CAPÍTULO 1

ANTECEDENTES Y TERMINOLOGÍA DEL CÓMPUTO FORENSE (CF) O INFORMÁTICA FORENSE (IF)

CÓMPUTO FORENSE

Capítulo 1 ANTECEDENTES Y TERMINOLOGÍA DEL CÓMPUTO FORENSE (CF) O INFORMÁTICA FORENSE (IF)

1.1 CÓMPUTO FORENSE (CF) O INFORMÁTICA FORENSE (IF).

El Cómputo Forense está adquiriendo una gran importancia dentro del área de la información debido a que actualmente la mayoría de las personas almacenan la información en medios digitales, como un disco duro, memorias USB , Ipad , iPod, memorias externas, memorias de cámara, celulares, etc., es decir, todo aquel dispositivo que pueda almacenar información. Esto ha dado auge al desarrollo de nuevos espacios como las telecomunicaciones.

Hoy en día el internet se ha involucrado en la vida cotidiana de la mayoría de la gente: el uso de las computadoras por parte de las compañías de negocios, cuentas de correo, transacciones bancarias etc. Lo cual abre paso a un nuevo campo de investigación criminal denominado CF que consiste en recuperar la información de una evidencia de una manera confiable y sobretodo que sirva para sustentar un caso de manera legal, es importante resaltar que actualmente en México no existen leyes que regulen un procedimiento Informático Forense.

La IF ayudar a resolver grandes crímenes, en este contexto, la escena del crimen es la computadora y la red a la cual está conectado. Cuando se realiza un crimen informático, la evidencia de modificaciones, alteraciones que sufra una base de datos, un sistema de redes o ataques internos queda guardada en dispositivos digitales (Xombra, 2012), el aprovechamiento de las fallas tecnológicas sobre infraestructuras es un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos, esta información es analizada por la Informática Forense utilizando procedimientos y herramientas adecuadas para analizar y recabar la prueba verídica que de fé de algún hecho sospechoso y tal motivo encuentre a la persona que es culpable.

En una entrevista realizada al Doctor Jeimy J. Cano sobre "¿Cuánto se puede tardar en reunir las suficientes pruebas o evidencia para dar con la persona que es autor de un ataque? Responde al respecto:

"Es una pregunta complicada de responder, pues muchas veces el informático forense debe prepararse para fallar en identificar a la persona real que cometió el ataque. Pues la versatilidad que ofrece Internet para enmascarar direcciones IP, correos electrónicos, entre otros aspectos, sugiere un gran conocimiento técnico y paciencia por parte de los atacantes, los cuales también consideran estrategias "anti-forenses" que limiten las investigaciones y la efectividad de las mismas. La recolección de pista puede ser demorada, algunos casos pueden llevar años en esta labor." (Cano, 2006)

Por lo tanto el tiempo que se tarda en encontrar una evidencia y a la persona que es autor de un ataque depende del tipo de evidencia y de las diferentes herramientas que se empleen para detectar la anomalía o intrusión en los sistemas informáticos.

El CF es una ciencia relativamente nueva, los países en los que tiene mayor auge son Argentina, Colombia, Bolivia, Venezuela, España y Estados Unidos, en estos países la IF ya está regulada dentro del marco de la ley y es válida como evidencia digital presentada en un caso legal. El especialista de la IF debe poseer sólidos conocimientos técnicos, prácticos y conocer las herramientas de uso a emplear, estar al día en bugs (vulnerabilidades) de sistemas (sistemas operativos, software y hardware) (Cano, 2006).

1.2 ORIGEN

El mundo va cambiando día con día, de igual manera evolucionan los avances tecnológicos, la sociedad y también sus delitos informáticos, esto origina nuevas necesidades de fortalecer las normas jurídicas en materia penal, la eficacia y eficiencia de una mejor calidad de vida dentro del ámbito nacional e internacional. De este problema o mal social es de donde surge la Informática Forense.

A finales del siglo XX, los sistemas informáticos se convirtieron en las herramientas más poderosas para todas las personas o empresas, esta situación ha llamado la atención de auditores, investigadores, especialistas debido a que con el empleo de estas nuevas tecnologías que utilizan al máximo sus ventajas de productividad, puedan ser vulnerables de algún mal uso, el comercio electrónico aumenta los accesos a las redes de las empresas y la información corporativa necesita estar protegida de forma más fiable e incluso necesita de un mayor grado de control. El robo de información en las empresas y de la propiedad intelectual es una de las mayores áreas del delito corporativo por lo que hay que poner especial cuidado (Areritio, 2008) .

La evolución tecnológica hoy en día, está sumida en la gestión integral de la empresa y por eso las normas y estándares propiamente informáticos deben estar presentes en ella, en consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa.

Cabe aclarar que la tecnología no gestiona propiamente a la empresa, sino que ayuda a la toma de decisiones, actúa como un apoyo dentro de la organización, debido a que a través de una auditoría se monitorea el cumplimiento de normas y procedimientos, permitiendo así cotejar una información veraz, pues está basada en el resultado del cumplimiento de ciertas normas establecidas dentro de la empresa. Es por eso, que debido a su importancia en el funcionamiento correcto de los procesos dentro de una empresa, existe lo que hoy se conoce como Informática Forense.

El Cómputo Forense no sólo se ha transformado en una disciplina clave en la investigación, también es utilizada para asegurar los organismos de control y transparencia de las empresas, de tal manera que la seguridad de realizar una copia forense de la empresa sirva para la prevención de algún mal manejo, ya que es una forma de tener una copia detallada de cada uno de los movimientos que se han hecho en los sistemas, ya sea transacciones electrónicas, e-mail, actualización de información, etc. (Cano, 2010)

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garantizar la verdad de la evidencia digital que se pudiese aportar en un procedimiento judicial (Noblett, 2000). Desde 1984, el Laboratorio del FBI (Buro Federal de Investigaciones) y otras agencias que persiguen el cumplimiento de la ley, empezaron a desarrollar programas para examinar evidencia en medios digitales y electrónicos.

Frecuentemente se pueden extraer de los sistemas de computación transacciones de negocios privados, comunicaciones con cómplices, indicadores de fraude, etc. A menudo todos los intentos de los delincuentes y de los atacantes para ocultar o borrar sus evidencias tienen éxito y un pequeño detalle obtenido por un forense, puede ser la clave para sacar a la luz y probar un delito (Areritio, 2008); el informático forense debe recabar todo tipo de evidencias para poder demostrar delitos y mejorar la seguridad de una organización.

1.3 CASOS DE CÓMPUTO FORENSE

La informática forense se basa en hechos premeditados para recabar pruebas y luego analizarlas. El análisis forense en sistemas informáticos, se apoya de aplicaciones que tengan un papel importante para recaudar la información y pruebas necesarias. Es posible investigar (aún cuando internet permite el anonimato y el uso de nombres falsos) quién es el dueño de sitios web, quiénes son los autores de determinados artículos y otros documentos enviados a través de redes o publicados en la misma, las modificaciones, alteraciones e incluso la destrucción de los datos y otros manejos dolosos de bases de datos de redes internas o externas. El rastreo depende en sí de quién y cómo realizó el ataque o cualquier otra acción, es posible buscar atacantes exteriores de sistemas e incluso se conocen casos donde se ha determinado la autoría de virus, los hábitos de los usuarios de los computadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, haciendo posible saber de todas las actividades realizadas en un computadora determinada (Xombra, 2012).

Las imágenes digitales y otros medios audiovisuales pueden estar protegidos no sólo por derechos de autor (copyright) sino por las llamadas marcas de agua digitales que sirven para determinar el origen del archivo aunque hayan sido modificados para disfrazarlos y darle una apariencia distinta, son frecuentes las inspecciones judiciales sobre páginas Webs y archivos, tendientes a la fijación de hechos que ocurren dentro del vasto mundo electrónico digital.

Para realizar este análisis forense se necesita de personas que tengan un amplio y sólido conocimiento del uso de herramientas forenses, dispositivos de hardware, software de incursión en redes, a estas personas normalmente se les llama Informáticos Forenses.

A continuación se enlistan algunos casos prácticos en los que se ha aplicado un procedimiento forense:

- El caso de Joe Jacob's (Manzo, 2008), que fue juzgado en NY por distribución de drogas en diferentes escuelas, el juez que llevó su caso necesitaba evidencia para condenar a esta persona por tráfico de droga, así como saber quién era su proveedor. Se obtuvo como evidencia un diskette, en éste contenía información oculta, por este motivo se empleó la informática forense, el objetivo era encontrar información del nombre del proveedor de marihuana de Joe Jacob's, su dirección y saber si la escuela secundaria de Smith Hill que Joe Jacob's frecuentaba era la única en la que distribuía drogas.

  Haciendo uso de las herramientas de la informática forense, con el análisis forense se encontró en el diskette un archivo que fue eliminado, se restauró y así se dió con el nombre del proveedor de drogas de Joe Jacob's, llamado Jimmy Jungle, su dirección y el nombre de las escuelas y los días en que distribuía la droga.

YanapTI (Empresa Boliviana de Informática Forense) (YanapTI, 2009b) ha participado en casos para esclarecer hechos por ejemplo de entidades financieras, robos de tarjetas de crédito o de débito, manipulación de cajeros

automáticos, manipulación cajas de ahorro, homicidios, análisis de celulares y casos de destrucción de información y así determinar la gravedad del borrado de información, así como si es intencional determinar la magnitud de la destrucción de la información; a continuación su descripción:

- Un caso de fraude que involucra dos jurisdicciones Argentina y Chile el gerente que administraba a la empresa en los dos países era sospechoso de tener un acuerdo de los precios con proveedores y éstos lo favorecían de manera personal, ya se habían hecho auditorias en varias ocasiones, telemarketing, análisis de precios de mercado que proveía a la empresa y nada se encontraba entonces se realizó una adquisición forense en su computadora y se recuperó un documento que había escrito y no lo había guardado pero lo había impreso y daba información de cuentas y activos en el extranjero en Europa que él había adquirido y que marcaba que sus ingresos como gerente no correspondían con ese documento que decía que tenía cierto patrimonio.

  Aquí se demuestra que la informática forense es una herramienta muy eficiente para investigar. Es muy importante resaltar que los procedimientos de la informática forense deben ser muy claros y que garanticen a todas las partes, especialmente en este caso al gerente, que la información de su computadora no fue alterada y se obtuvo que nadie introdujo ese documento; así mediante el análisis forense tener la certeza que cualquier otro perito que haga la investigación compruebe que este documento no fue modificado (YanapTI, 2009a).

- Otro caso de fraude fue el de un gerente de una empresa multinacional que intercambiaba información sensible con la competencia, entonces de alguna manera robaba información; se realizó una auditoría y una investigación previa porque se sospechaba de esta situación, pero no se encontró nada, se hizo una copia forense del disco duro, se resguardó el disco notarialmente, entonces el peritaje encontró en su carpeta de correo electrónico correos que enviaba desde su cuenta corporativa

aparentemente a su hija, parecía ser un correo sencillo diciendo "*que bonito paseo de la semana pasada te mando las fotos*", y del análisis forense que se hizo se detectó que no era un archivo con fotos sino archivos de hojas de cálculo y documentos con información que probaban el delito por el cual había sido sancionado (YanapTI, 2009a).

1.4 TERMINOLOGÍA

En el presente trabajo de investigación se hace referencia a esta disciplina como Cómputo Forense (CF) o Informática Forense (IF) como términos totalmente iguales.

El Cómputo Forense es una disciplina que no sólo hace uso de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y de sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido, también ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats (Noblett, 2000), el hecho de darle doble clic a un archivo modificaría la última fecha de acceso (Xombra, 2012). Es importante localizar toda aquella evidencia que aclare un mal uso de la información, no importa que haya sido borrada, el proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información.

Es muy importante mencionar que la IF no tiene parte preventiva, es decir, no se encarga de prevenir delitos, para ello se encarga la seguridad informática, es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática (Xombra, 2012):

- **Seguridad informática:** Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un

sistema de información seguro y confiable. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas, este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Otro término dentro del contexto de la Informática Forense es:

- **Auditoría informática:** Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los

mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Otros términos relacionados con el CF son:

- **Jurisdicción** (Palomar de Miguel, 2000)**:** Es la facultad que tiene el estado para administrar justicia en un caso concreto por medio de los órganos judiciales instituidos al efecto.
- **Informático Forense:** Persona que emplea sus conocimientos del uso de herramientas forenses en dispositivos de hardware, software y redes, para esclarecer un hecho.
- **Evidencia:** Prueba digital que va ha ser analizada por alguna herramienta forense.
- **Pista:** Evidencia para esclarecer algún hecho en el que se ha incurrido un delito.
- **Análisis Forense:** Procedimiento que utiliza las etapas del CF ayudado de las herramientas forenses para esclarecer una evidencia.
- **Estado Íntegro:** Momento en que la evidencia no sufre ninguna alteración.
- **Estado comprometedor:** Momento en que la evidencia sufre alteración causando algún daño.
- **Cadena de Custodia** (López, Haver, & León, 2001): La identidad de personas que manejan la evidencia en el tiempo del suceso y la última revisión del caso. Es responsabilidad de la persona que maneja la evidencia asegurar que los artículos son registrados y contabilizados durante el tiempo en el cual están en su poder, y que son protegidos, llevando un registro de los nombres de las personas que manejaron la evidencia o artículos con el lapso de tiempo y fechas de entrega y recepción.
- **Imagen Forense**: Llamada también "Espejo" (en inglés "Mirror"), la cual es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos y las áreas borradas incluyendo particiones escondidas.

- **Análisis de Archivo**: Examina cada archivo digital descubierto y crea una base de datos de información relacionada al archivo (metadatos, etc.), consistente entre otras cosas en la firma del archivo o hash (indica la integridad del archivo), autor, tamaño, nombre y ruta, así como su creación, último acceso y fecha de modificación.
- **Análisis Forense Informático**: Se puede definir como el proceso de aplicar el método científico a los sistemas informáticos con la finalidad de asegurar, identificar, preservar, analizar y presentar la evidencia digital de forma que sea aceptada en un proceso judicial (Colobran, Arqués, & Galindo, 2008).

1.5 IMPORTANCIA Y OBJETIVOS

Hikal (2009) cita que la importancia que tiene el CF es:

"Que se enfoca a aquellos casos en los que se utiliza el equipo de cómputo como medio para cometer una conducta presuntamente delictuosa así, como cuando el equipo es violentado en sus partes lógicas (programas) o en sus partes físicas".

Con la finalidad de averiguar qué ha ocurrido y quién ha sido el presunto autor relacionado con el uso de las tecnologías de información se utiliza una disciplina establecida entre el marco jurídico y la tecnología denominada Informática Forense.

El objetivo de un análisis forense (Xombra, 2012) es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios los acontecimientos que tuvieron lugar desde el mismo instante en el que el sistema estuvo en su estado integro hasta el momento de detección de un estado comprometedor, tomando en cuenta los siguientes puntos (Gutiérrez, 2006):

- La importancia que tiene el Cómputo Forense
- La compensación de los daños causados por los criminales o intrusos
- La persecución y procesamiento judicial de los criminales

- El uso de herramientas de la informática forense para averiguar qué ha ocurrido, mediante la recolección de evidencia

Éstos deben ser llevados a cabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta la información contenida de la evidencia hasta que se obtengan todas las pruebas posibles.

1.6 DEFINICIÓN

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. El término *computer forensic*, proceso forense, informática forense o *forensic computing* en el esquema de certificación CISSP (Certified Information Systems Security Professional) hace referencia a:

"Una ciencia, técnica o disciplina relacionada encargada de la investigación de los delitos y abusos relacionados que tienen que ver con los computadores y con las redes que los conectan, de una manera repetible y competente" (Areritio, 2008).

A continuación se citan algunas definiciones de diferentes autores sobre el Cómputo Forense:

Para Juan Carlos Guel (2012), jefe del Departamento de Seguridad en Cómputo de la Dirección General de Servicios de Cómputo Académico y Coordinador del Equipo de Respuesta a Incidentes en Seguridad en Cómputo UNAM, señala:

"La Informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo".

Es decir, el cómputo forense opera diversas herramientas informáticas para determinar el estado de un sistema luego de que sus medidas de seguridad

han sido sobrepasadas y vulneradas, con la finalidad de encontrar evidencias que permitan definir, con toda certeza, los mecanismos que los intrusos utilizaron para acceder a ella, así como de desarrollar las mejoras y/o técnicas que deben seguirse para evitar futuras incursiones ajenas en el sistema.

Para el FBI (2012) es:

"La ciencia que aplica de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional".

Javier Areritio Bertolín (2008) lo define como:

"*El proceso mediante el cual se identifican, preservan, analizan y presentan las evidencias digitales de manera que sean aceptables legalmente en una vista judicial o administrativa*" (Areritio, 2008).

Para G.Noblett, Michael (2000):

"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 las hipótesis relacionadas con el caso; o como la 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".

Hikal (2000) la define como:

"*Disciplina que aplica conocimientos técnicos y científicos relacionados al estudio de las computadoras, incluyendo:*

- *Diseño*
- *Funcionamiento*
- *Métodos de almacenamiento*

- *Uso de la información presentada en internet combinando aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano".*

Para Gómez L. y Del Neuquén P. J (2004):

"*El proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable"*.

Finalmente con base en las definiciones anteriores se puede decir que el CF es:

"Una disciplina que se encarga de analizar evidencias digitales para reconstruir hechos pasados y haciendo uso de sus herramientas forenses, ayuda a encontrar las pruebas clave para esclarecer un hecho en el que se ha incurrido en un delito".

Esta definición es considerada de aquí en adelante en este trabajo.

1.7 CLASIFICACIÓN DE LOS DELITOS EN EL CF

Ya se han dado algunas experiencias en Venezuela y otros países de habla hispana, uno de los más destacados es España, en donde se ha solicitado la determinación de la autenticidad e integridad de los datos, por ejemplo de mensajes de e-mail pudiéndose relacionar con un remitente, dirección de correo, computadora y hasta con una persona determinada e inclusive la relación entre estos elementos y los datos anexos (attachments) que se encontraban en el e-mail almacenado previamente en el equipo incurso (Xombra, 2012).

El eje central de los delitos informáticos se da en la manipulación de los datos de entrada, programas y salidas de computadoras, así como la falsificación de los sistemas informáticos y el espionaje de información, estos elementos producen en una persona un daño en su patrimonio, por ejemplo en el Código Penal brasileño se tipificó el delito de inserción de datos falsos en sistemas de

información y el delito de modificación o alteración no autorizada de sistemas de información de la administración pública (Ramos Junior, 2008).

Existen delitos que se cometen a través de Internet y causan afectación a bienes jurídicos de diversa naturaleza y se clasifican de la siguiente manera:

A). Delitos patrimoniales

De acuerdo con la información que proporciona Banamex, Citybank, el fraude electrónico causa una gran afectación a los usuarios de la banca, siendo el país de los Estados Unidos el principal blanco de dichos ataques, con un cincuenta y dos por ciento, los ataques informáticos se generan en contra de los clientes y no en contra de la institución que los acredita, lo que obedece a que los sistemas de protección que gozan las instituciones bancarias, tales ataques se llevan a cabo a través de dos programas que se denominan: *Phising* (Delito de estafa cibernética) y *Pharming* (Persona que suplanta una vulnerabilidad de software) el propósito de esos programas es hacerse de los recursos del usuario del banco (Consejo de la Judicatura Federal, 2008).

Ante los ataques de los defraudadores cibernéticos se han instrumentado sistemas básicos de protección que debe tener cualquier usuario de Internet:

- Tener una herramienta antivirus vigente y actualizado.
- Poseer herramientas anti-intrusos.
- Tener un firewall personal.
- Tener autorizados parches de seguridad, y
- Controlar las entradas y salidas de las unidades USB y disquetes para evitar las descargas de impresiones fotográficas.
- No compartir el e-mail.
- No enviar información confidencial.
- No dar clic a ligas adjuntas a e-mailes, y
- Proteger siempre el equipo con antivirus.

A los esfuerzos de esta institución bancaria se añade la unidad ICRAI su objetivo es el análisis de los sistemas informáticos a través del CF, realizan

análisis de las computadoras, revisión de las computadoras en el momento en que se están utilizando y detectan los fraudes cibernéticos.

Para proteger este delito hay una reciente reforma al artículo 52 de la Ley de Instituciones de Crédito, en la que se establece que:

"Las instituciones de crédito pueden suspender o cancelar el trámite de operaciones en los casos en que su clientela pretenda realizar el trámite de operaciones mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, cuando cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida"

Esta reforma resulta sin lugar a duda de un gran apoyo legal al usuario desprotegido en el mundo del Internet.

B) Delitos de pornografía

El Código Penal Federal (Alfaomega, 2012) en su artículo 201 establece el tipo descriptivo consistente en que:

"Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa".

"La misma pena se impondrá a quien con fines de lucro o sin el, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieran las acciones anteriores".

"De igual manera se establece la pena de prisión de ocho a dieciséis años, a quien por sí a través de terceros, dirija administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de dieciocho años, en el

mismo precepto en su parte define como pornografía infantil, la representación sexualmente explicita de imágenes de menores de dieciocho años".

C) Delincuencia organizada

En aquellos casos de que la averiguación previa de alguno de los delitos a que se refiere la ley contra la delincuencia organizada, o durante el proceso respectivo, el Procurador General de la República o el titular de la Unidad Especializada consideren necesaria la intervención de comunicaciones privadas, lo solicitarán por escrito al Juez de Distrito, expresando (Alfaomega, 2012):

"El objeto y necesidad de la intervención, los indicios que hagan presumir fundadamente que en los delitos investigados participa algún miembro de la delincuencia organizada, así como los hechos, circunstancias, datos, y demás elementos que se pretenda probar".

Las solicitudes de intervención deberán señalar:

"A la persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizarán; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención" (Alfaomega, 2012).

"Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores".

Los delitos informáticos son importantes para la IF porque permite amparar alguna evidencia que encuentre a una persona culpable y permita mediante reformas de ley dar un seguimiento judicial.

CAPITULO 2

CÓMPUTO FORENSE

Capítulo 2 CÓMPUTO FORENSE

El CF permite analizar dispositivos de hardware, software y las redes a las cuales están comunicados haciendo uso de herramientas forenses que permiten esclarecer un hecho. En este contexto se presentan las herramientas que usa el CF, etapas para realizar un análisis forense, las ventajas que tiene la IF con el uso de herramientas forenses y lo que se espera en un futuro.

2.1 DISPOSITIVOS A ANALIZAR EN EL CF

La infraestructura informática a ser analizada es toda aquella que tenga una memoria (informática), por lo que se pueden considerar los siguientes dispositivos:

- Disco duro de una Computadora o Servidor
- Documentación referida del caso
- Logs de seguridad
- Información de Firewalls
- IP, redes
- Software de monitoreo y seguridad
- Credenciales de autentificación
- Trazo de paquetes de red
- Teléfono Móvil o Celular
- Agendas Electrónicas (PDA)
- Dispositivos de GPS
- Impresora
- Memoria USB

2.2 USOS Y PRIORIDADES

Existen varios usos de la informática forense (López et al., 2001), muchos proviene de la vida diaria, cuando se hace mal uso de un bien informático y se necesita aclarar algún delito, entre éstos se encuentran:

1. **Prosecución Criminal**: La evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
2. **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. **Investigación de Seguros:** La evidencia encontrada en computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. **Temas corporativos**: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
5. **Mantenimiento de la ley**: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tenga la orden judicial para hacer la búsqueda exhaustiva.

La prioridad del CF es preservar lo más íntegramente posible las evidencias del crimen, esto significa resguardar y proteger el hardware y las redes a las cuales se conecta es decir colocar el sistema fuera de servicio (offline). Si el sistema, por parte del administrador o empresa, requiere que siga funcionando, la investigación forense no podrá seguir el rumbo correcto porque se podría seguir haciendo mal uso del hardware o la red y lo cual ocasionaría cualquier posibilidad de persecución del intruso que está haciendo mal uso de los sistemas de información.

La “escena del crimen” cambiaría si se sigue utilizando, no se podría calcular el daño de la alteración. Por lo tanto es mejor sufrir un *"downtime"* de red, mientras que se realiza el análisis forense del sistema (Xombra, 2012).

Se tiene que establecer prioridad entre el funcionamiento inmediato y la investigación forense detallada porque de estas medidas depende que la investigación siga su curso adecuadamente y se tome en cuenta que la evidencia debe quedar fuera de servicio (offline) para que no sufra más alteraciones por parte de intrusos.

(a) **Funcionamiento inmediato**: Teniendo presente que las huellas dejadas por el/los intruso(s) pueden haberse eliminado por descuido del administrador y su equipo, y que el servidor puede seguir teniendo puertas traseras bien ocultas. Esta opción permite estar operativo en poco tiempo.
(b) **Investigación forense detallada**: Esta opción supone un mayor tiempo de permanencia offline si no existen planes de contingencia y procedimientos para el backup (copia de seguridad) del servidor (Xombra, 2012).

2.3 ETAPAS

El cómputo forense lleva a cabo una serie de etapas para recabar la o las evidencias que permitan esclarecer algún hecho, son identificación, preservación, análisis y presentación se detallan de la siguiente manera (Cano, 2009):

A) Identificación

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

B) Preservación

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia electrónica para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, se refiere al proceso que se requiere para generar una copia “bit-a-bit” de todo el disco, el cual permite recuperar en el siguiente paso, toda la

información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

C) Análisis

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, entre otros.

D) Presentación

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de un peritaje y de su correcta interpretación sin hacer uso de tecnicismos.

2.4 HERRAMIENTAS

El Dr. Jeimy Cano (2006), menciona que las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los intrusos y saber a ciencia cierta qué hicieron en el sistema, se han desarrollado al paso del tiempo para que ayuden en cuestiones de velocidad y faciliten identificar lo que realmente le pasó al sistema y qué es lo que le puede suceder; por otro lado, se han desarrollado herramientas bastantes sofisticadas en contra de los análisis forenses (herramientas y técnicas que intentan no dejar rastros, camuflarlos o borrarlos, de tal manera que se dificulte una posterior investigación).

El personal que labora en la informática forense debe poseer sólidos conocimientos técnicos y prácticos y conocer las herramientas de uso, estar al día en bugs (vulnerabilidades) de sistemas (sistemas operativos, software y hardware).

2.4.1 Clasificación de las herramientas de la Informática Forense

Actualmente existen cientos de herramientas las cuales se pueden clasificar de la siguiente manera (Nits, 2012):

A) Herramientas para la Recolección de Evidencia

Existen una gran cantidad de herramientas para recuperar evidencia (ver Tabla 1.a y 1.b). El uso de herramientas sofisticadas se hace necesario debido a (López et al., 2001).

1. La gran cantidad de datos que pueden estar almacenados en una computadora.
2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de computadoras.
6. Mecanismos de encripción o de contraseñas.

Tabla 1.a: Herramientas de recolección de evidencia

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
AccessData Forensic ToolKit (FTK)	Procesa datos de archivos de correo electrónico, analizar el registro, llevar a cabo una investigación, descifrar archivos, descifrar contraseñas. y elaborar un informe de todos con una sola solución	Server 2008 R2 / Windows7 (64-bit)	$12,500 M/N	http://www.accessdata.com/products/digital-forensics/ftk
OSForensic	Conjunto de utilidades para informática forense, esto es, para investigadores y todas aquellas personas que deseen comprobar qué se ha hecho con un ordenador.	Windows XP	Gratuito	http://osforensics.softonic.com/

Tabla 1.b: Herramientas de recolección de evidencia (continuación)

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
Sleuth Kit (Forensics Kit)	Permite analizar volúmenes de datos y sistemas de archivos	FreeBSD,Linux OpenBS Mac OS X, SunOS y Windowsv	Gratuito	http://ahornero.wordpress.com/2009/05/25/analisis-forense-digital-the-sleuth-kit/
Hetman software (Recuperador de datos borrados por los criminales)	Recupera datos de discos duros, externos y USB, todo tipo de tarjetas de memoria como SD, SDHC, Usb.	Windows 95 / 98 / Me / NT / 2000 / XP / 2003 / Vista	Gratuito	http://hetmanrecovery.com/file_uneraser/hetman_uneraser.htm

B) Herramientas para el Monitoreo y/o Control de Computadoras

Algunas veces se necesita información sobre el uso de las computadoras, por lo tanto existen herramientas que monitorean el uso para poder recolectar información. Existen algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente (López et al., 2001).

Dentro de este contexto están las presentadas en la tabla 2 (ACISSI, 2011):

Tabla 2: Herramientas de monitoreo

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
KeyLogger	Se oculta con una combinación de teclas y registra todo lo que se escribe con el teclado**.**	Windows XP	Gratuito	http://keylogger-gratis.softonic.com/
dcfldd (DD Imaging Tool command line tool and also works with AIR)	Aplicación de código abierto que proporciona una interfaz gráfica para el comando dd	Unix/Linux	Gratuito	http://www.howtoforge.com/creating_dd_images_with_air
Foremost (Data Carver command line tool)	Consola para recuperar archivos basándose en sus cabeceras, pies de página y las estructuras de datos interna	Linux	Gratuita	http://www.unixmen.com/recover-deleted-files-with-foremost/
netcat (Command Line)	Permite abrir fácilmente conexiones de red TCP o UDP tanto para la creación de clientes/servidores y poner a prueba aplicaciones de diseño propio.	Linux	Gratuito	http://netcat.softonic.com/linux
cryptcat (Command Line)	Es un software de código abierto que le permitirá realizar Intercambio de Archivos.	Windows (95/98/NT/2000/XP)	Gratuito	http://www.software112.com/products/cryptcat-encrypting-netcat.html

C) Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero debido a que no existe nada como un sitio 100% seguro, se debe estar preparada para incidentes, como ejemplos la tabla 3.a y 3.b:

Tabla 3.a: Herramientas de marcado de documento

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
R-Studio Agent	Para equipos donde los archivos se v an recuperar a través de la red. Soporta protocolo TCP/IP, y compatible con Microsoft Network	WinNT/2000/XP/2003/ Vista/2008/Windows 7	Adquirida en la compra de R-Studio	http://www.data-recovery-software.net/
R-Studio Emergency (Bootable Recovery media Maker)	Se ejecuta desde un arranque de CD / DVD, USB o cualquier otro dispositivo de medios extraíble o disco flexible	PowerPC Macintosh, Linux y UNIX/ Windows	Adquirida en la compra de R-Studio	http://www.data-recovery-software.net/
R-Studio NTFS	Recuperar datos de discos NTFS locales en las computadoras modernas, donde las particiones NTFS son muy comunes. Apoyo ExtFS se ha añadido como una cortesía para los amantes de Linux.	Windows 2000/2003/XP/Vista/2008/Win7) y **Ext2/Ext3/Ext4 FS** (Linux).	49.00 US	http://www.data-recovery-software.net/
R-Studio	Se ejecuta desde un dispositivo extraíble, cuando es necesario recuperar documentos en una PC, cuando el SO no puede iniciarse porque sus archivos están dañados o eliminados	Windows 2000/2003/XP/Vista/2008/Win7, (Macintosh), (FreeBSD/OpenBSD/NetBSD/Solaris) (Linux)	79.99 US	http://www.data-recovery-software.net/
E-Detective - DecisionComputer Group (Para análisis de redes)	Descifrar, reensamblar y reconstruir varias aplicaciones de Internet y servicios como el correo electrónico (POP3, IMAP y SMTP).	Windows	Gratuito	http://www.software112.com/products/edetective.html

Tabla 3.b: Herramientas de marcado de documento (continuación)

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
Paraben (Para análisis de correo electrónico)	Recupera correo electrónico eliminado	Windows	Gratuito	http://www.freedownloadmanager.org/es/downloads/El_Examinador_de_Correo_electr%C3%B3nico_de_Red_de_Paraben_36680_p/
Forensic and Log Analysis GUI	Software de código abierto que le permitirá realizar Motores / Servidores de bases de datos	Linux/BSD/UNIX-like OSes	Gratuito	http://www.software112.com/products/forensic-and-log-analysis-gui.html
md5deep (MD5 Hashing Program)	Operación recursiva, puede aceptar una lista de hashes conocidos y compararlos con un conjunto de archivos de entrada	Mac OS X	Gratuito	http://mac.softpedia.com/get/Utilities/md5deep.shtml
NTFS-Tools	Recupera datos NTFS, debido a ataques de virus, formato accidental de disco, errores de partición y cualquier otro tipo de pérdida de datos que ocurra	Windows, Linux	49 US	http://www.freedownloadmanager.org/es/downloads/search.php?string=NTFS-Tools&search=All&match=Any&search_btn=Buscar+%3E%3E%3E
R-Studio Network Edtion	Recuperación de datos a través de la red.	Windows 7	$124.99 US	http://www.data-recovery-software.net/

D) Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS “Portable Evidence Recovery Unit”.

Como ejemplo se encuentran las presentadas en la tabla 4:

Tabla 4: Herramientas de Hardware

HERRAMIENTA	DESCRIPCIÓN	PLATAFORMA	COSTO	SITIO WEB
USBDeview (Para análisis de USB)	Permite saber que dispositivos USB perconectan con una PC, estén conectados o no. Da tipo de dispositivo, número de serie y fecha.	Windows	Gratuito	http://usbdeview.softonic.com
qtparted (GUI Partitioning Tool)	Lee la mayoría de sistemas de ficheros,crea, copia y corta particiones.	Linux	Gratuito	http://qtparted.softonic.com/linux
X-Ways Trace	Realiza un seguimiento y analizar la actividad de navegación por internet y supresión de ficheros a través de la paelera de reciclaje.	Win 95/Me/NT/2000/XP	$ 49.90 Euros	http://www.winhex.com/index-e.html
X-Ways WinHex	Inspecciona, editatodo tipo de archivo de navegación por internet ,archivos borrados , visitados,desde tarjetas de cámaras digitales.	Win 95/Me/ NT/2000/XP	Profesional: 69.90 Euros Specialist: 199.99 Euros.	http://www.ways.net/corporate/conect.html

Hay más herramientas forenses utilizadas por el cómputo forense las cuales se mencionan en la Tabla 5.

Tabla 5: Herramientas forenses

HERRAMIENTA	DESCRIPCIÓN	SITIO WEB
F.I.R.E	Destaca dentro de las distribuciones Linux específicas para informática forense.	http://biatchux.dmzs.com
WinHex	Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM.	http://www.x-ways.net
Encase	Herramienta propietaria, la cual ha demostrado ser un dispositivo útil a los peritos forenses en diferentes casos	http://www.guidancesoftware.com/
Snort	Herramienta libre por excelencia una de las mejores	http://www.snort.org
Ossim	Herramienta de monitorización	http://www.guidancesoftware.com
Ettercap	Excelente sniffer de redes	http://ettercap.sourceforge.net/
NMap	Potente localizador de vulnerabilidades	http://www.insecure.org/nmap/
Nessus	Otro proyecto para scanear vulnerabilidades	http://www.nessus.org
Ethereal	Otro potente sniffer	http://www.ethereal.com
Fport	Identifica puertos abiertos y aplicaciones asociadas a ellos	http://foundstone.com/
Putty	Excelente cliente SSH	http://www.chiark.greenend.org.uk/~sgtatham/putty/
Stunnel	Programa que cifra las conexiones TCP bajo SSL	http://www.stunnel.org/
AirSnort	Herramienta wireless para recuperar claves cifradas	http://airsnort.shmoo.com/
Aircrack	sniffer y WEP craqueador de wirless	http://www.cr0.net:8040/code/network/
Achilles	Herramienta para testear la seguridad de las aplicaciones web	http://www.mavensecurity.com/achilles
NetStumbler	Localizador de los puntos de acceso wireless	http://www.stumbler.net/
Dsniff	Sniffer	http://www.datanerds.net/mike/dsniff.html
VNC	Administrador remoto	http://www.realvnc.com/
The Autopsy	Browser para la informática forense	http://www.sleuthkit.org
PyFlag	Herramienta para recuperar discos en RAID	http://pyflag.sourceforge.net/
Promqry 1.0	Línea de comandos, 113 KB	http://download.microsoft.com/download/b/b/6/bb6ea193-2880-43c3-b84b-b487a6454a17/promqrycmd.exe
PromqryUI 1.0	Interfaz gráfico, 255 KB	http://download.microsoft.com/download/7/2/6/7262f637-81db-4d18-ab90-97984699d3bf/promqryui.exe

2.4.2 Herramienta EnCase

Como caso específico se hace referencia a la herramienta *EnCase* porque es la más utilizada por un informático forense durante un análisis forense. El análisis con esta herramienta permite analizar cualquier dispositivo electrónico como disco duro, memoria de celular, memoria USB, es decir todo aquello que pueda almacenar información importante para detectar alguna anomalía y así encontrar una evidencia. (Ver figura 2.1)

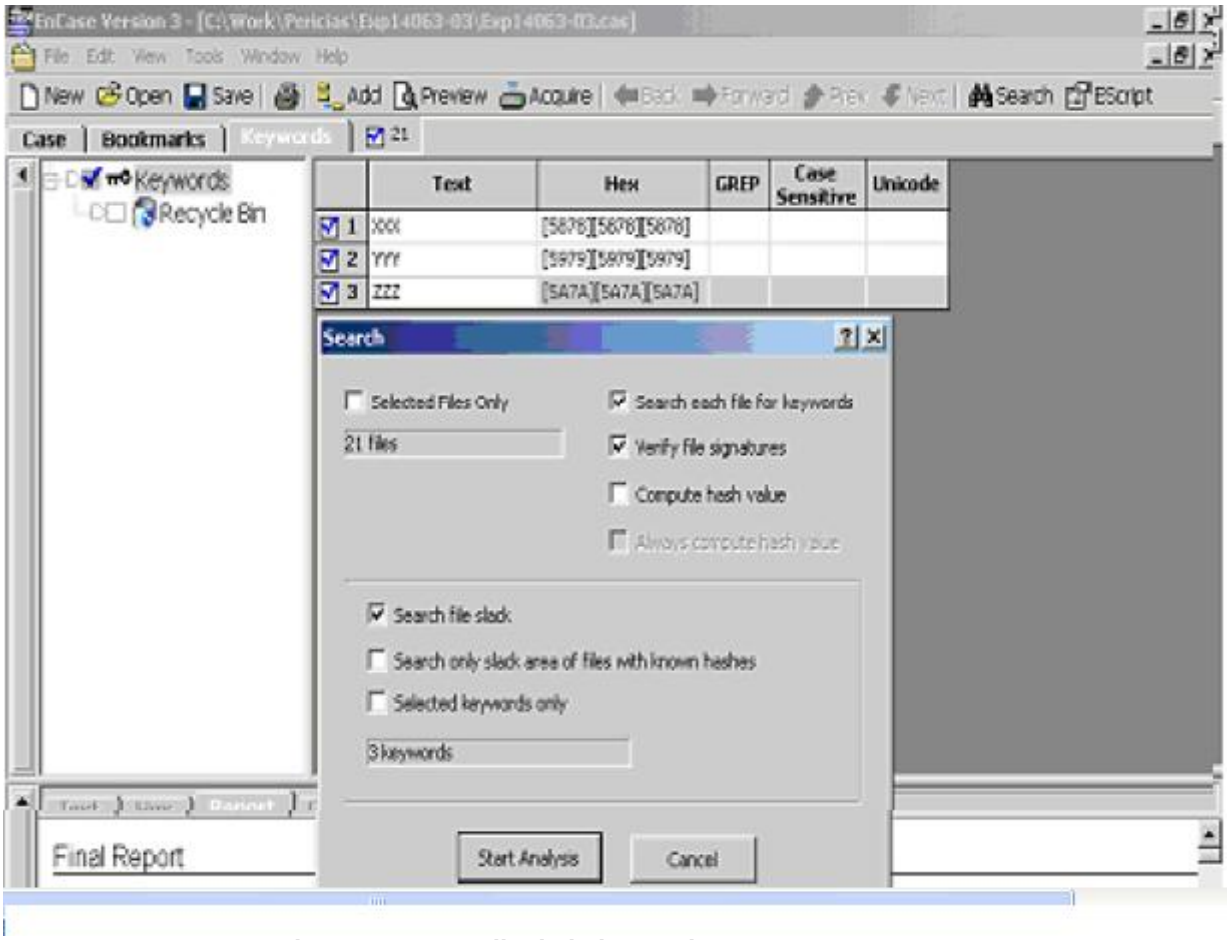

Figura 2.1: Pantalla de la herramienta EnCase

La herramienta EnCase es desarrollada por Guidance Software Inc., permite asistir al especialista forense durante el análisis de un crimen digital, es una herramienta de software líder en el mercado, es el producto más ampliamente

difundido y de mayor uso en el campo del análisis forense. Sus principales características son (Xombra, 2012):

- **Copiado comprimido de discos fuente:** EnCase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen, los archivos comprimidos resultantes pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra cantidades importantes de espacio en el disco de la computadora del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinando la evidencia y buscando otra evidencia.

- **Búsqueda y análisis de múltiples partes de archivos adquiridos:** Permite al examinador buscar y analizar múltiples partes de la evidencia, muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos "zip" y otros tipos de dispositivos de almacenamiento de la información con EnCase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si está comprimida o no y puede ser colocada en un disco duro y ser examinada por el especialista. En varios casos la evidencia puede ser ensamblada en un disco duro grande o un servidor de red.

- **Diferente capacidad de almacenamiento:** Los datos pueden ser colocados en diferentes unidades, como discos duros IDE o SCSI, drives ZIP y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.

- **Varios campos de ordenamiento:** EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuándo se

creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

- **Análisis compuesto del documento:** Permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el *slack* interno y los datos del espacio unallocated.

- **Búsqueda automática y análisis de archivos de tipo zip y attachments de e-mail. firmas de archivos, identificación y análisis:** La mayoría de las gráficas y de los archivos de texto comunes contienen una pequeña cantidad de *bytes* en el comienzo del sector los cuales constituyen una firma del archivo. EnCase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechoso haya escondido un archivo o simplemente lo haya renombrado, EnCase detecta automáticamente la identidad del archivo e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.

- **Análisis electrónico del rastro de intervención:** Son sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computadora. EnCase proporciona los únicos medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente con la característica de ordenamiento, el análisis del contenido de archivos y la interfaz de EnCase, virtualmente toda la información necesitada para un análisis de rastros se puede proporcionar en segundos.

- **Soporte de múltiples sistemas de archivo:** EnCase reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones),

Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Con EnCase un investigador va a ser capaz de ver, buscar y ordenar archivos desde estos discos concurridos con otros formatos en la misma investigación de una manera totalmente limpia y clara.

EnCase provee una interfaz tipo Explorador de Windows y una vista del Disco Duro de origen, también permite ver los archivos borrados y todos los datos en el espacio (*Unallocated)*. También muestra el *Slack File* con un color rojo después de terminar el espacio ocupado por el archivo dentro del *cluster*, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos *Swap* y *Print Spooler* son mostrados con sus estampillas de datos para ordenar y revisar.

- **Integración de Reportes*:*** EnCase genera el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del investigador, favoritos, imágenes recuperadas, criterios de búsqueda y tiempo en el que se realizaron las búsquedas.

- **Visualizador integrado de imágenes con galería*:*** EnCase ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como *.gif* y *.jpg* del disco. Seleccionando la "Vista de Galería" despliega muchos formatos de imágenes conocidas, incluyendo imágenes eliminadas, en el caso de una vista pequeña. El examinador puede después escoger las imágenes relevantes al caso e inmediatamente integrar todas las imágenes en el reporte de EnCase. No es necesario ver los archivos gráficos usando software de terceros, a menos que el formato de archivo no sea muy conocido y todavía no sea soportado por EnCase.

2.5 VENTAJAS Y DESVENTAJAS DEL CF

Actualmente la tecnología y la forma de vida han cambiado y con ello la forma en que todos operan. Ahora toda la información es almacenada en las computadoras de manera automática, a diferencia de épocas anteriores en donde la información se almacenaba de manera manual y en papel. Esto conlleva cierto tipo de ventajas y desventajas que la Informática forense enfrenta.

2.5.1 Ventajas

La informática forense como nueva disciplina tiene grandes ventajas que ayudan a esclarecer a algún hecho mal intencionado utilizando dispositivos electrónicos por ejemplo (Ramirez, 2012):

- Se ayuda de herramientas que permiten dar de manera precisa los datos encontrados en cualquier dispositivo electrónico capaz de almacenar información.
- Es fiable por la objetividad y exactitud debido a que la información encontrada mediante sus herramientas no permite alterar información alguna.
- Un especialista en CF ofrece información exacta, completa, clara, precisa, veraz, objetiva y neutra, puesto que proviene de un elemento electrónico en el que no cabe subjetividad alguna.
- Es posible obtener información de manera veraz y rápida, imposible de obtener mediante cualquier otro procedimiento informático.
- La evidencia electrónica permite el esclarecimiento de ciertos delitos en los que estas pruebas son el único medio probatorio existente.
- La evidencia electrónica encontrada puede ser conservada y almacenada de tal forma que no ocupa tanto espacio.

- Varios profesionales opinan que el uso de documentos y firmas electrónicas favorecen el desarrollo del comercio electrónico y con el procedimiento empleado por el CF permite encontrar cualquier evidencia en caso de algún fraude o infiltración a la red.

2.5.2 Desventajas

- La mayor desventaja que enfrenta el CF es que como es una disciplina reciente y nueva no es conocida y sobretodo no está amparada por leyes que respalden la veracidad de las mismas pruebas encontradas durante un procedimiento forense a menos de que ésta sea una orden girada por un juez.
- Son muy pocos países los que ya tienen una reforma en el uso de CF; en México, es necesaria una reforma que ampare la evidencia digital encontrada por un informático forense.
- La falta de conocimientos para verificar su autenticidad hace que sea considerada más vulnerable y, por lo tanto, menos fiable que una prueba tradicional, constituyendo un inconveniente para su uso y admisibilidad.
- Los profesionales del derecho no creen en este tipo de evidencia debido al desconocimiento existente sobre los procedimientos de un procesado de datos mediante el uso de la informática forense y de la interpretación posible que se dé en las leyes.
- La falta de una regulación propia y sistemática, así como por la falta de jurisprudencia, los profesionales de derecho muestran un temor a la vulnerabilidad y facilidad con que estas pruebas pueden ser manipuladas, dado su alto grado de volatilidad, lo que resulta uno de los principales inconvenientes a la hora de probar su autenticidad. Algunos opinan que se trata de pruebas muy técnicas que son desconocidas para jueces y fiscales y que resultan difíciles de explicar, de ahí el rechazo a admitirlas en juicio (Merida & Fredesvinda, 2008).
- La falta de conocimiento en el uso de herramientas que no dan pie a la vulnerabilidad de la información a ser borrada, la fácil replicación de la información, la explotación de la información por vulnerabilidades en el

sistema, por lo tanto se piensa que se corre riesgo al manejar información por lo tanto se debe tener una manera de protegerlos y proteger a las personas que cuentan con información.

2.6 FUTURO

La IF es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o fraudes en las organizaciones. En este sentido, se tienen agendas de investigación a corto y mediano plazo para que se avancen en temas de especial interés en la conformación y fortalecimiento de las ciencias forenses aplicadas a los medios informáticos (Cano, 2006).

La evidencia electrónica o digital en la administración de justicia en muchas partes del mundo continua siendo una situación problemática por resolver (Brungs & Jamieson, 2003). Dada las características mencionadas previamente, se hace un elemento que requiere un tratamiento especial, más allá de las características legales requeridas, ya que éstas deben estar articuladas con los esfuerzos de seguridad de la información vigentes en las organizaciones. Las herramientas utilizadas actualmente en investigaciones forenses en informática están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos.

Sin embargo, la fragilidad inherente del software, la vulnerabilidad presente en las mismas y las limitaciones propias de los lenguajes y práctica de programación hacen que la comunidad académica y científica redoble sus esfuerzos para hacer de estos programas, herramientas más confiables y predecibles para los cuerpos de investigaciones judiciales y organizacionales (Cano, 2006).

Se necesita la formación de especialistas en informática forense, para realizar peritaje informático en el nivel de gobierno judicial, al ser el CF una ciencia aplicada naciente, se hace necesario iniciar la formación de un especialista en informática forense (Cano, 2009; White, Rea, Mckenzie, & Glorfled, 2004), esta formación necesariamente deberá ser interdisciplinaria y para ello se requiere el concurso de los profesionales del derecho, la criminalística, las tecnologías de información y la seguridad informática, como mínimo, sin perjuicio de que otras disciplinas académicas puedan estar presentes en la estrategia de profesionalización de estos nuevos especialistas.

Los diferentes escenarios y elementos que componen esta naciente disciplina auxiliar de la criminalística aclara que los conceptos expresados responden a una revisión de la práctica internacional sobre el tema y que el análisis forense para el caso en México requiere un estudio particular, debido a la falta de conocimiento de la IF y sobre todo de la regulación de la ley para que la evidencia electrónica sea válida como prueba en algún hecho que necesite ser aclarado.

La informática forense es la respuesta natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos) con el fin de enviar un mensaje claro a los intrusos, se necesita preparar y conocer el procedimiento del CF para responder a sus acciones con veracidad.

Un área interesante es la telefonía celular ya que en la actualidad almacena información verídica de todas las actividades que realiza una persona en los teléfonos celulares, entonces, los celulares están como una evidencia fuerte ya que se registran las últimas actividades de la persona que porta el celular, por lo tanto ayuda a esclarecer algún hecho o aportar algún dato importante que dé motivo a que las autoridades comiencen a investigar; un dato importante, es que no importa que se haya borrado la información del chip o de la memoria externa, porque la herramientas forenses permiten extraer todos los datos de la memoria del celular aún cuando hayan sido borrados, o que el chip haya sido

destruido, se utiliza un dispositivo llamado UFED (*Universal Forensics Extraction Device*, ”Dispositivo universal de extracción de datos forenses”), que está destinado a ser un dispositivo autónomo de acción inmediata de lucha contra narcotráfico, terrorismo y para medidas militares con independencia de la computadora, no necesariamente se necesita una computadora, lo que realiza este dispositivo de manera básica es (YanapTI, 2009a):

- Se conecta de un extremo mediante un cable el teléfono, se selecciona la marca de teléfono y se realiza la extracción completa de la información contenida dentro del teléfono, junto con la memoria externa y esta información recabada es presentada como evidencia electrónica en una corte judicial para esclarecer algún hecho. (Ver figura 2.2)

Figura 2.2 Dispositivo UFED

- Si el teléfono celular no tiene batería se cuenta con conectores especiales para cargar la batería (Ver figura 2.3). Lo importante es la clonación de tarjetas (Ver figura 2.4) con tecnología GSM, se toma el chip del usuario y se clona con la finalidad preservar los datos que existen en los teléfonos llamadas entrantes, salientes, fotografías, videos. Se crea la copia del chip en un nuevo chip es decir contiene los

datos iguales no se altera ningún dato ya que es una herramienta específica que se utiliza en el análisis forense para telefonía celular.

Figura 2.3 Maletín de telefonía celular de la informática forense

- En dado caso que el chip no lo tenga o lo hayan quitado se interviene mediante el operador y mediante los lineamientos legales que regulen y se recuperar los datos de identificación del chip y se mete manualmente al equipo y se recupera totalmente la información.

Figura 2.4 Clonación de tarjetas

La investigación de los próximos años hará que las computadoras y los celulares arrojen información sin necesidad de que tenga que ver con la computadora, un caso de fraude, secuestro o asesinato, la información del

celular, mostrará de manera eventual las últimas actividades o llamadas de la persona y así tener más elementos de investigación.

CAPÍTULO 3

EVIDENCIA DEL CÓMPUTO FORENSE

Capítulo 3 EVIDENCIA DEL CÓMPUTO FORENSE

Las huellas permiten reconstruir la ejecución de un hecho (el cual no tiene que ser necesariamente consecutivo de un delito) se encuentran almacenadas en apoyos digitales y se llaman genéricamente evidencias digitales o evidencias electrónicas (Hikal, 2009). La evidencia digital se puede modificar o eliminar fácilmente por la persona que está violando la información, sin embargo esto no es cierto, la IF permite reconstruir todos los archivos alterados o eliminados, se hace una copia exacta de la evidencia recabada y con el análisis forense se encuentra elementos suficientes para esclarecer un hecho.

3.1 BASES

Los investigadores del CF usan gran cantidad de técnicas para recabar evidencias y encontrar al intruso, incluyendo herramientas de software que automatizan y aceleran el análisis computacional, las bases que se deben tomar en cuenta durante un análisis forense son (Xombra, 2012):

- Experiencias, auditoría e inspecciones en computadores y páginas web
- Ubicación de origen de correos anónimos y archivos anexos.
- Determinación de propietarios de dominios como: .com, .net, .org y otros.
- Pruebas de violación de derechos de autor.
- Control preventivo y restricción de uso de computadores e Internet.
- Protección de información y derechos de autor.
- Recuperación de datos y archivos borrados intencionalmente o por virus.
- Recuperación y descifrado de las claves.

Para realizar un análisis forense es necesario tomar notas de lo que se hace con el disco duro y a qué hora, almacenándolas y guardándolas en una ubicación segura como por ejemplo una caja fuerte; se recomienda que siempre que se trabaje con la evidencia electrónica se esté acompañado por un colega para que conste a los efectos legales y el testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

Las copias deben ser hechas bit-por-bit, es decir es necesario hacer imágenes del disco, la investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se deben hacer tres copias del disco duro original, sobre todas las copias y el original debe llevar a cabo una verificación criptográfica un: checksum. En lo posible realizar dumps[1] de memoria y almacenarlos al igual que los discos.

Es importante que todos hechos que conciernen al caso durante la preparación, recuperación y análisis de la evidencia electrónica de un ataque sean anotados para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis, este documento deberá servir como una prueba del incidente o compromiso. Antes de apagar el sistema, será útil recoger algunos ejemplos de aquella información que posiblemente no ha sido cambiada por los intrusos, como la organización de sistema de ficheros logs, el nombre del host, su dirección IP del fichero e información de algunos dispositivos.

El análisis de la comunicación de datos es realmente importante, ahí se trabajan en dos actividades (Xombra, 2012):

- Intrusión en una red de computadoras o mal uso de la misma.
- Interceptación de datos.

La intrusión en una red de computadoras o mal uso de la misma es la actividad principal de la IF cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las siguientes funciones (Xombra, 2012):

a) Detección de la intrusión.
b) Detectar la evidencia, capturarla y preservarla; y
c) Reconstrucción de la actividad específica o del hecho en sí.

[1] Dump: Es la acción que se realiza para generar un archivo en el que se han grabado todos los datos en la memoria.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal, este comportamiento incluye el acceso no autorizado, modificación del sistema en forma remota y el monitoreo no autorizado de paquetes de datos. La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis. La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia, para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros y/o técnicos de software.

Antes de realizar un análisis forense se debe tener en cuenta la siguiente información**:**

a) Sistema operativo afectado.
b) Inventario de software instalado en el equipo
c) Tipo de hardware del equipo
d) Accesorios y/o periféricos conectados al equipo
e) Si posee firewall
f) Si está en el ámbito del DMZ (Zona desmilitarizada)
g) Conexión a internet
h) Configuración
i) Parches y/o actualizaciones de software
j) Políticas de seguridad implementadas
k) Forma de almacenamiento de la información (cifrada o no)
l) Personas con permisos de acceso al equipo
m) La PC está dentro del DMZ (Zona Desmilitarizada)
n) Existe IDS (Sistema de Detección de Intrusos)
o) Cuántos equipos en red

3.2 EVIDENCIA DEL CF

La evidencia electrónica es única, cuando se compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia electrónica es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia electrónica es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario (Casey 2002).

Debe tomarse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales de porque ya que esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, utilizan varias herramientas por ejemplo *checksums* o *hash* MD5 (Intelcard Systems, 2012).

La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia electrónica (Cassou, 2009):

- Sobre recolectar evidencia electrónica, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
- Cuando es necesario que una persona tenga acceso a evidencia electrónica original, esa persona debe ser un informático forense.
- Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia electrónica, debe ser documentada completamente, preservada y disponible para la revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia electrónica mientras que ésta esté en su posesión.

- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia electrónica es responsable de cumplir con estos principios.

Los principios desarrollados para la recuperación de la evidencia electrónica tienen los siguientes atributos:

- Consistencia con todos los sistemas legales.
- Permitir el uso de un leguaje común.
- Durabilidad.
- Capacidad de cruzar límites internacionales.
- Capacidad de ofrecer confianza en la integridad de la evidencia.
- Aplicabilidad a toda la evidencia forense.

3.3 GUÍAS QUE DEBEN DE EMPLEAR DURANTE LA RECOLECCIÓN DE UNA EVIDENCIA EN EL ANÁLISIS FORENSE

El procedimiento para la recolección de evidencia varia de país a país, sin embargo, existen unas guías básicas que pueden ayudar a cualquier informático forense, que le permite realizar un recolección de evidencia electrónica exitosa (Intelcard Systems, 2012).

3.3.1 Lineamientos Generales para la Recolección de Evidencias

El aspecto más importante a la hora de recolectar evidencia, es la preservación de la integridad de la información, ejemplo la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil. La primera gran decisión que se debe tomar a la hora de recabar evidencias electrónicas, un investigador podría estar tentado a llevarse todo el equipo que encuentre, para no arriesgarse a dejar piezas de información potencialmente importantes, sin embargo, esta alternativa tiene sus inconvenientes, ya que el investigador podría terminar siendo demandado por dañar o alterar la vida de una persona o de un negocio más de lo absolutamente necesario, lo indicado sería llevarse sólo lo mínimo necesario para efectuar una investigación.

Lo primero que se debe preguntar el informático forense es qué partes se deben buscar o investigar, el hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia electrónica, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen, ejemplo el contrabando y el robo, es por esto que es lo primero que debe ser recolectado. Generalmente, es necesario recolectar computadoras y, de ser necesario, elementos de almacenamiento (CDs, cintas magnéticas, *diskettes*, etc.) que puedan contener evidencia electrónica.

En este punto se debe tomar otra decisión crítica: ¿los equipos involucrados en una investigar? deben ser apagados o deben permanecer prendidos? respondiendo a esta interrogante muchas agencias de cumplimiento de la ley recomiendan apagar los equipos en todas las situaciones, y los expertos en IF insisten en que es la mejor alternativa debido a la posibilidad de que la evidencia sea destruida mientras la computadora permanece encendida. Aún así, hay casos en que apagar un equipo puede causar más daños que beneficios, por ejemplo, si se trata de un servidor que presta servicios a muchas personas que no necesariamente están involucradas en una investigación, la mejor opción para el investigador es utilizar su buen juicio y sentido común para determinar las acciones a seguir.

Cuando se recolecta todo el contenido de una computadora, en general los pasos a seguir son los mismos:

- Toda la evidencia importante debe ser leída de la memoria RAM.
- La computadora debe ser apagada
- La computadora debe ser reiniciada usando otro sistema operativo que desvíe el existente y no cambie el contenido de el (los) disco(s) duro(s).
- Debería sacarse una copia de la evidencia electrónica encontrada en el (los) disco(s) duro(s).

Debe tenerse en cuenta que cuando se habla de hacer una “copia” de un disco duro, ésta debería ser una copia bit-a-bit de todo el contenido de éste;

muchísima información está “escondida” en sitios no-convencionales de un disco.

Hay otra gran categoría de evidencia electrónica que puede ser recolectada en el caso de los crímenes informáticos, y es la evidencia presente en las redes. Todo el flujo de información que corre a través de una red, sea interna o externa de una organización, o aún en Internet, podría contener evidencia potencialmente útil a la hora de investigar un crimen, por ejemplo, usurpación de correos electrónicos, intercambio de información ilegal a través de Usenet (por ejemplo la pornografía infantil) o uso del IRC (Red de comunicación en tiempo real) para concertar crímenes, práctica común entre la comunidad hacker, que no podrían cometerse sin la utilización de redes.

La diferencia entre la evidencia electrónica y la evidencia en las redes es que la evidencia electrónica es almacenada en una computadora y la otra es que la información corre a través de la red. Un informático forense debe hacer esfuerzos para poder demostrar que la evidencia en Internet es auténtica y no ha sido modificada mientras estaba siendo transmitida o recolectada.

3.3.2 Análisis de Evidencias

Existen varias formas de buscar la evidencia en cualquier dispositivo electrónico, muchos criminales no tienen la más mínima idea de cómo funcionan las computadoras, y por lo tanto no hacen un mayor esfuerzo para despistar a los investigadores, excepto por borrar archivos, que pueden ser recuperados fácilmente. Cuando los usuarios de DOS o Windows borran un archivo, los datos no son borrados en realidad, a menos que se utilice software especial para borrar.

Una vez que se cuenta con todas las posibles evidencias recabadas para un procedimiento de análisis forense, con ayuda de las herramientas de la IF se empieza la reconstrucción de información destruida, la recuperación de información oculta con el objetivo de preservar la integridad de la información

que se está analizando, preferiblemente trabajando sobre una copia realizada de la evidencia original, y no trabajar sobre la evidencia original para evitar alteraciones que podrían invalidar la evidencia como una prueba aceptable ante la ley.

La clave de la IF es el procedimiento de análisis de discos duros, disco extraíbles, CDs, discos SCSI, y otros medios de almacenamiento, el análisis no sólo busca archivos potencialmente incriminatorios, sino también otra información valiosa como *passwords*, *logins* y rastros de actividad en Internet (López et al., 2001).

3.3.3 Cuidados en la Recolección de Evidencia

La recolección de evidencia es un aspecto frágil del Cómputo Forense, especialmente porque requiere de prácticas y cuidados adicionales como (Intelcard Systems, 2012):

- Se debe proteger los equipos del daño.
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información.
- En algunas ocasiones será imposible reconstruir la evidencia, si no se tiene cuidado de recolectar todas las piezas que se necesiten.

CAPITULO 4

NORMATIVIDAD DEL CÓMPUTO FORENSE

Capítulo 4 NORMATIVIDAD DEL CÓMPUTO FORENSE

El uso de evidencias electrónicas se ha convertido en un elemento necesario para tratar de esclarecer delitos cometidos a través de dispositivos electrónicos, es por esto que es importante saber cómo está regulada la evidencia electrónica respecto a la prueba tradicional, a los medios de prueba, al documento electrónico y a la firma electrónica.

El CF necesita ser regulado para que sea válido como prueba en contra de una persona que ha cometido algún delito, se muestra a lo largo del capítulo las leyes que hay actualmente y qué reformas necesitan hacerse para que la IF tenga mayor credibilidad, y que los profesionales de derecho se enriquezcan de este nuevo conocimiento y de la ventaja que se tienen al emplear un análisis forense para esclarecer un hecho.

4.1 HISTORIA DE LOS DELITOS INFORMÁTICOS

La concepción de los delitos informáticos en México tendrá escasos diez años; sin embargo, en los Estados Unidos de Norteamérica, la primera propuesta de legislar con este respecto, se presentó en 1977 por el senador Ribicoff en el Congreso Federal.

Años después, en 1983 en París, la OECD (Organización para la Cooperación y Desarrollo Económico) designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros, la modificación de su legislación penal de forma que se integraran los nuevos delitos informáticos.

En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la recomendación emitida el 13 de septiembre de ese año, presentaron una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional. También se llegó a discutir sobre estos temas en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal

de las Naciones Unidas celebrado en el mismo año, y en la Conferencia de Wurzburgo, en Alemania, en 1992. En 1996, se estableció por el Comité Europeo para los problemas de la delincuencia, un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.

Con el fin de combatir los delitos informáticos, sobre todo los cometidos a través de las redes de telecomunicaciones en Internet, como pueden ser las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violan la dignidad humana y la protección de los menores, se elaboró un borrador del instrumento legal obligatorio al recién formado "Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras".

Por tanto el borrador que elaboró el comité sirve para combatir los delitos que se cometen en computadoras a través de la redes y permite proteger a las personas que han sido objeto de un delito informático.

El 23 de noviembre de 2001, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, la convención sobre delitos informáticos, cuyos objetivos fundamentales fueron los siguientes (Muñoz, 2002):

- Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.
- Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas, y
- Establecer un régimen dinámico y efectivo de cooperación internacional.

En México el sistema jurídico incluyó a los delitos informáticos justamente con las reformas que se publicaron en el Diario Oficial de la Federación el 17 de mayo de 1999.

Los novedosos ilícitos se ubicaron dentro de Título Noveno del código punitivo federal, al que se denominó "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática" (Muñoz, 2002):

Resulta de interés la exposición de crear una reforma en los procedimientos informáticos, al considerarse que la iniciativa propone adicionar un capítulo al código penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contenga, por lo que se pretende cuidar la privacidad y la integridad de la información.

Para un legislador fue de suma importancia proteger el acceso no autorizado a computadoras y las redes a las que está conectada, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos, ilícitos que no son privativos de nuestro entorno, sino que suceden con frecuencia en el ámbito internacional y que constituyen, desde luego, un grave problema ante la revolución tecnológica que ha rebasado las estructuras de contención, control y vigilancia por parte de los Estados.

El diverso delito de revelación de secretos que establece el artículo 211 del enunciado Código Penal Federal, prevé sanción de uno a cinco años, cuando:

"La revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público, o cuando el secreto revelado o publicado sea de carácter industrial, el subsecuente numerario de dicho ordenamiento legal, dispone que a quién revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión".

Tales ilícitos también pueden considerarse como un fin en tratándose del uso de computadoras, sobre todo cuando se trata de información de tipo industrial, en relación con el, de la ley del enjuiciamiento penal federal, la Primera Sala

del más alto Tribunal de Justicia de la Nación, ha establecido de que el vocablo "indebidamente" empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, el segundo, porque su sentido puede fijarse desde el punto de vista jurídico y determinar cuando la conducta es indebida para considerarse delictuosa. Además, el hecho de que el Código Penal Federal no contenga un anunciado especial que desentrañe el significado de ese elemento normativo, lo cual se entiende por constituir un elemento de valoración jurídica, no implica infracción a la citada garantía, debido a que se trata de un concepto cuyo contenido resulta claro tanto en el lenguaje común como en el jurídico.

En México existen leyes para delitos informáticos, pero no hay una ley o reforma que hable de la validez de la evidencia que emerge de un procedimiento forense realizado por la informática forense, ésta es una problemática que necesita ser regulada y tenga validez en caso de que se viole el uso de un dispositivo electrónico o un mal uso en una red.

4.2 DELITOS INFORMÁTICOS Y ÉTICA DEL CÓMPUTO FORENSE

4.2.1 Delitos Informáticos

La red se integra por diferentes actores (usuarios, proveedores de acceso, proveedores de hosting y de housting), el usuario es la persona física o jurídica que mantiene la página, el titular y el encargado de la página, el proveedor de acceso a Internet es la empresa que se dedica a conectar a los usuarios individuales a la red a cambio de un precio, generalmente mensual y el proveedor de alojamiento o *housing* es aquella empresa que destina parte de su sistema o de su espacio virtual para alojar la página de una persona.

El proveedor de acceso en la mayoría de los casos es local al lugar del usuario, pero quien brinda el housing y/o el hosting puede estar en cualquier lugar del mundo, en el caso, el proveedor de alojamiento, es decir el lugar en donde se aloja la página, puede ser a modo de ejemplo el conocido portal yahoo.com cuyos servidores se encuentran en los EE.UU. y su página principal se indica

como www.yahoo.com, la funcionalidad de cada uno de los actores en la red, se complica demasiado, debe aplicarse el derecho.

Por lo tanto un usuario que acceda al servicio del Internet en los Estados Unidos de Norte América, puede estar llevando a cabo conductas delictivas que se ejecuten materialmente en un diverso país, esa situación dificulta, desde luego la aplicación del derecho penal, porque por principio y a fin de cumplir con el marco normativo básico, se debe establecer la existencia del delito, posteriormente tiene que identificarse al sujeto activo, aspecto que tratándose de ilícitos que se llevan a cabo a través del Internet no se facilita, dado el incipiente impulso que se ha dado a la materia de informática forense (Batiz, 2004).

Aún ubicando la identidad del trasgresor de la ley penal es necesario su enjuiciamiento con las formalidades esenciales del procedimiento, lo que se torna más difícil ya que se destacó la conducta lesiva que se realizo en diverso país, es por ello que la necesidad que impone la Constitución en nuestro país de seguir con un debido proceso legal, en el que se cumplan con las formalidades esenciales del procedimiento, se dificulta en relación con los delitos informáticos, desde luego, existen algunos avances en cuanto a la configuración de dichos delitos en la ley penal, así como a mecanismos para lograr con técnicas forenses en materia de informática la ubicación del lugar en que se llevó a cabo la conducta delictuosa; sin embargo, el problema se complica para lograr la identificación del sujeto activo en un delito que difícilmente deja huellas y rastros a seguir.

En este sentido, se han distinguido dos figuras delictivas a las que se les ha denominado (Campoli, 2006) el ***phishing*** **(**estafa cibernética**)** así como el ***trapping*** **(**la manera en que se disfraza la estafa**)**, las que conducen a la utilización, obtención, transferencia o disposición indebida de fondos de los clientes de las instituciones de crédito, como su resultado real y tangible, incluso puede darse el caso en que intervengan también funcionarios o empleados de las instituciones bancarias.

Citibank México (Consejo de la Judicatura Federal, 2008) desarrolló una unidad de cómputo forense, cuyos objetivos se centran en dos aspectos, el primero, realizar un análisis del equipo de cómputo sobre lo que ya pasó, en el que generalmente se trabaja sobre el disco duro del usuario, en este caso del cliente del banco que ha denunciado la sustracción de su capital al ser víctima de un ataque informático; y el segundo aspecto se enfoca a que en vivo se conecte a la computadora y se pueda analizar el programa o aplicación.

Por tanto en diversos ordenamientos se limitan a otorgarles valor probatorio a los documentos o instrumentos que se obtienen por medios electrónicos, por esto es necesaria la legislación en materia del CF.

4.2.2 Ética en el manejo del Internet

Al producirse la interacción mundial a través del Internet, es necesario para algunos establecer reglas básicas de comportamiento por parte del usuario, así como de los prestadores del servicio; por el contrario, existe quienes piensan que al ser el Internet un bien de la humanidad debe seguir un patrón de comportamiento libre en el que el recorrido por lo que se ha denominado la supercarretera de la información no se limite, y sólo esté sujeta a la habilidad de cada usuario para conducirse en ese mundo virtual.

Se necesita crear reglas para que sus intereses no choquen entre sí, ante un sistema de comunicación mundial, que comprende una gran disparidad de cultura, edad, educación, no tan sólo es congruente sino indispensable crear un manual del comportamiento del usuario, manual que no debe limitarse a un estudio nacional, sino a un plano internacional, con la distinción de que no debe encontrarse elevado a la categoría de una norma con todos sus atributos legales, pero que sí debe servir de patrón para una mejor interacción en el Internet, y para desmotivar en principio, conductas reprobables, así como conductas lesivas, ejemplo las personas pueden jugar en casinos virtuales sin ninguna regulación, a la fecha actual se puede decir que el único contenido de Internet prohibido y sancionado en nuestro país es el de la pornografía infantil.

Lo anterior da una idea de lo grave que resulta no tener reglas de comportamiento en el uso de las diferentes formas del Internet, sistemas informáticos y dispositivos informáticos por este motivo es necesario regular a el CF ya que éste provee herramientas de tecnología de punta que permiten detectar anomalías, en un sistema, fraudes, extorciones, delincuencia etc., así de alguna manera los usuarios y toda persona que hace uso indebido de la tecnología informática, mediría más lo que hace, para evitar algún procedimiento judicial, ya que la informática forense a través de la metodología que realiza, daría las pruebas electrónicas suficientemente precisas que avale el ilícito que se está cometiendo.

4.3 JURISDICCIÓN Y COMPETENCIA DEL CÓMPUTO FORENSE

El derecho informático, surge como una nueva rama del Derecho, como consecuencia de las siguientes consideraciones de que se requiere una regularización de los bienes informacionales, porque la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico; es necesaria la protección de datos personales. Debido al atentado sufrido a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas; el flujo de datos transfronterizos. Sobre el favorecimiento de restricción en la circulación de datos a través de fronteras nacionales; la protección de programas. Como solución a los problemas más provocados por la llamada piratería o pillaje de programas de cómputo; los delitos informáticos en sentido amplio. Así como la comisión de verdaderos actos ilícitos en los que se tenga en la computadora un instrumento o fin.

El desarrollo de nuevos ordenamientos destinados a regular el flujo de información a través de sistemas computacionales, tendrá incidencia en el ámbito penal. La Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas (Cassou, 2009).

1. **Fraudes cometidos mediante manipulación de computadoras:**
    a) Manipulación de los datos de entrada.
    b) Manipulación de programas.

c) Manipulación de datos de salida.

d) Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas

a) Utilizando sistemas informáticos como objetos.

b) Utilizando sistemas informáticos como instrumentos.

3. Daños o modificaciones de programas o datos computarizados

a) Sabotaje informático.

b) Virus.

c) Gusanos.

d) Bomba lógica o cronológica.

e) Acceso no autorizado a sistemas o servicios.

f) Piratas informáticos o hackers.

g) Reproducción no autorizada de programas informáticos con protección legal.

La reforma constitucional en materia de delitos informáticos causa un gran impacto al hacer más sencillo el establecimiento de los datos necesarios para el libramiento de una orden de aprehensión; sin embargo, se estima que también es un arma de doble filo, puesto que eventualmente podrán emitirse órdenes de aprehensión sin la certeza jurídica de que exista la totalidad de los elementos necesarios para ello (Cassou, 2009).

La jurisdicción es la facultad que tiene el Estado para administrar justicia (Palomar de Miguel, 2000), la competencia, en cambio, es la atribución legítima a un juez u otra autoridad para el conocimiento o resolución de un asunto (Cassou, 2009).

El artículo 104 de la Constitución Federal (Porrúa, 2012) establece que:

"Corresponde a los tribunales de la federación conocer de todas las controversias del orden criminal que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano".

En razón de ello existen tres órbitas de juzgados que operan sobre el mismo territorio pero que entienden en cuestiones materiales diferentes. Así, por ejemplo, existen tribunales federales, y juzgados de dicha entidad federativa, ambos con poderes de actuación sobre el mismo ámbito territorial pero entienden sobre hechos materiales diferentes.

Mientras que los tribunales del estado, son competentes para conocer respecto de los delitos en los que se dilucidan conductas tipificadas por el Código Penal vigente en el estado, los tribunales federales conocen, por su parte, de las controversias del orden criminal que se suscitan sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano. Además, los tribunales federales intervienen en los casos en que se solicite la extradición de una persona con motivo de la comisión de un delito.

Las cuestiones de competencia han significado desde siempre una problemática de difícil resolución dentro del marco de cualquier sistema jurídico. Los problemas de jurisdicción y competencia vienen desde hace mucho tiempo, tan sólo por citarlo, desde la generación del IUS COMMUNE, el derecho como orden ha encontrado solución parcial a dichos problemas a través de diferentes figuras, ya la declinatoria, ya las cuestiones de competencia, etc. (Campoli, 2005).

Sin embargo, como ya se destacó, la incorporación de nuevas tecnologías a la vida moderna ha traído consigo una nueva problemática jurídica. En consecuencia, surge una serie novedosa de planteamientos jurídicos y entre estos nuevos planteamientos se encuentra la naturaleza de los jueces que deben conocer de los antijurídicos cometidos a través de Internet.

La respuesta debe corresponder a los tribunales de la federación, por lo que lo ideal no es contemplar una serie de figuras jurídicas diseminadas a lo largo de diversos ordenamientos que conformen el sistema jurídico mexicano, sino que deben incluirse en una ley especial en la que de modo sistematizado aglutinen las diferentes conductas lesivas, esa clasificación y distinción no deberá ser determinante y terminal, porque el desarrollo y la innovación tecnológica, de

modo irremediable conduce a que día a día, surjan nuevas y variadas conductas que generen afectación a terceros, por lo que es mejor no establecer conductas casuísticas en dicha ley especial (Cassou, 2009).

También es relevante, la formación del juez de instrucción que deba conocer de los delitos de dicha índole, su preparación debe ser acorde a las nuevas tecnologías que se aplican en materia de informática, sabido es que el juez es un conocedor de derecho, un experto en la materia, pero además de ello debe estar apoyado en un panel de expertos en informática que le provean de las aclaraciones a las dudas que surjan dentro de un proceso jurisdiccional, con independencia de los diferentes dictámenes periciales que las partes ofrezcan para clarificar los puntos en controversia; tal aportación consideramos sería de gran utilidad y beneficio para el mejor desarrollo y eficaz impartición de justicia (Tinajeros, 2006).

En México existe una unidad especializada en delitos informáticos de la Procuraduría General de la República, por lo que sería más conveniente aprovechar los recursos y cobertura tecnológica que se le han asignado para tratar de contrarrestar los ilícitos informáticos que se cometen a través de Internet (Ayala, 2009).

4.3.1 El derecho a la no intervención de las comunicaciones privadas

En el Diario Oficial de la Federación del 3 de julio de 1996, se publicó el decreto mediante el cual se declararon reformados los artículos 16,20, fracción I y penúltimo párrafo, 22 y 73, fracción XXI, de la Constitución Política. Por lo que concierne al artículo 16, la reforma le adicionó dos párrafos, que pasan a ser el noveno y el décimo, por lo que también recorrió en orden progresivo los tres últimos párrafos.

La primera parte del párrafo noveno establece, como regla general, el carácter inviolable de cualquier tipo de comunicación privada, dentro de las cuales quedan incluidas las telefónicas y radiotelefónicas que se mencionan expresamente en la exposición de motivos. La inviolabilidad de las

comunicaciones privadas forman parte del derecho a la intimidad o a la privacía, que ya se encontraba implícito en el primer párrafo del artículo 16 de la Constitución, en cuanto prevé la inviolabilidad del domicilio y de la correspondencia; y que ha sido reconocido expresamente por los artículos 17.1 del Pacto 218 Internacional de Derechos Civiles y Políticos, y 11.2 de la Convención Americana sobre Derecho Humanos. El primero de estos preceptos dispone: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". El artículo 11.2 de la Convención Americana es casi idéntico.

El mismo párrafo noveno del artículo 16 establece la posibilidad de que la autoridad judicial federal autorice la intervención de cualquier comunicación privada. Esta autorización debería haber quedado prevista como una excepción frente a la regla general de la inviolabilidad de las comunicaciones privadas. Sin embargo, la redacción del párrafo no resulta precisa, pues no regula la autorización de la intervención como una verdadera excepción, sino como una muy amplia posibilidad sujeta a lo que dispongan las leyes ordinarias.

El párrafo noveno sólo indica que pueden solicitar la autorización: 1) la autoridad federal que faculte la ley, y 2) el titular del Ministerio Público de la entidad federativa correspondiente: Inicialmente se estimó que por la amplitud de la redacción del párrafo, dentro de la expresión "autoridad federal que faculte la ley" pueden quedar no sólo los agentes del Ministerio Público Federal, sino prácticamente cualquier autoridad federal, con la única condición de que la faculte la ley para tal fin, lo que se descartó con motivo de que es al Ministerio Público a quien corresponde la investigación y persecución de los delitos. La facultad para otorgar la autorización se atribuye exclusivamente a la "autoridad judicial federal", es decir, a los órganos del Poder Judicial de la Federación (Cassou, 2009).

El tema del derecho a la no intromisión de las comunicaciones privadas es un punto álgido en el Internet, Nora Cherñavsky (2003) sostiene que las conductas y contenidos a restringir deben estar tipificadas legalmente, haciendo

compatible las conductas sin valor con el mayor y más amplio de los respetos a la libertad de expresión y al derecho hoy fundamental de tener acceso a la información, con lo que a su juicio se pretende que el ciudadano visualice al Estado como aliado en la lucha contra los riesgos que sufren los beneficios de la expansión de la actividad informática y no como una amenaza a sus derechos a la intimidad y libertad.

Desde el entorno jurídico que rige a México la investigación de los delitos en el Internet (Riquert, 2008) es problemático no sólo por los aspectos de transterritorialidad y trasnacionalidad, sino también porque la Constitución reconoce como un derecho subjetivo público la no intervención de las comunicaciones privadas, entiéndase no como un obstáculo al precitado derecho, más bien, se refiere a la dificultad de que el Ministerio Público en su afán persecutorio logre llevar a cabo las pesquisas necesarias.

Ciertamente, de modo indefectible y sólo en aquellos casos que lo faculte la ley ordinaria, el Ministerio Público podrá solicitar a la autoridad judicial federal la autorización de intervenir las comunicaciones privadas, lo que el legislador ordinario reservó en aquellos casos de que exista delincuencia organizada, en que el Procurador General de la República o el titular de la Unidad Especializada lo consideren necesario, con expresión del objeto y necesidad de la intervención, y que los indicios hagan presumir fundadamente que en los hechos investigados participe algún miembro de la delincuencia organizada.

La medida anterior tiene como objeto proteger el derecho a la comunicación privada, reservándose la intromisión legal, por consiguiente, no existe manera de que el Estado a través de la representación social persiga aquéllos delitos que podrían considerarse no graves por la legislación penal, los ilícitos más comunes son los desvíos patrimoniales a través de Internet, no podrían obtenerse datos provenientes de una intromisión legal a las comunicaciones privadas, en un contexto similar se conduce Marcelo A. Riquert (2008) al señalar la necesidad de actualizar la legislación en relación con los abusos relacionados con la informática que deben ser combatidos con medidas jurídico penales.

Como ejemplo, el fenómeno de robo de identidad (Cassou, 2009), se ha expandido como plaga, en las estadísticas de la Comisión Federal de Comercio de los Estados Unidos de Norte América, sólo en ese país en los últimos cinco años se han robado cuentas bancarias y tarjetas de crédito que han afectado a veintisiete millones de personas, casi el cinco por ciento de los adultos norteamericanos, con un perjuicio de cincuenta mil millones de dólares.

Lo anterior refleja la existencia de delitos informáticos (Riquert, 2008) que sin necesidad de revestir la gravedad que requiere la ley penal, producen una afectación significativa en el detenimiento del patrimonio de muchas personas, por lo que es un verdadero reto tratar de instrumentar los mecanismos necesarios para disminuir la incidencia delictiva a través de Internet por el Estado Mexicano. Además, los tribunales federales intervienen en los casos en que se solicite la extradición de una persona con motivo de la comisión de un delito.

La cuestión que trae el caso bajo análisis debe plantearse en los siguientes términos: Cuando se trata de una conducta lesiva cometida a través del Internet ¿debe comprenderse que la competencia corresponde a los tribunales de la federación o recae en la de las entidades federativas? y de obtenerse una respuesta en tal o cual sentido ¿existe algún motivo jurídico para establecer por qué debe ser uno u otro? (Riquert, 2008)

Con lo anterior descrito es necesario que los delitos que se generen a través del Internet sean del orden federal, esto obedece a que con regular frecuencia se ejecutan por personas que físicamente se encuentran en un país extranjero, situación que desde luego dificulta en gran medida no tan sólo su identificación, sino también su enjuiciamiento.

Otro factor a tomar en cuenta es que el problema se reduce nuevamente a no entender quién o quiénes son los actores de la red y cuál es la funcionalidad de cada uno. Por lo general los órganos jurisdiccionales que atienden las consignaciones correspondientes desconocen y les resulta incomprensible el diferente rol que asume por un lado quien ha elaborado y sistematizado la página, que no es necesariamente la misma que presta el servicio de la página

de Internet, e incluso, puede intervenir un tercero que sólo se encuentra al acecho para infiltrarse en la PC del usuario, todo ello genera que los procesos jurisdiccionales no se estructuren con una dirección adecuada e incluso con grandes limitantes para una entidad federativa, que conduce a que en muchas ocasiones queden impunes.

4.4 NORMAS QUE DEBE TOMAR EN CUENTA UN INFORMÁTICO FORENSE

Actualmente la realidad competitiva de las empresas, hace imprescindible para ellas acoplarse a las tecnologías de seguridad de información disponibles, por lo que es prioritario que las empresas tomen medidas para proteger su información estratégica tanto de ataques internos como externos y a todos los niveles.

La informática forense va mucho más allá de verificar e identificar la intrusión o ataque en los sistemas informáticos de una empresa, una labor importante es adiestrar y concientizar al personal involucrado dentro de la red organizativa y en indicar las medidas preventivas a seguir para evitar que la información de la empresa sea vulnerable.

A medida que el internet crece, lo hace de igual manera el número de acciones ilegales contra la seguridad de las redes corporativas, por ello hay que preguntarse:

a) ¿Quién lleva a cabo estos incidentes?
b) ¿Qué los posibilita?
c) ¿Qué, quién y por qué los provoca?
d) ¿Cómo se evitan?
e) ¿Cómo se producen?
f) ¿Qué medidas se deben implementar?
g) ¿Se pueden realizar acciones jurídicas legales?

Es necesario que las organizaciones concreten sus políticas de seguridad, con el objetivo de planificar, gestionar y controlar aspectos tan básicos como:

• **Definición de seguridad:** Para los activos de información, responsabilidades y planes de contingencias se debe establecer qué hay que proteger y cómo.

• **Sistema de control de acceso**: Se deben restringir y maximizar los permisos de acceso para que cierto personal pueda llegar a una determinada información, estableciendo quién puede acceder a una determinada información y de qué modo.

• **Respaldo de datos:** Hacer copias de la información periódicamente para su posterior restauración en caso de pérdida o corrupción de los datos.

• **Manejo de virus e intrusos**: Establecer una política de actuación ante la presencia de malware, spyware y virus evitando los riegos para la seguridad.

Las políticas y una estimación preliminar de los riesgos, observando y analizando los posibles puntos débiles de la infraestructura organizativa de la red.

Se debe realizar una reunión presencial del personal gerencial y/o directivo para instruirles que:

a) Muchas veces el gasto en seguridad informática es considerado poco rentable.
b) Se debe valorar el costo que les supondría una pérdida de información frente al costo de protegerla.
c) La inversión en las medidas de seguridad será más alta para aquellas aplicaciones que presenten mayor riesgo y un mayor impacto en el caso de ser suspendidas.
d) Las medidas de seguridad tomadas racionalmente, provocarán en las organizaciones beneficios tales como aumento de la productividad, aumento en la motivación e implicación del personal.

En la implementación de políticas de seguridad es importante la implicación de la alta dirección y su concienciación en la importancia que tienen las tecnologías y la protección de la seguridad en el éxito de las empresas. Otros

requisitos previos a la implantación es establecer quién será el encargado de planificarla y aplicarla y la asignación de responsabilidades. El objetivo es conseguir que las medidas de seguridad den resultados a corto plazo pero con vigencia a largo plazo, es decir, no se puede cambiar la política de forma continua, para no crear confusión.

El desarrollo de políticas de seguridad debe emprenderse después de una evaluación de las vulnerabilidades, amenazas y riesgos. Una vez analizado el campo de trabajo, se debe empezar a establecer las medidas de seguridad del sistema pertinentes. Se ha de conseguir sensibilizar a toda la organización de la importancia de las medidas que se deben tomar para facilitar la aceptación de las nuevas instrucciones, leyes internas y costumbres que una implantación de un sistema de seguridad podría acarrear.

Es importante además de planificar, analizar e implantar sistemas y políticas de seguridad, establecer medidas de control, planes de contingencia y realizar auditorías sobre los sistemas implantados y su correcto cumplimiento. Auditar las políticas de seguridad instituidas en la empresa, tiene como objetivos analizar el nivel de cumplimiento de las políticas puestas en marcha y detectar "agujeros" para evolucionar en las mismas.

Por último, se han de conocer las posibles incitaciones que pueden llevar a los usuarios del sistema a cometer "delitos" sobre la seguridad interna para sugerir las soluciones a aplicar.

4.4.1 Análisis de riesgos

La información es un bien muy valioso para cualquier empresa. Garantizar la seguridad de la información es por tanto un objetivo ineludible e inaplazable especialmente del departamento de tecnología de la información. Multitud de amenazas ponen en riesgo la integridad, confidencialidad y disponibilidad de la información.

El análisis de riesgos es un estudio detallado de los bienes a proteger, "intangibles", las amenazas a las que están sometidos, posibles

vulnerabilidades, contramedidas establecidas y el riesgo residual al que están expuestos.

Uno de los objetivos principales de establecer una política de seguridad es el de reducir al mínimo los riegos posibles, implementando adecuadamente las diferentes medidas de seguridad. Cuando se establecen los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional total.

Hay multitud de herramientas para llevar a cabo un análisis de riesgos. Una de las más importantes es MAGERIT ("Metodología de Análisis y Gestión de Riesgos de los sistemas de información de las Administraciones Públicas"), método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Existen otras herramientas como las siguientes:

- MARION
- CRAMM
- BDSS
- RISK
- ARES
- BUDDY SYSTEM
- MELISA
- RISAN, etc.

4.4.2 Reacción y Prevención de Intrusiones

Las normas de seguridad standard establecen que todos los archivos deben estar protegidos en función de la naturaleza de los datos que se almacena en ellos. Además, las empresas deberán tomar precauciones control de acceso, asignación y cambio de contraseñas del personal, especificar las funciones y obligaciones del personal que accede al fichero, hacer copias de seguridad, etc. El informático forense debe verificar el correcto funcionamiento de:

- **Firewalls:** Son programas que evitan que entren personas no autorizadas en el equipo y bloquean la entrada o salida de ficheros que considera sospechosos. A la hora de instalar uno hay que tener en cuenta la preselección del mismo, configurabilidad, actualizaciones y el análisis de los costos.
- **IDS (Sistema de detección de intrusos)**: Alertan de la realización de ataques con éxito e incluso de ataques en progreso. Aspectos sobre un IDS a tener en cuenta:
    a) respuesta
    b) instalación
    c) análisis de los eventos que suceden en la red
    d) facilidad de administración
    e) costo de expansión
- **IRTS**: Es un equipo de personas que llevan a cabo la gestión directa del incidente en el seno de una organización.
- **Antivirus**: Herramientas especializadas en detectar y eliminar virus y otras amenazas de un computador (Existen muchas empresas antivirus, las cuales cuentan con software para servidores).
- **Software Anti-Spam**: Filtra el correo, clasificando e identificando los mensajes indeseados.
- **Análisis forense**: Es muy importante a la hora de analizar los alcances de una intrusión en una computadora.

4.4.3 Consideraciones inmediatas para la auditoría de la seguridad

Las normas que se deben tener para elaborar la evaluación de la seguridad son:

a) Uso de la computadora: Se debe observar el uso adecuado de la computadora y su software que puede ser susceptible a:

- Tiempo de máquina para uso ajeno
- Copia de programas de la organización para fines de comercialización (copia pirata)

- Acceso directo o telefónico a bases de datos con fines fraudulentos

b) Sistema de acceso: Para evitar los fraudes electrónicos se debe considerar de forma clara los accesos al computador de acuerdo a:

- Nivel de seguridad de acceso
- Empleo de las claves de acceso
- Evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo

c) Cantidad y tipo de información: El tipo, cálidad y cantidad de información que se introduce en las computadoras debe considerarse como un factor de alto riesgo ya que podrían producir que:

- La información este en manos de algunas personas
- La alta dependencia en caso de pérdida de datos

d) Personal: Se debe observar este punto con mucho cuidado, ya que habla de las personas que están involucradas al sistema de información de forma directa y se deberá contemplar principalmente:

- La dependencia del sistema a nivel operativo y técnico
- Evaluación del grado de capacitación operativa y técnica
- Contemplar la cantidad de personas con acceso operativo y administrativo
- Conocer la capacitación del personal en situaciones de emergencia

e) Medios de control: Se debe estimar la existencia de medios de control para saber cuándo se produce un cambio o hay fraude (intrusión) en el sistema. Se debe prestar atención con detalle el sistema debido a que podría

generar indicadores que pueden actuar como elementos de auditoría inmediata, aunque ésta no sea una especificación del sistema.

f) Rasgos del personal: Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema, ya que pueden surgir:

- Malos manejos de administración
- Malos manejos por negligencia
- Malos manejos por ataques deliberados

g) Instalaciones: Es imperativo no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar:

- La continuidad del flujo eléctrico
- Efectos del flujo eléctrico sobre el software y hardware
- Evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.
- Verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones

h) Control de residuos: Observar cómo se maneja la basura (temporales, entre otros tipos de ficheros o datos) de los departamentos de mayor importancia, dónde se almacena y quién la maneja.

i) Establecer las áreas y grados de riesgo: Es vital crear una conciencia en los usuarios de la institución evaluada sobre el riesgo que corre la información y hacerles entender que la seguridad es parte de su trabajo. Para esto se deben dar detalles sobre los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe tener un impacto positivo dentro del resguardo de los datos y la seguridad integral dentro de una institución se deben llevar a cabo lo siguiente:

a) Definir elementos administrativos
b) Definir políticas de seguridad
c) A nivel departamental
d) A nivel institucional
e) Organizar y dividir las responsabilidades
f) Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
g) Definir prácticas de seguridad para el personal:
h) Plan de emergencia (plan de evacuación)
i) Números telefónicos de emergencia
j) Definir el tipo de pólizas de seguros
k) Definir elementos técnicos de procedimientos
l) Definir las necesidades de sistemas de seguridad para: hw y sw
m) Flujo de energía
n) Cableados locales y externos
o) Aplicación de los sistemas de seguridad incluyendo datos y archivos
p) Planificación de los papeles de los auditores internos y externos
q) Planificación de programas de desastre y sus pruebas (simulación)
r) Planificación de equipos de contingencia con carácter periódico
s) Control de desechos de los nodos importantes del sistema:
t) Política de destrucción de basura copias, fotocopias, etc.

Finalmente la normatividad es importante para el CF, sin la normatividad el CF no tendría como protegerse y regularse, las leyes son importantes, aunque en México la iniciativa de ley se creen y se desarrolle lentamente.

CAPITULO 5

CÓMPUTO FORENSE EN MÉXICO

Capítulo 5 CÓMPUTO FORENSE EN MÉXICO

En este capítulo se dará a conocer la actividad que tiene el cómputo forense en México, la empresa que se especializa en delitos informáticos en México así como las diferentes actividades que tiene esta empresa para resolver algún delito informático.

5.1 APLICACIONES

Esta es una nueva especialidad dentro de la ciencia forense; su presencia en nuestro país se sitúa desde hace una década y al igual que los especialistas en computación y sistemas así como los relacionados con el acceso a internet, es una herramienta útil para iniciar o reforzar causas judiciales y por otro lado para prevenir los delitos que continuamente se cometen por medio de la red.

Hoy en día el cómputo forense no sólo se aplica en nuestro país desde el punto de vista de persecución de delitos, también a nivel interno en las organizaciones, principalmente para detectar si alguien de la misma empresa ha realizado comunicación o transferencias de información de la empresa a un tercero.

Asimismo se utiliza para:

a) Validar la seguridad de las computadoras que realizan las transferencias electrónicas bancarias,
b) Identificar cómo se realizó un ataque a los servidores internos,
c) Comprobar el robo de secretos industriales o propiedad intelectual haciendo uso de las computadoras, la transferencia de numerarios a cuentas personales por parte de las personas que tienen acceso a la banca electrónica y muchas cosas más.

La computadora o teléfono celular saben más de lo que uno cree, las contraseñas, visitas a Internet, programas que se ejecutan en la computadora, fotografías que se descargan, compras que se realizan en línea, todo queda registrado en los dispositivos electrónicos que se utilizan y aunque se borren los historiales de archivos o programas que utilicen, la evidencia siempre se queda en los dispositivos.

"La evidencia es como obtener una huella digital y se hace toda una investigación en la escena del crimen", explica Andrés Velázquez (2012), fundador y director de MaTTica, primera firma dedicada al cómputo forense en México.

Con las herramientas forenses se puede saber cuántas veces se ha ejecutado Word en una computadora, ya que existen pequeñas cajas negras que guardan todo. Cuando se escribe en una computadora o en un iPad se están grabando en esta caja nuevas palabras, números de cuenta, teléfonos de parientes, es decir todo lo que se escribe (Sánchez, 2012).

5.2 LABORATORIO DE INVESTIGACIONES DE DELITOS INFORMÁTICOS

MaTTica es un laboratorio especialista en investigar casos de ataques cibernéticos o robos de información a empresa. Ser víctima de un ataque cibernético puede causar pérdidas considerables debido al valor de la información, sin embargo menos de 40 por ciento de los usuarios que utilizan *gadgets (*dispositivo electrónico que tiene un propósito y una función específica*)* protegen sus datos, lo que incrementa su vulnerabilidad.

En este laboratorio usando tecnología especializada, los investigadores forenses realizan una copia fiel del ordenador sujeto de investigación, y es en este duplicado donde los expertos en cómputo forense buscan e interpretan la información para averiguar quién, cómo y cuándo pudo haber perpetuado un delito a través de las tecnologías de la información.

En México, entre 27 y 30 por ciento de las personas que venden o regalan su celular no eliminan su información; 70 por ciento no borra usuario y contraseña en redes sociales y, de acuerdo con la firma CPP (Profesional de protección Certificado), uno de cada tres que adquiere un *gadget* de segunda mano encuentra datos confidenciales, cinco por ciento de éstos son datos bancarios (Chávez, 2011).

5.2.1 MaTTica

Mattica es una empresa que ofrece servicios de investigación digital para la reacción ante incidentes relacionados con el robo de información, fraudes, espionaje, amenazas y cualquier mal uso de la información sensible dentro de la organización. Para el sector público utiliza estos servicios además de la tecnología de punta para la correcta impartición de justicia, labores de inteligencia y seguridad estatal o nacional. A continuación se presenta una descripción de sus servicios:

- **Investigaciones digitales**: Están conformadas por técnicas científicas y analíticas a infraestructura tecnológica cuyo objetivo es identificar, preservar, analizar y presentar información almacenada en medios digitales que permitan determinar la posible autoría de acciones, que pueden ser una amenaza, estos procedimientos cumplen con los requerimientos legales.

- **Implementación de laboratorios**: Tienen experiencia en implementación y ofrecen consultoría especializada que abarca desde el dimensionamiento, definición de la capacidad de las investigaciones que se realizarán; procedimientos, formatos, capacitación y el suministro de hardware y software especializado para sector privado y público.

  - **Sector Privado**: se detectan incidentes relacionados con el manejo de la información digital en la organización como: robo o fuga de información, fraudes, espionaje industrial, violación a los derechos de

autor, difamaciones y abuso de confianza entre otros, incluyendo las instituciones financieras.

- **Sector Público**: se denominan como Unidades Especializadas en la Investigación de Delitos Informáticos; creados para investigar y perseguir delitos que usan la tecnología como medio o fin, siendo entonces indispensables para la correcta impartición de justicia, labores de inteligencia y seguridad estatal o nacional. Son distribuidores autorizados de las herramientas líderes en el mercado para el análisis de sistemas operativos (Windows y Mac), análisis forense en vivo, teléfonos celulares, protectores contra escritura y estaciones forenses digitales especializadas.

- **Borrado seguro:** El borrado tradicional de la información contenida en un medio de almacenamiento simplemente elimina las tablas que indican en dónde está ubicada la información, pero los datos permanecen en el disco.

- **Recuperación de datos**: MaTTica puede realizar la recuperación de información a nivel lógico cuando alguien por error o descuido elimina o le da formato a la información contenida en un disco.

  Cuando se presenta un daño en el hardware del disco duro, es posible intentar la recuperación de información a nivel físico, como aquellos afectados por una caída, discos duros baleados o incluso hasta aquellos involucrados en algún incendio.

- **Apoyo jurídico:** Apoya a despachos de abogados, abogados internos y otros a interpretar y asesorar para proceder legalmente ante pruebas para poder judicializar o perseguir un delito.

- **MaTTica Universitty:** Brinda capacitación especializada en investigaciones digitales y cómputo forense tanto presenciales como en línea, imparten cursos *(www.mattica.com*).

En su oficina del piso número 12 ubicada en la Ciudad de México, rodeado por documentos y una alta seguridad que denota la filosofía de Mattica en la práctica, Andrés Velázquez explica que rastrear información de un equipo vulnerado es posible gracias a la memoria de los discos duros y en general del *hardware*, que gracias a sensores acumulan todo lo que se haga en ellos.

El delito informático no está tipificado, lo que hace complicado utilizar los hallazgos del cómputo forense como pruebas; sin embargo, Velázquez advierte que el objetivo principal es crear cultura en torno a la ciber seguridad para establecer mejores prácticas dentro y fuera de organismos empresariales, gubernamentales y personales.

5.2.2 El cómputo forense en MaTTica

En MaTTica, a un especialista forense se le llama CSI (Crimine Scene Investigation) de las computadoras porque llega a la escena del crimen para obtener y extraer datos de una forma que tenga una validez legal, y analizar su contenido.

Andrés Velázquez dice que:

"Los peligros potenciales en el ciberespacio van en aumento. En el 2011, la creación de nuevos virus y software malintencionado creció 41% en el 2011 respecto al año anterior con 403 millones de nuevas amenazas, reveló la firma de seguridad informática Symantec en su Reporte de Amenazas a la Seguridad en Internet, publicado el año pasado. Pero es el robo de información lo que más preocupa a los clientes que acuden a MaTTica" (Sánchez, 2012).

De acuerdo con Symantec (2012), en los primeros meses del 2012, la filtración y robo de datos de empresas creció 41% respecto al año pasado. En el 2011, las pérdidas por este delito ascendieron a los 5.5 millones de dólares en el 2011.

Con o sin intención, "todos pueden ser delincuentes" de robo de información al guardar documentos del trabajo en el correo electrónico personal o al recopilar información interna de la empresa donde se trabajó anteriormente asegurando que el 80% de los robos de información tienen que ver con gente dentro de la organización, de los cuales el 34% es con dolo. La mayoría de las empresas se preocupa por los hackeos o crackeos a un servidor su empresa, pero casi nadie se preocupa de la gente que tiene dentro (Sánchez, 2012).

Desde hace más de 10 años, Andrés Velázquez ha estado envuelto en investigaciones digitales, cuando nadie se estaba especializando en esta disciplina en México, este escenario motivó al experto en cómputo forense a crear MaTTica.

Hace algunos años Andrés Velázquez fué al Consejo de la Judicatura para presentar su solicitud para ser perito en cómputo forense y le contestaron que esa disciplina no existía.

MaTTica ha apoyado a policías cibernéticas y a las áreas de investigación de las autoridades judiciales, además han trabajado con instituciones internacionales como la Organización de las Naciones Unidas (ONU) y la Organización Internacional de Policía Criminal (Interpol).

Al respecto Velásquez dijo:

"Se platicó con Ministerios Públicos, incluso con los peritos que están aplicando para entrar a la PGR y la mayoría no tienen idea de esta rama. El gran problema es el desconocimiento de la poca ley que existe; además de que no se han aceptado iniciativas de ley que permitan llegar a aspirar a cooperación internacional y tener más claro las tipificaciones del combate a los derechos informáticos" (Sánchez, 2012).

Velázquez mostró cómo recuperar archivos de datos, lo hizo con una serie de programas que leen el MBR (Registro de memoria principal) de un dispositivo y

más allá tienen la capacidad de leer el hexadecimal del sistema de archivos. Ante los ojos de los espectadores en Campus Party el experto pudo saber cuál es el tipo de archivos de una memoria USB, desplegar o visualizar los encabezados, hacer la búsqueda del contenido de los mismos y recuperarlos exitosamente, de igual manera mostró cómo acceder a información sobre los archivos mismos, los metadatos de una foto, la fecha de creación de un documento de Word o la última vez que un usuario modificó la información y en ciertos casos hasta quién lo modificó. En algunas ocasiones los investigadores forenses digitales han podido recuperar datos eliminados de un teléfono celular.

Es difícil que un usuario lea el contrato de uso de Twitter, Facebook o Flickr. Aquí, está el primer error, ya que se aceptan obligaciones y derechos en forma legal, incluso sobre manejo y divulgación de la propia información sin conocerlos, el segundo error es que en ocasiones se omiten las preferencias de privacidad y, por tanto, se comparte más de lo que se quisiera con los demás y el tercer error es que se proporciona información en exceso como fotografías, ubicaciones y datos personales (Bazán-Canabal, 2010).

No se debe olvidar que cualquier usuario con acceso a nuestra información puede republicar o utilizar los datos libremente, y el uso que le dé está fuera del alcance de las leyes de protección o acuerdos de privacidad con la red social en cuestión.

El hecho es, que cualquier comportamiento, descuido, error o actividad que se realice en las plataformas sociales web genera una evidencia (huella digital), casi imborrable, que vulnera la privacidad de las personas y los expone, mientras más datos se proporcionen, más información se puede obtener.

5.3 UN CASO EN CHIHUAHUA, POLICÍA CIBERNÉTICA

La Unidad Estatal de Delitos Electrónicos e Informáticos, conocida como la Policía Cibernética, a unos meses de su creación ha registrado 52 ataques de

la ciber delincuencia, entre pederastia, suplantación de identidad, fraude, extorsión, acoso sexual, homicidio y otros.

A la fecha ha resuelto 40 casos de los que le han denunciado, con un patrullaje intenso en 17 redes sociales, en los principales servidores de correo electrónico y el mundo de la banda ancha, una tarea a la que la Fiscalía General del Estado comienza a destinar cada vez mayores recursos en vista de las nuevas modalidades del crimen.

Las armas de los elementos de la Policía Cibernética no son muy sofisticadas, una computadora, acceso a internet y la inteligencia de cada uno de ellos y, aunque no usan pistola, radios ni esposas, han logrado la detención de extorsionadores, homicidas y defraudadores, delincuentes que aprovechan las tecnologías de la información para realizar ataques virtuales y reales.

El reporte de la Unidad Cibernética de la Fiscalía indica que durante un año y 4 meses (30 de abril del 2012) se han cortado los conductos de redes que incurren en delitos o en violaciones a las leyes mediante el patrullaje, la denuncia de afectados y la utilización de herramientas tecnológicas como la intervención directa en sitios ilegales que suplantan la identidad o incurren en otros ilícitos.

Esa nueva división de investigación trabaja con un agente del Ministerio Público asignado y una gran cantidad de elementos que, sin uniformes, sin ser detectados, sin ser ubicados físicamente, investigan y patrullan la red, operan conexiones con grandes servidores de correo electrónico como Gmail y Hotmail, para detectar amenazas y ubicar delincuentes involucrados en todo tipo de delitos.

El número de agentes cibernéticos es un misterio, no se revela por razones de seguridad, pues están involucrados en investigaciones delicadas todos los días y tienen la estrategia de trabajar así, desde el anonimato, para no ser detectados y poder entregar mejores resultados.

De acuerdo con los reportes internos, trabajan en investigaciones sobre pederastia, suplantación de identidad, fraude, amenazas, extorsión, homicidios, acoso sexual, administración fraudulenta e incluso terrorismo virtual y real, las cuales se mantienen bajo reserva, pues los resultados mostrados hasta la fecha han sido satisfactorios, en buena medida por la secrecía de las pesquisas que realizan los agentes.

La Policía Cibernética mantiene presencia formal en Facebook, Twitter, Sonico, Hi5, Twoo, Orkout, Friendster, Econozco, Neurona, Dejaboo, Xing, Google+, Badoo, Metroflog, Fotolog, MySpace, entre otras plataformas, pero además los elementos realizan un patrullaje diario, encubierto, para detectar posibles riesgos y amenazas.

De manera paralela, otros elementos de la corporación se dedican a investigar denuncias ya presentadas por la vía tradicional ante el Ministerio Público o las que se reciben diariamente vía correo electrónico.

La corporación nació en la Fiscalía del Estado ante la necesidad de una unidad especializada para atender la nueva generación de crímenes, así como los delitos tradicionales que tienen como herramienta algún tipo de tecnología, sobre todo internet y la utilizada en los teléfonos celulares.

Anualmente, 431 millones son afectados en todo el mundo por ataques informáticos, de acuerdo a reportes de la Organización de Naciones Unidas, por lo que el gasto en seguridad en la red de empresas de todo tipo ha llegado al récord de 338 mil millones de dólares. Pese a ello, la ciber delincuencia ha obtenido ganancias globales de 12 mil 500 millones de dólares (MaTTica, 2012).

En México, el 83 por ciento de los internautas adultos fueron víctimas de algún tipo de delito mientras navegaban en internet, con pérdidas de casi 2 mil millones de pesos. La situación se agrava en Estados con grandes adelantos tecnológicos como Chihuahua (MaTTica, 2012).

Las cantidades ganadas por la ciber delincuencia se vuelven cada vez mayores y pueden compararse con otros delitos como el tráfico de drogas, armas o personas, pero con una ventaja adicional, los delincuentes no exponen el pellejo, ya que operan desde las computadoras, teléfonos celulares y otros dispositivos móviles.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Se cumplió con el objetivo de realizar un análisis documental para dar a conocer la disciplina denominada Cómputo Forense y la importancia que tiene en nuestros días, su evolución y el impacto que tiene en México, así como su metodología y herramientas que emplea una evidencia digital.

Se dieron a conocer las herramientas y la metodología que se utiliza para analizar una evidencia digital en el CF para aclarecer un hecho en el que se ha incurrido en un delito.

El cómputo forense es disciplina encargada de la investigación de los delitos y abusos relacionados que tienen que ver con las computadoras y con las redes que las conectan, de una manera repetible y competente.

El objetivo de la informática forense es ayudar a la justicia a esclarecer los delitos informáticos tales como fraudes, extorsión telefónica, asesinatos, pornografía infantil, narcotráfico, robo a tarjetas de crédito e incluso proteger a personas que sean acusadas injustamente por jerarquía que se da en una empresa, mediante un análisis de evidencia que le permite de manera certera y eficaz detectar, identificar, recuperar las pistas suficientes para esclarecer algún hecho que perjudique la estabilidad de una persona o empresa.

La IF hace uso de herramientas forenses que permiten la recuperación de evidencias digitales, ya sea la recuperación de información de discos duros, memorias flash, memorias de cámaras digitales, teléfonos celulares, dispositivos de audio, todo aquel dispositivo que almacene datos, ya que mediante su análisis forense se encuentra información verídica que no puede ser alterada debido a que los procedimientos que usan estas herramientas forenses no permiten que se pueda alterar o filtrar información que ocasione la falta de credibilidad en la información encontrada en una evidencia electrónica así es que esta puede ser presentada ante un juez.

El CF es una disciplina muy novedosa y que puede dar mucho auge y ayudar a encontrar pistas de forma precisa no importa que la información sea borrada ya

que el uso de sus herramientas permiten recuperar todo tipo de archivos aun cuando toda la información sea borrada se recupera, mostrando todos los datos, cuándo fue creado, cuántas modificaciones sufrió, cuándo se eliminó, fechas de acceso, cuántas veces se utilizó además de mostrar las características de cada uno de los archivos o documentos que se encuentren dentro de la evidencia electrónica.

Es una disciplina relativamente nueva lleva pocos años está muy fuerte en países como Argentina, Bolivia, España, E.U. y Venezuela, desafortunadamente en México está muy débil debido a las leyes que rigen actualmente en México, no existe una reforma que ampare un procedimiento forense, solo se hace mediante una orden judicial emitida por un juez que solicite un peritaje, hace falta darle credibilidad regulándola para que sea válida.

Desafortunadamente en México el crear una ley ó realizar una reforma es muy lento debido a que se necesita cometer el delito para crear una ley o reforma, el sistema mexicano no prevee como proteger un delito antes de cometerlo sino una vez cometido crean la ley para poder proteger y castigar el delito cometido, por lo tanto se necesita dar a conocer esta disciplina CF y lo importante que es para resolver algún caso en el que se haya incurrido en un delito, esto cambiaria a México en la forma en la que resuelve sus delitos cometidos mediante medios digitales además con las herramientas y equipo forense permite un avance tecnológico.

En México para ser un informático forense se tiene que tener experiencia en alguna área informática, por su profesión requerirán obligatoriamente presentar la Cédula Profesional, para acreditar de haber cursado y terminado la licenciatura de su especialidad, ejemplo si es de la rama de Ingenierías, con sus subdivisiones (Civil, Mecánico, Electrónico, Informática, Computación, etc.) acreditarán la Licenciatura en Ingeniería, con su especialidad. El perfil que debe de complementar a un informático forense es tener conocimientos en las herramientas forenses, conocer las nuevas tecnologías de información así

como las nuevas tecnologías de investigación informática y mantenerse a la vanguardia.

Una problemática que presenta el CF es la falta del conocimiento sobre esta disciplina debido a que los profesionales de Derecho desconocen cómo trabaja, las características que tiene y el tipo de herramientas que emplea y sobretodo que son pruebas tan fiables que no puede existir error o alteración alguno de alguna evidencia encontrada porque las herramientas que emplea un Informático forense detecta todo tipo de modificación realizada a cualquier documento.

RECOMENDACIONES

Las empresas deberían tener un laboratorio de Informática Forense como seguridad y así resolver problemas internos y junto con la justicia esclarecer los malos manejos de información en diferentes instituciones y que personas que pueden ser inocentes y fueran acusadas de mal manejo informático por precautela de la información puedan ser sancionadas.

En México mientras una iniciativa de ley no se concrete, se penalice o capacite a servidores públicos para poder reconocer y realizar procesos judiciales apoyados en la evidencia electrónica encontrada por un Informático Forense, seguirán existiendo huecos legales que los cibercriminales seguirán utilizando para hacer sus fechorías, el Cómputo Forense necesita ser válido en procedimientos y leyes jurídicos para que tome fuerza y sea objeto de estudio para los profesionales del Derecho.

Como propuesta se sugiere un proyecto o trabajo de investigación a desarrollar entre un Lic. en Derecho y un Lic. en Ingeniería en Computación el tema de “Propuesta de reforma de ley para regular el Procedimiento de Informática Forense”.

REFERENCIAS

ACISSI. (2011). *Seguridad informática Ethical Hacking . Conocer el ataque para una mejor defensa* (ENI ed.). España.

Alfaomega. (2012). *Código Penal Federal*. México: Alfaomega.

Areritio, J. (2008). *Seguridad de la Información Redes, Informática y Sistemas de Información*. Madrid, España: Paraninfo.

Ayala, S. C. (2009). *Elementos necesarios para la creación de una legislación integral en materia de delitos informáticos en México.* Universidad Michoacana de San Nicolás de Hidalgo, Morelia, Michoacán.

Batiz, V. (2004). Panorama general del marco jurídico en materia informática en México. *Revista de Derecho Informático*.

Bazán-Canabal, C. A. (2010). Entre el cómputo forense, las redes sociales y la vida diaria. *Netmedia online*.

Brungs, A., & Jamieson, R. (2003). *Legal issues for computer forensics. .* Paper presented at the Conference on Information Systems, Australia.

Campoli, G. (2005). Pasos hacia la reforma penal en materia de delitos informáticos en México. *Revista de Derecho Informático, 79*.

Campoli, G. (2006, diciembre de 2006). Los dos delitos más comunes y controversiales por medios informáticos: clonación de tarjetas de crédito y phising o transferencias electrónicas y legítimas. *Revista de Derecho Informático*.

Cano. (2006). Introducción a la informática forense. *Revista ACIS*.

Cano. (2009). Estado del arte del peritaje Informático.

Cano. (2010). *Contra el Fraude, Prevención e Investigación en América Latina* (Management ed.). Argentina.

Casey , E. (2002). *Handbook of Computer Crime Investigation: Forensic Tools and Technology*. San Diego California, USA: By Casey Eoghan.

Cassou, J. (2009). Delitos informáticos.

Colobran, M., Arqués, J. M., & Galindo, E. (2008). Administración de Sistemas operativos en Red. *Rambia del Poblenou,* 156.

Consejo de la Judicatura Federal, M. (2008). *Videoconferencia "Delitos cibernéticos.* Paper presented at the Delitos cibernéticos, Veracruz.

Chávez, G. (2011). MaTTica, El negocio del cómputo forense en México. *El Excelsior*. Retrieved 07 de Diciembre de 2012, from http://www.excelsior.com.mx/index.php?m=nota&id_nota=772112

Gutiérrez, J. D. (2006). Informática Forense

Hikal, W. (2009). *Introducción al estudio de la Criminología* (Porrúa ed. Vol. Primera edición). México D.F.: Porrúa.

Intelcard Systems, C. (2012). Ciber Forensic. Retrieved 16 de Septiembre, 2012, from http://anticyberforensics.wordpress.com/2010/02/20/intellectual-property-intel-corporation-v-intelcard-systems-sdn-bhd-ors-high-court-malaya-kuala-lumpur/

López, O., Haver, A., & León, R. (2001). Informática Forense: Generalidades, aspectos técnicos y herramientas. Universidad de los Andes. Colombia.

Manzo, G. (2008). Un caso práctico de la Informática forense. *Geronet*.

MaTTica. (2012). En Chihuahua: resuelve 40 casos la policía cibernética. *El Heraldo de México*. Retrieved 04 de diciembre de 2012, from http://www.mattica.com/2012/04/mexico-chihuahua-resuelve-40-casos-policia-cibernetica/

Merida, I., & Fredesvinda, L. H. (2008). Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad; un proyecto europeo. *5*(2), 139-152.

Muñoz, O. (2002). La convención sobre delitos informáticos. *Revista de derecho informático*.

Nits. (2012). Información de Tecnología. Retrieved 17 de septiembre, 2012, from http://www.nist.gov/itl/

Noblett, M. (2000). *Recovering and Examining Computer Forensic Evidence* (Hall ed. Vol. 2).

Palomar de Miguel, J. (Ed.) (2000) Diccionario de juristas (Vols. II). México: Porrúa.

Porrúa (Ed.). (2012). *Constitución Política de los Estados Unidos Mexicanos*. México.

Ramirez, G. A. (2012). Informática Forense. Universidad de San Carlos Guatemala, Facultad de Ingeniería.

Ramos Junior, H. S. (2008). Delitos cometidos contra la seguridad de los sistemas de informaciones de la administración pública brasileña, Revista de Derecho Informático, núm. 115, febrero de 2008. *Revista de Derecho Informático, núm. 115*.

Riquert, M. A. (2008, Marzo de 2008). "Estado de la legislación contra la delincuencia informática en México-Sur". *Revista de Derecho Informático*.

Sánchez, J. (2012). Cómputo forense: los CSI de la Informática. *El economista*.

Tinajeros, E. (2006, septiembre de 2006). Nuevas formas de delinquir en la era tecnológica: Primeras observaciones sobre espionaje, fraude y sabotaje informático. *Revista de derecho informático,* 298.

White, D., Rea, A., Mckenzie, B., & Glorfled, L. (2004). *A model and guide for an introductory computer security forensic course. Proceedings of the Tenth Americas Conference on Information Systems.* Paper presented at the A model and guide for an introductory computer security forensic course. Proceedings of the Tenth Americas Conference on Information Systems, New York.

Xombra. (2012). Cómputo Forense o Informática Forense. Xombra. Retrieved 04 de Septiembre de 2012, 2012, from http://www.xombra.com/go_news.php?articulo=1942

YanapTI (Writer) (2009a). Informática Forense INFOFOR 2009 PII. In Q. n. m. pierda (Producer), *Que no me Pierda* Bolivia.

YanapTI (Writer) (2009b). Laboratorio de Informática Forense. In Bolivisión (Producer). Bolivia