convencimiento que la prevención es el mejor remedio y que adelantándonos a los posibles escenarios futuros va a ser mucho más efectiva y eficiente la respuesta que tengamos que aplicar.

En este sentido, se considera que desde las áreas de recursos humanos de las Fuerzas de Seguridad y los Cuerpos Forenses se deberían propiciar campañas de reclutamiento de personal con formación en Informática, al tiempo que se desarrollen programas de capacitación y perfeccionamiento en Delitos Informáticos que tengan continuidad en el tiempo, convirtiéndose en políticas institucionales con objetivos a mediano y largo plazo. Dichos programas de formación deberían incluir no solo planes de formación para personal especializado sino también cursos de introducción para el resto de los cuadros institucionales a cargo de investigaciones, ya que redundaría en una mayor compenetración de las áreas de investigaciones criminales con las posibilidades que le brinda las nuevas especialidades criminalísticas.

Asimismo, se considera que sería sumamente útil la organización de jornadas de intercambio jurídico pericial informático, que cuente con la participación de Peritos Informáticos Forenses, personal y funcionarios judiciales y efectivos de las fuerzas de seguridad encargados de la investigación de delitos, a efectos de acercar los pormenores de la especialidad a todos los actores que intervienen en los procesos de investigación criminal. Las mismas permitirían intercambiar información, actualizarse en torno a las nuevas aplicaciones y tópicos de la actividad pericial, al tiempo que favorecería el accionar mancomunado de los distintos interventores al participar de un espacio común que les permita interactuar y conocerse.

Dichas medidas, si bien pueden presentar sus dificultades desde el punto de vista burocrático y administrativo, requieren principalmente de voluntad y del compromiso por parte de los responsables de implementar políticas institucionales que permitan fomentar el surgimiento de mecanismos que apunten a promover el desarrollo de cuadros más profesionales y eficientes, y

lograr una mejora constante y sustancial en la investigación criminal, con el consiguiente beneficio para el conjunto de la sociedad.

Bibliografía

AIRALA, A. (2002) La informática Forense. *Policía y Criminalística, 344 (11).* 32-39

CANO MARTINEZ, J. (2009). Computación Forense. México D.F. Alfaomega Grupo Editor

CASEY, E. (2000) Digital Evidence and Computer Crime. Academic Press. Op.Cit.

DARAHUGE, M. (2011). Manual de Informática Forense. Buenos Aires. Errepar.

TELLEZ VALDES, J. (2008) Derecho Informático (4ª Edición). México. McGRAW-HILL/INTERAMERICANA EDITORES.

TOBARES CATALÁ, A. y CASTRO ARGÜELLO, M. (2010) Delitos Informáticos. Córdoba. Advocatus

VAZQUEZ ROJAS, M. (2008) La prueba informática desde la teoría racional de la prueba. *Policía y Criminalística, 376 (21).* 14-27

Sitios públicos consultados

www.first.org (Febrero 2013)

www.arcert.gov.ar (Febrero 2013)

www2.opensourceforensics.org (Febrero 2013)

www.porcupine.org/forensics/tct.html (Febrero 2013)

www.lacnic.org (Febrero 2013)

ANEXOS

Modelo de Informe Pericial sobre Equipos Informáticos

PERICIA N°: -----12/GCM.-

MENDOZA, 24 de Abril de 2.012.-

SR. JUEZ:

El que suscribe, XXXXXXXXXXXXXXX, eleva el Informe Pericial solicitado por el SR. JUEZ XXXXXXXXXXXXXXX, Secretaría Penal de la DRA. XXXXXXXXXXXX, en relación a Autos N°: XX.XXX-C, caratulados: "Fiscal S/ Av. Delito".

I - OBJETO PERICIAL.-

La presente peritación tiene por objeto analizar el material que se acompaña a los fines de determinar si el mismo podría ser utilizado en la grabación y copias de Cds originales.-

II - ELEMENTOS OFRECIDOS.-

A tal fin, del total de los elementos recepcionados en este Gabinete, solo se describen aquellos que son objeto del análisis pericial:

UNA (1) caja de cartón en la que se lee impreso comercialmente "COMPUTER KITS..." y manuscrito en uno de sus laterales se lee "201-Z-05", cerrada con cinta engomada transparente, que tiene adherido trozos de cinta engomada transparente con la leyenda "FRAGIL" y UNA (1) hoja de papel blanco en la que se lee "193-P-05", donde se halla UN (1) gabinete de computadora color blanco en el que se lee "PanoramiC... 3744233-A22", con su tapa colocada sin sus correspondientes tornillos, en el cual se observa UNA (1) disquetera de 3 1/2" y UNA (1) lectora _ grabadora de Cds, ambos instalados en su parte delantera.

Se somete el material antes descripto a las operaciones de rigor.-

III - OPERACIONES REALIZADAS.-

1) Comprobación de características del Gabinete (CPU): El mismo consta de un procesador Intel Celeron con una velocidad de 600MHz, con una memoria RAM de 192 Mb y un sistema operativo instalado de Windows 98.

2) Búsqueda de Programas para ser utilizados en la grabación de Cds: Se encontraron DOS (2) programas compatibles con la utilización de la grabadora de Cds que se describen a continuación: A.- "Clone CD versión 4.2.0.2" el cuál es utilizado en copia directa de un CD a otro, para lo cual realiza una imagen en el disco rígido de la PC la cual luego es grabado en un CD virgen y B.- "Nero versión 6.0" este es utilizado en la grabación de Cds de todo tipo de formatos, con la posibilidad de tomar archivos de audio del tipo MP3 u otros del disco rígido y

convertirlos a formato de CD de audio para posibilitar su lectura en cualquier tipo de equipo de música; se deja constancia que este último es una versión de prueba o gratuita, la cual se hallaba vencida al momento de esta pericia por lo cual no permitía el uso del mismo con sus funciones, no pudiéndose determinar la fecha exacta de vencimiento de la misma.-

3) Búsqueda de carpetas con archivos de formato de audio y video: Se encontraron las siguientes carpetas con los contenidos que se describen a continuación:

A.- "D:\MUSICA" la cual posee en su interior otras carpetas con archivos en formato MP3 de audio.

B.- "D:\1-CLAUDIA\GRABACIONES" la cual posee en su interior archivos en formato MP3 de audio y MPG de películas comprimidas.

4) Comprobación del funcionamiento de la grabadora: Para ello se utilizó el programa de grabación "Clone CD" antes mencionado y UN (1) CD con archivos de texto. Estos archivos fueron tomados por la grabadora, y luego crea una imagen del mismo en el disco rígido, para luego ser grabados mediante el mismo programa en UN (1) CD marca Imation, el cual se devuelve junto con esta pericia, comprobándose el correcto funcionamiento de la Grabadora.-

- CONCLUSIONES.-

A raíz de los estudios realizados, el suscripto se encuentra en condiciones de ofrecer las siguientes conclusiones:

El CPU analizado se encuentra funcionando en correctas condiciones, y el mismo posee programas de grabación capaces de realizar copias de Cds originales o no originales a un nuevo CD según figura en el apartado III del presente informe.-

Se comprobó el correcto funcionamiento de la Grabadora de Cds inserta en el CPU según consta en el apartado III del presente informe.-

Es cuanto puedo informar.- Se agrega en devolución CD utilizado en prueba de grabación. Se adjunta en devolución el material detallado en el apartado II.-

Modelo de Informe Pericial sobre Aparatos de Telefonía Celular y Chips

PERICIA N°: -----12/GCM.-

MENDOZA, 24 de Abril de 2.012.-

SR. JUEZ:

El que suscribe, XXXXXXXXXXXXXXX, eleva el Informe Pericial solicitado por el SR. JUEZ XXXXXXXXXXXXXXX, Secretaría Penal de la DRA. XXXXXXXXXXXXX, en relación a Autos N°: XX.XXX-C, caratulados: "Fiscal S/ Av. Delito".

I - OBJETO PERICIAL.-

La presente pericia tiene por objeto analizar el contenido de datos del material que se acompaña a los fines de realizar una descripción detallada del mismo.-

II - ELEMENTOS OFRECIDOS.-

A tal fin, se describen aquellos elementos recepcionados en este Gabinete que son objeto del análisis pericial:

UN (1) sobre de papel manila abierto en el que se lee "SOBRE Nº 6", continente de:
UN (1) celular color gris marca comercial "NOKIA" con chip el cual se denomina en adelante como "CEL1",
UNA (1) tarjeta SIM de la empresa "CLARO" la cual se denomina en adelante como "CHIP 1",

Se somete el material antes descripto a las operaciones de rigor.-

III - OPERACIONES REALIZADAS.-

1) Comprobación de características del celular: detallado en el apartado IV del presente informe.-

2) Búsqueda de Registro de llamadas entrantes, salientes y llamadas perdidas: detallado en el apartado IV del presente informe.-

3) Búsqueda de mensajes de texto entrantes y salientes: detallado en el apartado IV del presente informe.-

4) Búsqueda de Registro almacenados en el Organizador de Agenda: detallado en el apartado IV del presente informe.-

5) Búsqueda de contactos telefónicos: detallado en el apartado IV del presente informe.-

6) Determinación de titularidad y Número Telefónico: NO se puede establecer con los

métodos disponibles en este Gabinete.-

7) Obtención de Número de Serie del Chip: detallado en el apartado IV del presente informe.-

8) Análisis de Carpetas: detallado en el apartado IV del presente informe.-

IV- CONCLUSIONES.-

A raíz de los estudios realizados, el suscripto se encuentra en condiciones de ofrecer las siguientes conclusiones:

"CEL 1":

EL TELEFONO CELULAR ANALIZADO CORRESPONDE AL MODELO "GD330" DE LA EMPRESA "LG" Y POSEE ALMACENADOS LOS SIGUIENTES DATOS, DISCRIMINADOS EN CUADROS POR RUBROS:

LLAMADAS RECIBIDAS			
FECHA	**HORA**	**NÚMERO ORIGEN**	**NOMBRE DE CONTACTO**

LLAMADAS REALIZADAS			
FECHA	**HORA**	**NÚMERO DESTINO**	**NOMBRE DE CONTACTO**

CONTACTOS DE AGENDA			
NOMBRE	**NUMERO**	**NOMBRE**	**NUMERO**

BUZON DE ENTRADA DE MENSAJES DE TEXTO		
PROVENIENTE DE:	**FECHA Y HORA:**	**TEXTO**

ELEMENTOS ENVIADOS DE MENSAJES DE TEXTO		
DESTINO:	**FECHA Y HORA:**	**TEXTO**

ORGANIZADOR – CALENDARIO		
Fecha Recordatorio	**Rango Horario**	**Texto**

EN CUANTO A LA TITULARIDAD DE LA LÍNEA Y SU NÚMERO TELEFÓNICO NO PUDIERON ESTABLECERSE LOS MISMOS CON LOS MÉTODOS DISPONIBLES EN ESTE GABINETE.-

El CELULAR EN CUESTION POSEE INSTALADO UN CHIP PERTENECIENTE A LA EMPRESA "CtiMovíl" (Claro) Y CUYO NUMERO DE IDENTIFICACION ES EL "xxxxxxxxxxxxxxxxxxx".-

SE ANALIZO EL CONTENIDO DEL CELULAR EN DONDE SE HALLARON UN TOTAL DE VEINTIOCHO (28) FOTOGRAFÍAS FAMILIARES DE BAJA CALIDAD LAS QUE SE HALLAN GRABADAS EN LA MEMORIA INTERNA DEL APARATO.-

SE DEJA CONSTANCIA QUE EL CELULAR ANALIZADO POSEE PROBLEMAS MECÁNICOS EN LA TECLA NAVEGADORA CENTRAL.-

"CHIP 1":

El CHIP ANALIZADO PERTENECE A LA EMPRESA "Claro" CON NUMERO DE IDENTIFICACION "XXXXXXXXXXXXXXXXXXX" Y POSEE ALMACENADOS LOS SIGUIENTES DATOS, DISCRIMINADOS EN CUADROS POR RUBROS:

CONTACTOS DE AGENDA			
NOMBRE	**NUMERO**	**NOMBRE**	**NUMERO**

BUZON DE ENTRADA DE MENSAJES DE TEXTO		
PROVENIENTE DE:	**FECHA Y HORA:**	**TEXTO**

ELEMENTOS ENVIADOS DE MENSAJES DE TEXTO		
DESTINO:	**FECHA Y HORA:**	**TEXTO**

EN CUANTO A LA TITULARIDAD DE LA LÍNEA Y SU NÚMERO TELEFÓNICO NO PUDIERON ESTABLECERSE LOS MISMOS CON LOS MÉTODOS DISPONIBLES EN ESTE GABINETE.-

Es cuanto puedo informar.- Se adjunta en devolución el material detallado en el apartado II**.-**