UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“UNA INTRODUCCIÓN AL CÓMPUTO FORENSE”

TRABAJO ESCRITO EN LA MODALIDAD DE EXAMEN GENERAL

DE CONOCIMIENTOS QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA: ***DURÁN GÓMEZ KELLEN IRWIN***

ASESORA: ***ING. SILVIA VEGA MUYTOY***

MEXICO, D.F. ABRIL 2008

DEDICATORIA

Agradezco en primeramente a mis padres y hermanos, quienes de una u otra forma han influido en mi vida para tratar de hacerme una mejor persona, aquellos que con cariño, comprensión, preocupación y apoyo me dieron una formación, quienes de la misma forma con observaciones, regaños y energía me hicieron ver mis fallas como ser humano y como hombre.

A las mujeres de mi familia, por que han sido de alguna forma todas parte fundamental en mi desarrollo, desde mis abuelas, de quienes no he tenido más que cariño y confianza, mis tías, quienes han sido para mí desde madres hasta amigas, por supuesto la más importante, mi madre, porque de ella siempre aprendí que la fuerza de voluntad es lo que te permite lograr tus objetivos, que si sigues un camino recto en tus objetivos, logras llegar a ellos, mi hermana, que me ha enseñado a ver las cosas desde otra perspectiva y quien también me ha acompañado durante mi crecimiento.

A los hombres de mi familia, que siempre me han mostrado cariño, preocupación, que han sido ejemplo en mi formación, quienes siempre me demostraron apoyo de las formas más desinteresadas y nobles que pude haber imaginado. Mi padre y mi hermano, quienes me están demostrando que se puede cambiar cuando realmente se quiere hacerlo, mis tíos, que nunca han dejado de estar ahí pese a diferencias o distancias.

A todos ustedes que de alguna manera me han acompañado en mi vida durante grandes o cortos periodos de tiempo, les agradezco y espero que la vida me permita estar igual ahí para ustedes, porque esta sería una de mis mas grandes alegrías.

Durán Gómez Kellen Irwin

INDICE

OBJETIVO

Dar a conocer los principios básicos de los que se compone el cómputo forense en las distintas vertientes del conocimiento en que este puede aplicarse, sus principales áreas de oportunidad así como la gran necesidad de contar con métodos y estrategias de investigación forense en la recuperación de información, legislación y prevención, que día a día aumenta a nivel mundial.

INTRODUCCIÓN

En este documento, se abordará un tema de gran interés a nivel mundial y que es crucial para el desarrollo de informática y las comunicaciones, el cómputo forense, el cual representa una rama de la seguridad informática, la cual brinda grandes retos y nos representa una serie de posibilidades que hoy por hoy son necesarias en prácticamente todos los sectores. Se tratará de dar un panorama introductorio que permita generar un interés en un tema que aún para muchos ingenieros y las personas en general es algo no muy conceptualizado como tal. Muchos piensan que el cómputo forense es solo aquel que se encarga de las aplicaciones que se usan en las investigaciones, tales como simulaciones y recreaciones de eventos ocurridos, reconstrucción de rostros o cuerpos humanos. La panorámica general que se abarca, es apenas el inicio de un área llena de oportunidades, tanto para desarrolladores, como para aquellos que quieran realizar este tipo de investigación, con todas las herramientas y técnicas que implican. Se trata también de dar una vista muy a groso modo de la situación legal y el como este campo potencial, esta afectando muchas áreas a su alrededor con su crecimiento, tal es el marco legal bajo el que se necesitan sustentar muchas investigaciones forenses, debido a su fácil invalidación por no existir aún lineamientos con consistencias suficientes.

Veremos que el cómputo forense es algo más que lo que usualmente se creé que es, debido a que ésta es la encargada de tomar a equipos de cómputo y enfocarse a ellos, así como a sus partes como un objeto de investigación más que como una herramienta para la solución de un problema. En este caso el daño es hecho al equipo o con el equipo.

El documento esta elaborado con un carácter general y trata de exponer del modo más claro posible las múltiples características de este campo, así como de dar una implicación de sus orígenes y la creciente necesidad que lo sustenta.

El trabajo tiene un enfoque introductorio, se trata de hacer referencias generales a algunos puntos que con mayor profundidad, requerirían muchísimo tiempo. También debe mencionarse que muchas herramientas no son mencionadas, debido a que en estos momentos hay muchas y muy poderosas, así que sólo se hace referencia a las más comunes de modo que nos permitan ver cual es su aplicación.

I. ASPECTOS BÁSICOS DEL CÓMPUTO FORENSE

JUSTIFICACIÓN

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho

para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.
Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"
Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.
Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.
No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

1. ASPECTOS BÁSICOS DE CÓMPUTO FORENSE

1.1 CONCEPTOS PREVIOS

A continuación, se presentarán algunos conceptos que deben ser mencionados para la mejor comprensión de los puntos que se abordan más adelante. Se da una breve descripción de sus orígenes, así como el motivo que justifico su concepción. Dándonos así una perspectiva más amplia que nos permita ser más objetivos y tener una mejor asimilación del tema.

- **Hacker**

Interesado en la investigación y conocimiento de cómo operan los dispositivos, la mayoría son buenos programadores, conocen el porque de las vulnerabilidades, siempre en busca ávida de información..[1]

En la década de 1960, el término "hacker" se usaba para referirse a alguien que era considerado un buen programador de computadoras, un maestro en los sistemas de cómputo, capaz de manipular programas y hacer todo lo que quieran con ellas. Los primeros hackers que surgieron en el Instituto Tecnológico de Massachussets (MIT) en los años 60's estaban impulsados por el deseo de dominar las complejidades de los sistemas computacionales y de empujar la tecnología más allá de sus capacidades conocidas.
A finales de los 60's y principios de los 70's, el término "hacker" era asociado con un grupo extremo radical, el movimiento "yippie"[2] La palabra hacker aplicada en la computación se refiere a la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites que tendría la mayoría de la gente. Lo hackers son muy curiosos, prueban todas las formas que ellos conocen para poder acceder a sistemas. No cesan en la investigación de un sistema que están estudiando hasta que los problemas que se le presenten quedan resueltos.[3]

[1] http://www.unam-cert.unam.mx

[2] La corriente yippie fue un movimiento hippy anarquista, particularmente oscuro. Los yippies tomaron su nombre de un partido de ficción el"Youth Internacional Party", que llevaron acabo una política escandalosa y surrealista de subversión surrealista y una maldad política desproporcionada.
[3] http://www.monografias.com/trabajos12/hacking/hacking.shtml

- **Cracker**

Persona que utiliza en forma indebida los conocimientos adquiridos para hacer daño a los sistemas de cómputo. [4]

Es otro término que se origina durante los primeros años de las comunicaciones electrónicas, usado para describir a aquellos individuos que rompían sistemas de seguridad. Aunque en realidad las definiciones están muy divididas hacia este tipo de personas en general se les considera los verdaderos culpables de los problemas que existen en la Internet. Se dice que ellos son los responsables de crear virus informáticos y dañar todo lo que esta a su alcance.

- **Delito Informático**

Se define como delito informático a cualquier actividad o conductas ilícitas, susceptibles de ser sancionadas por el derecho penal, que en su realización involucre el uso indebido de dispositivos informáticos como medio o fin.

Los delitos informáticos se incrementan en función de las posibilidades de las personas de adquirir computadoras y otras tecnologías, mientras más bajan los costos de los equipos mayor cantidad de gente se incorpora al uso de las nuevas tecnologías. Los países industrializados tienen pleno acceso a la tecnología de la información, los niños comienzan su aprendizaje del uso de las PC en la escuela primara, y la gente tiene acceso gratis a equipos de cómputo en librerías o universidades, también pueden rentar éstos en un Café Internet, la mayoría de las personas saben como enviar un correo o como descargar un archivo a través de la Internet, esto no requiere tener grandes conocimientos en el uso de los recursos informáticos. Hoy día algunos criminales informáticos requieren ser muy buenos programadores (ellos serían la elite hacker), pero muchos Otros no necesitan tantos conocimientos. Con avanzadas habilidades técnicas es fácil para un criminal informático hacer todo lo que se le ocurra, como sacar información de equipos remotos, o alterar la información, dar de baja equipos, etc.

[4] M. Farías-Elinos & V. Bátiz-Álvarez LIDETEA / Escuela de Ingeniería / Facultad de Derecho Coordinación General de Investigación Universidad La Salle Grupo de Seguridad de RedCUDI (Internet-2 México)

1.2. CÓMPUTO FORENSE

Actualmente este se ha convertido en una herramienta indispensable desde niveles corporativos hasta ambientes domésticos, debido a las distintas áreas que día a día esta conquistando la tecnología y a la integridad que en cada uno de sus datos le requiere.

Seguridad en cómputo

La informática forense forma parte de la seguridad en cómputo, **la seguridad en cómputo** se compone de diversos procesos y técnicas que buscan brindar integridad en los sistemas de información, también tiene diversas etapas, se puede decir que la seguridad en cómputo busca prevenir cualquier ataque o intrusión no autorizada a un sistema, hay dos diferentes formas de reaccionar en un ambiente de seguridad, de manera **proactiva y reactiva**, en la forma proactiva se encuentran todos los componentes tanto físicos como lógicos, como son los firewalls, detectores de intrusos, control de acceso tanto al medio como a los centros de cómputo, etc. En la forma reactiva se encuentran los planes de contingencia, servidores de respaldo, y es en este apartado donde entra la informática forense, pues una vez que se han visto vulnerados los sistemas de seguridad de la red de datos y que ha recibido algún tipo de daño, es el trabajo de la informática forense determinar quién y cómo consiguió dañar o simplemente entrar a una red privada, pero también en este proceso de investigación el informático forense debe obtener evidencia que sirva para poder fincar responsabilidades judiciales al autor de algún delito informático.

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, con la finalidad de encontrar evidencias que permitan definir, con toda certeza, los mecanismos que los intrusos utilizaron para acceder a ella.

A través de diferentes aplicaciones en cómputo, se puede determinar cómo fue violentado un sistema, la manera en que fue traspasada su seguridad, y una vez que los intrusos estuvieron dentro, determinar con técnicas sumamente sofisticadas, qué fue lo que hicieron y cuáles fueron los archivos que borraron, así como las modificaciones que realizaron, mientras se precisa la duración del ataque, desde la entrada hasta la salida.

Orígenes

Usar tecnología informática en la investigación de un delito usando una computadora u otras herramientas digitales, ha desarrollado una nueva ciencia llamada informática forense, tiene sus inicios en el FBI[5] cuando fundan el CART (Computer Analisys and Responce Team) en el año de 1984 y es quien se encarga de examinar todas las computadoras que requeriría el FBI. Para hacer sus investigaciones la informática forense tiene como objetivo identificar, preservar, analizar y presentar toda evidencia digital de manera que sirva para seguir un proceso judicial.[6]
Es precisamente Estados Unidos quien empieza a detectar los primeros delitos informáticos, ya que es en este país donde las computadoras tienen un mayor auge, es por ello que se ven en la necesidad de invertir en investigación que los ayude a frenar estas actividades delictivas.

El 22 de Noviembre de 1988 Robert T. Morris, un estudiante de la Universidad de Cornell (Ithaca, NY), protagonizó el primer gran incidente de seguridad (uno de sus programas se convirtió en el famoso worm o gusano de Internet) quedando miles de ordenadores conectados a la Internet inutilizados durante varios días (se calcula que un 10% de los ordenadores de los Estados Unidos quedaron bloqueados simultáneamente), y sufriendo pérdidas estimadas en varios millones de dólares, muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general.
Mientras que por un lado Internet crecía exponencialmente con la adhesión de redes importantes, tales como BITNET[7] o HEPNET[8], y por otro se producía un incremento en las

5 F.B.I. 'Federal Bureau of Investigation ' (en español Oficina Federal de Investigación) es el principal brazo de investigación del Departamento de Justicia (DOJ) de los Estados Unidos de América.
6 http://www.fbi.gob/hq/lab/fsc/backissu/oct2000/computer.htm#Examining%20Computer%20Evidence
7 BITNET: Antigua red internacional de computadoras de centros docentes y de investigación que ofrecía servicios interactivos de correo electrónico y de transferencia de ficheros utilizando un protocolo de almacenaje y envío basado en los protocolos Network Job Entry de IBM. Se conectaba a Internet a través de una pasarela de correo electrónico.

ventas de ordenadores personales (gracias al abaratamiento de la informática de consumo), se iba aumentando de manera espectacular el número de ataques en la red. Esta pasividad inicial, provocada, posiblemente, por el desconocimiento general que existía hasta ese momento de los problemas ocasionados por los ataques de los denominados popularmente como "piratas informáticos" (este término engloba a un amplio conjunto de vocablos anglosajones que definen distintas modalidades de ataque: hackers, crackers, lammers[9]...), dio paso a una preocupación generalizada por el tema de la seguridad en sistemas operativos y redes.

Poco tiempo después del incidente provocado por Morris, y ante la aparición de los peligros potenciales que podía entrañar un fallo o un ataque a los equipos informáticos, en la Universidad de Carnegie Mellon se creó el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet.
Esta idea pronto fue recogida por otros grupos y fue aplicada por los responsables de las direcciones IP, organismos oficiales, etc... Sin embargo, a nivel organizativo y de coordinación, cada grupo de seguridad es completamente independiente de los otros, es decir, la autoridad del CERT se puede considerar más moral que efectiva.

EI 1° de octubre del 2001 el departamento de defensa de los Estados Unidos, funda el Cyber Crime Center (DC3), con un equipo sumamente capacitado, está creado para evitar la proliferación de los delitos informáticos que día a día son más en ese país. [10]La misión de esta división es:
1. Procesar la evidencia digital y analizar todos los medios electrónicos.
2. Asegurar los sistemas dañados, evitando el acceso a ellos de gente no autorizada.
3. Hacer investigación y pruebas de los sistemas para evitar cualquier intervención en el futuro.

El 6 de enero del 2005 se inauguro el Silicon Valley Regional Computer Laboratory (SVRCFL) en San Francisco California EU, es una iniciativa nacional del FBI buscando crear laboratorios muy bien equipados para el análisis de evidencia digital, estos centros de

[8] HEPNET (*High Energy Physics NETwork*). Uno de los grupos pioneros en la construcción de redes paneuropeas en la década de los 80,
[9] Lamer: En terminología hacker, aquella persona que sabe poco sobre computación. También llamados así aquel que pretende ser hacker sin tener todos los conocimientos suficientes.
[10] http://www.dcfl.gov/dc3.htm

investigación en informática forense, auxiliarán en la investigación a las autoridades federales, estatales y locales, en la investigación y resolución de delitos en los cuales es necesario utilizar la tecnología informática.[11]

Aún cuando las computadoras hicieran su aparición muchos años antes, es hasta principios de los años 80s que en Estados Unidos se comienzan a detectar los primeros incidentes relacionados con las computadoras o sistemas automatizados.

Objetivos que persigue el cómputo forense

Se enfoca en el análisis de los sistemas que han recibido algún tipo de daño, la reparación de los daños causados por criminales o intrusos, persecución y procesamiento judicial de los criminales, creación y aplicación de medidas preventivas para casos similares. Estos objetivos se cumplen básicamente por el proceso de recolectar y analizar evidencia digital. En forma más general la informática forense estudia datos que pueden ser extraídos desde un disco duro u otra unidad de almacenamiento de computadoras. Es como un arqueólogo cuando excava un sitio en busca de datos históricos, los investigadores forenses extraen información desde una computadora o componentes de la misma. La información recuperada en muchas ocasiones se encuentra en algún disco, pero eso no quiere decir que sea fácil encontrarla y descifrarla, se tienen que revisar muchos registros de la computadora y determinar si fue un ataque remoto.

Delitos relacionados con las computadoras

Existen diferentes tipos de delitos, informáticos, a continuación se describen estos tipos de delitos reconocidos por naciones unidas.

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos de entrada

[11] http://sanfrancisco.fbi.gov/pressrel/2005/svrcfl010505.htn

Este fraude informático, es el principal delito cometido en el mundo de la informática, ya que es fácil de llevar acabo y difícil de ser descubierto. Para cometer este tipo de delito no es necesario tener conocimientos técnicos de computadoras y los puede llevar acabo cualquier persona que tenga privilegios de usuario dentro del equipo en el que se perpetra el daño.

Manipulación de programas

Este tipo de delito es más difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener buenos conocimientos técnicos de computadoras. Este delito consiste en alterar los programas residentes en la computadora o en insertar nuevos programas o nuevas rutinas al sistema. Un método muy utilizado por las personas que tienen conocimientos especializados en programación es el denominado Caballo de Troya, que consiste en insertar instrucciones al sistema operativo de la computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida

Se lleva acabo ubicando un objetivo al funcionamiento del sistema de la computadora. El ejemplo más común es el fraude que se hace en los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de cómputo especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito, lo que en la actualidad se conoce como clonación. Se aprovechan las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

- Como objeto

- Cuando se alteran datos de los documentos almacenados en forma digital.

- Como instrumento

Las computadoras se usan también para efectuar falsificaciones de documentos de uso comercial o Legal. Cuando empezó a disponerse de impresoras en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones a programas o datos computarizados.

Hace referencia al daño o modificación de información sin autorización, represente un punto muy recurrente.

Sabotaje Informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

- Virus: Es un programa que pueden adherirse a los programas legítimos dentro de una computadora y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de un dispositivo legítimo de soporte que ha quedado infectada, así como utilizando el método del Caballo de Troya.
- Gusanos: Se fabrica de forma similar al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- Bomba lógica o cronológica: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento predeterminado. Al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que

exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba

- Acceso no autorizado a servicios y sistemas informáticos. Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

- Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones como la Internet, recurriendo a uno de los diversos medios. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del Sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos con protección legal:

Este tipo de delito genera una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera legalmente, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.[12]

[12] http://lac.derechos.apc.org/cdocs.shtml?x=8325

Clasificación de los delitos informáticos

Los delitos informáticos se pueden dividir en dos vertientes como instrumento o medio y como fin u objeto. A continuación se dan algunos ejemplos de delitos en los que las computadoras se usan como medio

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Aprovechamiento indebido o violación de un código buscando penetrar a un sistema para darle instrucciones inapropiadas.
- Desviación de cantidades de dinero hacia una cuenta bancaria apócrifa.
- Daño en el funcionamiento de los sistemas, a través de los virus informáticos.
- Acceso en áreas informáticas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objeto, en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios, programas o personas morales, y las que son:

- Destrucción o daño de programas por cualquier método.
- Daño a la memoria de computadoras.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Robo de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).[13]

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones en contra de los propios sistemas como son:

- Acceso no autorizado: Uso ilegitimo de password y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

[13] Téllez Valdes, Julio. Derecho Informático Mc Gaw Hill pp. 103-104.

- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

La Internet permite llevar acabo otro tipo de delitos informáticos como son:

- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Características principales de los delitos informáticos

- Son conductas criminales de cuello blanco (white collar crime)[14] en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

[14] White collar crime son los delitos cometidos por gente con altos estatus socioeconómicos y con preparación técnica o profesional de alguna ciencia.

- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar más y más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.[15]

1.3. PERFIL DEL INFORMÁTICO FORENSE.

Analizando la información disponible en Internet, revistas y libros referentes al tema, se puede decir que la base del informático forense se fundamenta en la aplicación de conocimientos técnicos y procedimientos legales, en las situaciones donde los sistemas han sido vulnerados, usando los datos recopilados para generar una hipótesis de los hechos, y sustentándolo con la evidencia recolectada. El llegar a desarrollar una investigación en informática forense exige del investigador características y conocimientos que se describen a continuación.

[15] Téllez Valdes, Julio. Derecho Informático Mc Gaw Hill p. 163.

Características del informático forense

En base a las necesidades y exigencias que presentan hoy día los sistemas informáticos se puede decir que un investigador en informática forense debe de poseer las siguientes características[16]

- Poseer la habilidad de ser un excelente observador: poder ver aquellos detalles que normalmente son imperceptibles para la mayoría.
- Buena memoria: ordenar perfectamente las pistas que se van recolectando en el transcurso de la investigación, debe tener la capacidad de recordar sucesos, nombres, lugares y fechas.
- Documentar bien la información: Es muy complicado que un investigador guarde toda la información de la investigación en la cabeza, así que debe de ser muy preciso al documentar la información.
- Objetividad: no debe generar prejuicios, ni inmiscuir sentimientos, que afectan su capacidad de realizar una evaluación objetiva.
- Conocimientos: un buen investigador debe poseer conocimientos legales, reglas de evidencia, psicología criminal, conceptos y procedimientos de investigaciones, y conocimientos científicos.
- Habilidad de pensar como un criminal: poseer la habilidad de pensar como el criminal, le da al investigador la facultad de realizar procesos mentales, hipótesis y predecir las actividades del delincuente.
- Imaginación constructiva: el investigador debe de ser muy creativo para considerar todas las posibilidades y sacar conclusiones.
- Curiosidad: no quedar satisfecho con simplemente aclarar el caso. No es suficiente con saber quien cometió el delito, es necesario saber porque y exactamente como lo llevo acabo.
- Energía: el investigador debe trabajar duro, probablemente se vea envuelto en horas y horas de investigación. Un buen investigador debe estar preparado físicamente para los retos que se le presenten.
- Paciente: el proceso de las investigaciones es frecuentemente muy lento, es ir paso a paso, y muy probablemente sea necesario comenzar la investigación una y otra vez.
- Pasión por el aprendizaje: siempre estar abierto a obtener conocimientos de Otros campos en los que no se posean conocimientos.

[16] Debra Littlejohn, Scene of the Cybecrime, Syngress 2002,pp 136-139.

Adicionalmente de estas características generales, un informático forense necesita las siguientes características.

- Conocimientos en computación: los investigadores deben tener conocimientos sobre el funcionamiento de las computadoras, incluyendo tanto el software como el hardware.

Conocimientos en protocolos de redes de computadoras: en algunas ocasiones los delitos informáticos se llevan acabo mediante redes de computadoras, es por ello que los investigadores en informática forense necesitan conocimientos del proceso que llevan a cabo los sistemas al enviar un correo o al hacer la petición de una página Web, como se descargan las cosas desde la red, etc.

- Conocimiento de terminologías técnicas: es necesario saber los términos técnicos para facilitar la comunicación con los administradores de los sistemas a investigar.
- Conocer la cultura hacker: sólo un hacker puede atrapar a otro hacker, es necesario saber las técnicas usadas por los mismos para acceder y dañar sistemas, conocer su forma de pensar y analizar la forma de frenarlos.
- Conocimientos sobre seguridad informática: conocer acerca de las tecnologías que hay para proteger los sistemas, como lo es el firewall[17], conocer las debilidades de éstos mismos.

1.4. CÓMPUTO ANTI-FORENSE

La mente de los “inquietos” generalmente se mueve más allá de lo que de acuerdo con el manual, el software o hardware puede hacer. Estos personajes utilizan lentes divergentes, creativos y desafiantes para poner a prueba, la perspectiva (generalmente) convergente y focalizada de los encargados de la seguridad.

Se dice en la industria que estos “inquietos” tienen mucho tiempo y ellos no. Que estas mentes creativas son unos “desocupados”, que no procuran soluciones o alternativas para la seguridad, sino daños y problemas que los desgastan y los atrasan. Bien, este reclamo

[17] Firewall: (Muro de Fuego - Cortafuego). Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

(algunas veces justificado y otras no) es una alerta y llamado al orden para la función de seguridad de la información. Un llamado que les recuerda a cada uno de los protagonistas que deben reconocer que su sistema de gestión tiene una propiedad inherente que se llama inseguridad, esa que no se puede eliminar, sino descubrir y entender.

Lograr esto lleva tiempo y exige cambiar las rutinas del día a día de la gestión de seguridad, para ver lo que los inquietos ven. En este sentido, se requiere de los responsables de la seguridad establecer un sistema que permita administrar la variedad y conocer la complejidad propia de la dinámica de la seguridad de cada organización.

Toda esta presentación para evidenciar que tarde o temprano las organizaciones serán objeto de fallas o incidentes de seguridad, que de acuerdo con las políticas de la empresa, llevará a investigaciones y análisis para determinar y reconstruir los hechos, así como identificar los posibles responsables. En este sentido, la computación forense o informática forense existe, pues la inseguridad materializada existe: eliminación de información, alteraciones de datos, inadecuadas prácticas de disposición de medios, personal descontento, entre otras. La computación forense permite a las organizaciones adelantar las revisiones requeridas en medios tecnológicos para valorar lo que sucedió, y de manera científica, explicar lo que pudo ocurrir, siempre basado en hechos y evidencia verificable.

Sin embargo, aquellos que cruzan los límites de los derechos de los otros y atentan contra el orden establecido de la sociedad, quieren evadir los justos reclamos y sanciones que deben tener por sus actos. En este sentido, utilizando las habilidades de los inquietos, buscan la manera de distorsionar la realidad para “conducir la investigación” hacia donde ellos quieren y no hacia la verdad de lo ocurrido.

Este tipo de tendencia, profundiza en el cómo funcionan las herramientas forenses, sus alcances y limitaciones, y sobre ellas, detallar alternativas que procuren fallas y dudas sobre su adecuado funcionamiento y uso. En este contexto, los investigadores forenses en informática entran en desventaja, pues cualquier hallazgo que se obtenga con las herramientas será objeto de duda, la cual generalmente, se resuelve a favor del acusado.

La computación anti-forense surge como un reto positivo para la seguridad de la información y sus desarrollos futuros. ¿Por qué? los estudios y pruebas de concepto que adelantan las mentes inquietas, producen nuevas distinciones y propuestas que permiten a la industria continuar afinando sus desarrollos y no solamente fortalecer los actualmente disponibles. La madurez de una herramienta forense, podrí decirse, se mide en las constantes dudas y fallas que tiene que resolver para confrontar las observaciones de las mentes inquietas. Un producto que de manera sistemática es exigido y evaluado para conocer sus limitaciones. No se puede negar que la computación anti-forense establece un desafiante “lado oscuro” que debe invitar a “ver con otros ojos” lo que la realidad dice. Un

"lado oscuro" que canalizado y orientado para mejorar, es un aliado estratégico fundamental para repensar la seguridad de la información, pero mal utilizado, es una amenaza permanente que exige desaprender y mantenerse en crisis permanentemente para tratar de inferir los movimientos de los intrusos. Hablar de computación anti-forense es pensar en proyectos como *Metasploit Project* (http://www.metasploit.com/), la revista Phrack (http://www.phrack.org), la revista insecurity magazine http://www.insecuremag.com) y tantos otros esfuerzos internacionales, que tienen como objetivo establecer un referente real y preciso sobre la seguridad de la información: somos tan seguros, con el eslabón más débil de la cadena.
Dicho de otra manera, mientras más se conoce la inseguridad, más se entiende que tan seguro podría llegar a ser. [18]

1.5. SITUACIÓN JURÍDICA A NIVEL MUNDIAL

La problemática que han generado las tecnologías de la información no son exclusivas de uno o dos países, existen muchos países que se han visto afectados por este tipo de problemáticas y algunos de los cuales han empezado a tomar medidas desde hace ya algún tiempo. Tratando de mitigar o por lo menos controlar este problema que aqueja principalmente a los países más tecnificados. Cada uno de ellos ha desarrollado mecanismos legales que castigan a los responsables de los delitos informáticos, todo esto evidentemente con la finalidad de hacer disminuir estos.

Alemania:

Respecto a este país tenemos que destacar el hecho de que las medidas legales que se crearon, fueron producto de una necesidad creciente de prevenir efectos futuros, relacionados con delitos informáticos. El documento en si marca inicialmente un argumento legal, así como su sustento científico.

[18] CANO, J. (2004) Inseguridad Informática. Un concepto dual en seguridad informática. http://www.virusprot.com/art47.html

Desde 1986 existe la Ley contra la Criminalidad Económica, que contempla los siguientes delitos: espionaje de datos, fraude informático, alteración de datos, y sabotaje informático.

Concepto y Modalidades de la Criminalidad Mediante Computadoras

A) Concepto. Con la expresión "criminalidad mediante computadoras" se alude a todos los comportamientos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso punibles en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos. Dicho concepto, pues, abarca, por una parte, el problema de la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos mediante computadoras; de hecho, sin embargo, hasta el momento en Alemania Federal solo se han conocido pocos casos de violación de derechos personalismos en razón del aprovechamiento abusivo de datos conservados en una computadora. De cualquier forma, el legislador alemán, en la "Ley Federal de Protección de Datos", reforzó la regulación con normas penales poco precisas. Y, por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el uso abusivo de datos procesados automáticamente; las consideraciones siguientes se circunscriben a este segundo ámbito.

B) Modalidades. En Alemania Federal el punto de partida de la discusión acerca de la criminalidad mediante computadoras, consistió en determinar si efectivamente existía dicha forma de delincuencia. Gracias a las investigaciones efectuadas desde hace diez años por el Instituto de Criminología y Derecho Penal Económico de la Universidad de Friburgo, actualmente se puede ofrecer una recopilación bastante completa de asuntos penales tanto de la República Federal de Alemania como del ámbito europeo, para acreditar la existencia de tal criminología.[19]

Austria:

Ley de Reforma del Código Penal, promulgada el 22 de diciembre de 1987, contempla los siguientes delitos:

1.- Destrucción de Datos (126). En este artículo se regulan no sólo los datos personales sino los no personales y los programas.

2.- Estafa Informática. (148). En este artículo se sanciona a aquellos que con dolo causen un

[19] http://www.unifr.ch/ddp1/derechopenal/articulos/pdf/Tiedemann2.pdf

perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.[20]

Chile:

Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio "Artículo 3° ".

El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

España:

El Nuevo Código Penal de España, establece en su artículo 264-2, que se aplicará la pena de prisión de uno a tres años de prisión y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
En cuanto a estafas electrónicas, en su artículo 248 sólo tipifica aquellas que tienen ánimo de lucro por medio de manipulación informática. Sin detallar las penas en el caso de que el delito se lleve a cabo.

[20] http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm

Estados Unidos:

Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos; específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo.

Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.

Francia:

Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente: Artículo 41" El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2 000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".

Artículo 42 " El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20 000 a 2 000 000 francos, o con una de estas dos penas.

Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos en las condiciones que determine, y a expensas del condenado.

Artículo 43. "El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2 000 a 20 000 francos, o con una de las dos penas.

El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en le párrafo anterior, será castigado con pena de multa de 2 000 a 20 000 francos. Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos".

Gran Bretaña:

Debido a un caso de hacking en 1991, comenzó a aplicar en este país la Computer Misuse Act (Ley de Abusos Informáticos). Esta ley castiga con hasta 5 años de prisión o multa el intento exitoso o no, de alterar datos informáticos. Esta ley contempla la modificación de datos y los virus informáticos. Liberar un virus tiene una pena desde un mes a cinco años.

Holanda:

En marzo de 1993 comenzó a operar la Ley de Delitos Informáticos, en la que se penaliza el hacking, el phreacking, la ingeniería social (platicar con personas que poseen cierta información valiosa y obtenerla por medio de la conversación), y la distribución de virus.
La penalización de virus esta dividida en dos formas una es en el caso de que el virus se haya liberado por error y la otra si fue liberado con la intención de hacer daño. Si se demuestra que el virus escapo por error, la pena no supera el mes de prisión; pero si se comprueba que fueron liberados para hacer daño, la pena puede alcanzar los 4 años de prisión.

Italia:

En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos:

a) Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

b) Abuso de la calidad de operador de sistemas. Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.

c) Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.

d) Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a

otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

e) Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.

f) Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

g) Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

h) Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

i) Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

j) Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.

Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:

Artículo 35: " Utilización de la Informática. 1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de

datos no identificables para fines estadísticos. 3. Queda prohibida la atribución de un número nacional único a los ciudadanos. [21]

Cada uno de los países antes mencionados, así como muchos más que no se están abordando ponen especial atención en las áreas de oportunidad que más les afecten según sea el caso. Es evidente después de ver la manera en que se aborda cada caso, que los intereses particulares de cada país y su respectiva legislación tratan de dar cada uno a su manera una base que sustente a la figura del "delito informático". Lo cual nos dice que este fenómeno ya esta cobrando mucha fuerza a nivel mundial, debido al avance tecnológico que día con día nos sobrepasa.

1.6. SITUACIÓN LEGAL EN MÉXICO

En México la situación jurídica bajo la cual debería estar sustentada la investigación forense es muy joven aun, aunque en otros países este tema ya esta viéndose como de alto impacto en la vida diaria, esto debido al retraso que México tiene en muchos aspectos incluida la tecnología de la información, lo cual hace que tarde o temprano este tema sea fuente de muchas respuestas a problemas que ya existen, pero que aun no pueden alcanzar su solución por falta de preparación para tales eventos.

LEGISLACIÓN EXISTENTE PARA EL CÓMPUTO FORENSE EN MÉXICO

Respecto a este rubro, tenemos que comprender los distintos problemas que tenemos que enfrentar, debido a la poca atención que se ha prestado hasta hace un tiempo en materia de protección de información, recuperación e investigación de las causas que ocasionan este tipo de anomalías. En México, se puede describir puntos concretos y muy importantes para dar seguimiento a procesos legales, como lo son la investigación y la posibilidad de terminar con la impunidad que implica el complejo proceso de determinación, para el caso particular de lo delitos informáticos.

[21] http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm

- Se han tipificado algunos delitos informáticos en el Código Penal Federal y algunas otras legislaciones relacionadas.
- Es posible castigar intrusiones a sistemas informáticos
- No es claro el mecanismo de presentación de pruebas en un juicio sobre un acceso no autorizado a un sistema.
- Las personas y las organizaciones no saben qué deben hacer para denunciar un delito de este tipo
- Muchas organizaciones no tienen definidas políticas de uso permitido de sus recursos de cómputo
- La policía federal, a través de tratados internacionales, puede investigar más allá de las fronteras

Principales leyes y artículos referentes al cómputo forense.	
Código de Comercio (Colima)	• Uso no autorizado de programas y de datos, LFDA, Ley de Protección de Datos Personales del Estado de Colima [22]
Código de Comercio Ley de Instituciones de Crédito	• Obtención o interferencia de información que viaja por una red, Art. 167 Fracción VI Código Penal Federal
Ley del Mercado de Valores	• Acceso no autorizado a sistemas o servicios y destrucción de programa o datos, Art221 bis1 a 211 bis 7 Código Penal Federal
Código Federal de Procedimientos civiles	• Fraude, Art. 230 -231 Código penal para el D.F.
Código Penal del Estado de Sinaloa	• Capítulo V. Delito Informático. Artículo 217.
Propiedad intelectual	• Ley de Propiedad Industrial • Ley Federal del Derecho de Autor

[22] http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm

Cómputo Forense	• Código de Comercio • Código Federal de Procedimientos Civiles
Código Penal para el Distrito Federal	• Artículo 231 del Código Penal para el D.F.
Iniciativa de Ley Federal de Protección de datos personales	

Figura 1.1 Documentos legales disponibles en México.

1.7. CÓMPUTO FORENSE EN MÉXICO

En México, se han realizado fraudes por cerca de $1.38 millones de pesos en un año por medio de Internet; según estadísticas de la Policía Federal Preventiva, quien cuenta con la Policía Cibernética para poder seguir delitos principalmente de pornografía infantil y asesorar a la ciudadanía en cuestión de fraudes en Internet.

Esta infraestructura tecnológica puede ser desde un teléfono celular, una cámara digital, una computadora, una impresora, una memoria digital o hasta una agenda o asistente personal (PDA[23]). Todos estos elementos hoy en día tienen memoria, dispositivos que poco a poco se convierten en computadoras, ya que por ejemplo en un celular ya se puede tomar fotografías y almacenarlas en el mismo teléfono.

La trascendencia del tema de seguridad en los sistemas de cómputo recae necesariamente, en la importancia de la seguridad informática para cualquier persona, empresa, gobierno o país. En este ciber mundo, la vida cotidiana navega en el espectro virtual que tiene Internet,"el universo sin fronteras", donde los datos se difunden aparentemente sin control, cuestión sumamente delicada para la protección de datos de las instituciones y del propio individuo.

[23] PDA: Personal Digital Assistant

Por la naturaleza misma del ilícito, se puede llegar a pensar que los infractores –como suele suceder en la vida diaria– son gente externa al entorno social, no obstante, hay opiniones que indican lo contrario. "Las estadísticas muestran que el **75% de las intrusiones a sistemas de cómputo provienen de la propia empresa** o corporación.

En muchas ocasiones, en ambientes académicos, las intrusiones provienen de fuera debido principalmente a la administración de los equipos de cómputo, donde al investigador lo que le interesa, es que su equipo y proyecto funcionen de manera apropiada, restándole importancia a la administración y seguridad del equipo.

En ese sentido, la administración es un punto fundamental para evitar las intrusiones, sobre todo si se considera la vulnerabilidad de las mismas aplicaciones que utiliza el sistema, aunado al hecho de que conforme pasa el tiempo se dejan lagunas y puertas abiertas, las cuales son aprovechadas por los intrusos para lograr ingresar al sistema.

UNAM logros en el campo forense

(1994-2000)

- El Área de Seguridad en Cómputo, se encargaba de atender incidentes que reportaban los administradores de sistemas y de redes de la Universidad.
- Virus/gusanos en Windows
- Intrusiones en sistemas Unix.
- Se acudía y revisaba el equipo ingresando y haciendo uso de comandos del sistema (o copiados de otro similar) y de algunos scripts[24] sencillos.
- No había capacitación formal en el área de atención a incidentes y análisis forense
- Los análisis resultaban en hallazgos en el sistema de archivos de material que los intrusos habían dejado visible
- No se tenía una metodología ni se tomaban precauciones necesarias para un forense.
- Era difícil detectar intrusiones "sofisticadas"
- Cosas como los LKM Rootkits[25] (adore, knark) resultaban complejas para analizar

[24] Script: Es un conjunto de instrucciones. Permiten la automatización de tareas creando pequeñas utilidades.
[25] Cambian el contenido de la tabla de interrupciones, redireccionan, syscalls y en general cualquier cosa que se pueda ocurrir. No tiene límite de privilegios.

- Empezaba un auge global del análisis forense y se tenían las limitaciones propias de un área en surgimiento y evolución constante

2001

En 2001, se registra oficialmente UNAM-CERT ante FIRST

Los incidentes que se atienden son cada vez más importantes
Primeras experiencias con la iniciativa privada
Se observa la necesidad de capacitarse en materia de análisis forense
Se atiende una mayor cantidad de incidentes
Atención de algunos casos en secretarías de Estado (ministerios)

2002-2005

Incidentes con implicaciones más importantes dentro de la Universidad
Colaboración con entidades gubernamentales encargadas de la investigación de delitos informáticos.
Se participa ahora de monitoreos mundiales sobre actividad maliciosa
Se trabaja de manera coordinada con instituciones financieras afectadas por problemas de fraudes
Las distintas policías tienen ahora entidades dedicadas a la atención de delitos informáticos con las que UNAM-CERT ha colaborado en análisis forense
Las empresas más grandes han empezado a destinar más recursos a la atención a incidentes de seguridad informática
Algunas procuradurías estatales cuentan con peritos en seguridad informática que realizan investigaciones forenses
Muchos administradores de sistemas aún no tienen claro para qué sirve el análisis forense
En algunos casos sigue siendo difícil la respuesta al incidente
Se ha tenido que clasificar los incidentes y definir adecuadamente los recursos para la atención y análisis de los casos

EXPERIENCIAS OBTENIDAS DENTRO DE LA UNAM

En base a los logros que la UNAM ha obtenido en el aprendizaje del cómputo forense, he logrado aplicar dentro de la misma institución esas técnicas para solucionar problemas de seguridad y así dar un uso real a ese conocimiento, entre los principales casos que se atienden son:

- Casos frecuentes en la UNAM
- Abuso de recursos para afectar a otras redes
- Envío de correo spam[26]
- Sospechas de personas que acceden a archivos personales a los que no tienen permiso

Experiencias con entidades de Gobierno

Dentro de las experiencias de las que se tienes conocimiento una de ellas es aquella obtenida de la secretaria de estado donde se encontró un Solares "cackeado". Las conclusiones a las que se llegó después de la investigación son:

- El sistema no había sido craqueado.
- Se había perdido información
- Intento de ocultar omisiones de administración pretextando una intrusión

Con la iniciativa privada

Respecto a la iniciativa privada, es una situación delicada, ya que por lo regular estas no son tan abiertas a recibir ayuda, debido a el temor de que información sea al utilizada optan por emprender soluciones internas, debido a que todo este tipo de situaciones afectan su imagen y procuran siempre manejarlo los mas anónimamente posible..

En una empresa privada

- Se sospecha de accesos no autorizados
- Se acude a atender el incidente

[26] Se llama SPAM al correo basura, a los mensajes no solicitados habitualmente de tipo publicitarios enviados en cantidades masivas que perjudican de una u otra manera al receptor.

- Se realizan las primeras investigaciones
- La investigación es truncada por parte de la empresa
- La empresa va a arreglar internamente el asunto[27]

Instituciones Gubernamentales en México

En nuestro país actualmente existe una policía especializada para este tipo de delitos, la Policía Federa Preventiva instaló formalmente desde diciembre del 2002 un grupo de coordinación interinstitucional de combate a delitos cibernéticos, desarrollando en México la primera unidad de policía cibernética, que además de las acciones preventivas hacia los delitos cometidos en Internet y otros en los cuales se aplicaron medios informáticos, cuenta con un área especifica en materia de prevención y atención de denuncia de delitos, en sus inicios se componía por aproximadamente 75 expertos en diferentes áreas pero principalmente por especialistas en sistemas informáticos, criminalistas, psicólogos y sociólogos.

La misión de esta policía cibernética es identificar y desarticular organizaciones dedicadas al robo, tráfico y corrupción de menores, así como prevenir la elaboración, distribución y promoción de pornografía infantil en la Internet.

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el resto del mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de cómputo, el hacking, la venta de armas y drogas por Internet y el ciber terrorismo las cuales son amenazas para la sociedad. Se han detectado y desactivado en México 321 comunidades o sitios en Internet que promueven la pornografía infantil y más de 200 son mexicanas.

Se detectaron sitios relacionados con el robo o alteración de información, 163 de fraudes, dos de donación de señal satelital, dos de tarjetas de crédito y siete de ciber terrorismo.

[27] http://www.seguridad.unam.mx

"La misión de la policía cibernética de la PFP[28] es localizar y poner a disposición de las autoridades ministeriales personas dedicadas a cometer delitos informáticos. Es preciso señalar que la informática forense sigue todo el proceso judicial, no sólo entrega pruebas o evidencia digital, sino que va de la mano con todo el proceso judicial, así que el investigador informático debe de tener en cuenta la legislación informática que aplique en su país o localidad y apegarse a ellas. Otra de las actividades que lleva acabo esta policía, es realizar operaciones de patrullaje anti-hacker, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red. Análisis y desarrollo de investigaciones sobre las actividades de organizaciones locales e internacionales de pederastas, así como de redes de prostitución infantil.

La PGR[29] cuenta con un servicio de informática forense, en 1999 se crea el Departamento de Informática Forense, que depende de la Dirección General de Coordinación de Servicios Periciales de la Procuraduría General de la República, como un área auxiliar del departamento de Propiedad Intelectual y en el 2001 se convirtió en un departamento completamente independiente.

El objetivo de este cuerpo forense es, proporcionar los fundamentos técnicos que sirvan como soporte en la investigación de posibles hechos delictivos concernientes a la modificación, destrucción, reproducción o pérdida no autorizada de la información contenida en dispositivos electrónicos, así como el uso de la información presentada en Internet. La intervención del cuerpo forense de la PGR se enfoca a aquellos casos en los que se utiliza el equipo de cómputo como medio para llevar acabo una conducta presuntamente delictiva, así como cuándo el equipo es violentado en sus partes lógicas (programas) o en sus partes físicas[30].

El 29 de Octubre de 2003 se llevó a cabo un congreso anual llamado "Senior Law Enforcement Plenary" (SLEP) en la ciudad de México fue un encuentro bilateral entre México y Estados Unidos, uno de los puntos que tocaron fue, crímenes informáticos e intelectuales en el cual acordaron proveer a México el entrenamiento y capacitación al personal de la PGR por medio de agencias de inteligencia Estadounidense.

Existe en México también una empresa dedicada a hacer informática forense, llamada Laboratorio de Informática Forense GC (LIF-GC) es un equipo especializado en investigación e inteligencia en sistemas de cómputo y de evidencia digital. LIF ofrece servicios de análisis, investigación y prevención de conductas delictivas o irregulares en

[28] PFP- Policía Federal Preventiva
[29] PGR- procuraduría General de la Republica
[30] http://www.pgr.gob.mx/

medios cibernéticos. Para tal efecto, LIF-GC cuenta con la tecnología más avanzada para la aplicación de la metodología de la Informática Forense, así como el respaldo de especialistas en México y en el extranjero. [31]

1.8. ESPECTATIVAS A FUTURO

En un futuro a muy corto plazo, tenemos que este tema estará cada día más presente en nuestra vida diaria, así como lo es desde hace años tan solo como resultado de la inercia que se produce y que día a día crece debido al incremento en la digitalización e nuestras actividades Figura 1.1. A largo plazo se tendrá que pensar en infraestructura y servicios de apoyo que den solución real a grueso de población que requiera ser guiado en la solución de un problema en que se impliquen técnicas de cómputo forense. Dentro de estas necesidades se estima que sean las siguientes actividades las que requieran mayor atención y por tanto mejor solución:

- Los casos más frecuentes estarán relacionados con fraudes y bonets[32].
- Cada vez encontraremos con mayor frecuencia casos de fuga de información, sobre todo en instituciones gubernamentales y empresas privadas
- Tendrá que actualizarse la legislación vigente pues la actual es insuficiente.
- Cada vez habrá más casos de análisis forense, en la universidad y en los sectores público y privado.
- Se requiere capacitación para los administradores en cuanto a la atención a incidentes
- Se necesitan mecanismos de colaboración para tener retroalimentación y capacitación sobre cómputo forense

[31] http://ventana.presidencia.gob.mx/.
[32] Las bonets es una colección de PC-robots que funcionan de manera autónoma y automática, y el creador de la bonet suele utilizarlo para el fraude en línea, envío de Spam, robo de contraseñas e incluso para almacenar datos.

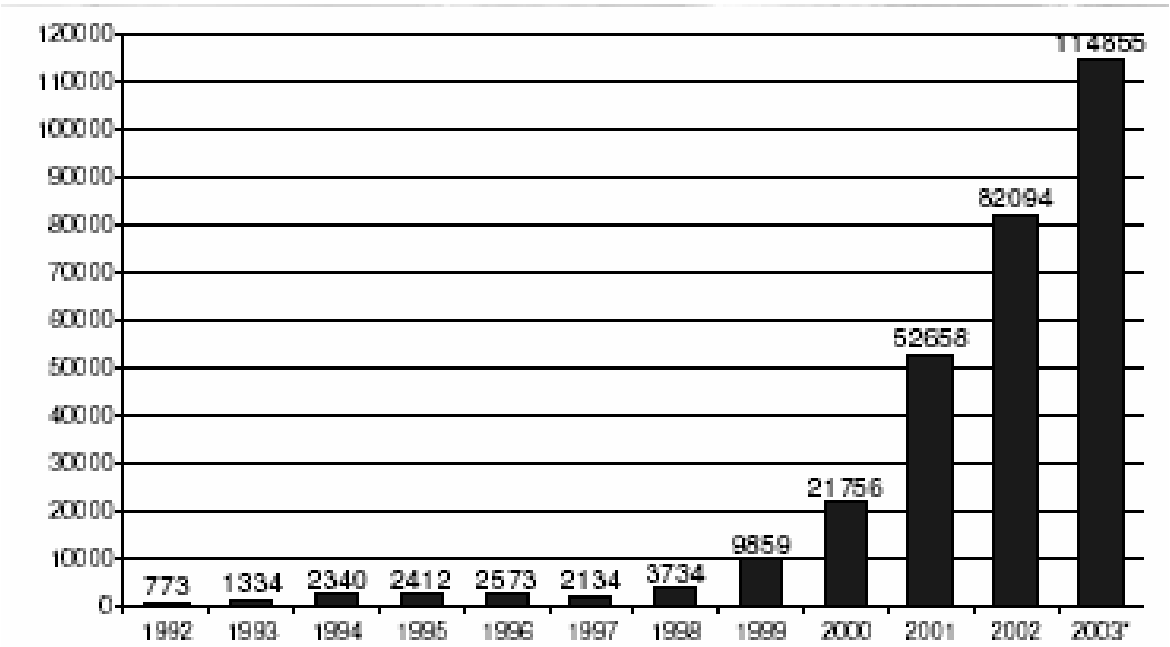

Figura 1.1 Incidentes reportados por CERT

Factores de influyen en las estadísticas.

Incidentes de seguridad

- No todos son registrados o se da aviso
- Por imagen corporativa, perdida de credibilidad

Lo más común:

- Robo de información ($ 170,827,000 usd)
- Fraudes ($ 115,753,000 usd)

Como lo evidencia la grafica anterior, se puede ver que el flujo de incidentes reportados, crece en una forma exponencial. Esto es una muy buena ejemplificación de que en seguridad informática, se tiene un campo muy amplio de acción, debido a que esta área es la responsable de prevenir, mantener y reparar todos aquellos daños que pueden perjudicar a una empresa o institución. Aunado a esto, se ve que es un camino aún largo, pero lejos de sentirse expuestos a merced de actores maliciosos y creer que no es suficiente, también se debe tomar en cuenta que esta rama valiosísima de la tecnología y particularmente de la

computación tiene un desarrollo en el que la aventajan los avances tecnológicos. Como se ha visto este tipo de técnicas fueron pensadas y requeridas tiempo después de la creación de las computadoras, por lo tanto hay un diferencial de tiempo, lo cual hace que estas graficas se disparen de esa manera. Aún queda mucho, por hacer, pero se esta en camino.

En México, se tiene un área de oportunidad muy buena en todos los aspectos, pero también es cierto que se tienen cosas a nuestro favor, la mayoría de las tecnologías que se adquieren en el país ya están muy documentadas fuera y esto permite no estar tan indefensos ante estas situaciones, por otro lado, la situación obliga a ser cada vez más competentes para cerrar la brecha de atraso con que contamos. En México hay grandes talentos en esta área crucial hoy día y se debe hacer todo lo posible porque sea un área prioritaria. Tenemos el talento y la inquietud, solo es necesario un mayor enfoque de recursos humanos y económicos.

II. TÉCNICAS Y HERRAMIENTAS DEL CÓMPUTO FORENSE

INTRODUCCIÓN

A diferencia con la disciplina forense tradicional, se tiene también una escena del crimen, la cual puede ser una computadora o un archivo. Una de las características principales de la investigación de infraestructura tecnológica es la fragilidad de la evidencia. Por ejemplo, al abrir un archivo de texto, con el simple hecho de darle doble clic al archivo, se modifica la última fecha de acceso al mismo, por lo tanto, ¿cómo poder mantener la evidencia sin ningún cambio?

Esta es una de las partes más difíciles dentro de la investigación, ya que con un simple cambio a la evidencia digital, ésta puede ser descartada por el mal manejo que haya tenido el investigador.

Si se sigue con la analogía con un caso normal, el arma dentro de una computadora puede llegar a ser una acción, o un flujo de datos que al llegar a la computadora desaparece y no es posible saber de ella. Por lo mismo, son muchos elementos los que hay que tomar en cuenta para poder hacer la investigación.

2.1 ALGUNAS CONSIDERACIONES

“Las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los culpables de una intrusión, y saber a ciencia cierta qué le hicieron al 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”.

En todo ese tiempo, se han aprendido muchas técnicas de intrusión que utilizan los crackers y hackers para extraer información a los sistemas de cómputo, y también se ha logrado con ello estudiar sus movimientos y aprender a diseñar nuevos métodos de seguridad.

Aunado a esto, el desarrollo de los exploits (vulnerabilidades) le permite al informático forense saber qué tipo de programas se pondrán de moda dentro de los próximos cinco meses, aproximadamente, generando con ello una base de estudio para ver y observar patrones de comportamiento.

2.2 TÉCNICAS

Así como se ha diversificado con el paso del tiempo la cantidad de formas de acceder a un equipo de manera no autorizada, también las distintas técnicas y estrategias que lo investigan han tenido una gran evolución. Tenemos que considerar que para cada situación hay que tomar medidas distintas, las que nos lleven a la mejor solución de la situación.

Pasos en que se divide el cómputo forense

Pese a que existen aún divergencias respecto a la metodología, la más generalizada y en la que la mayoría concuerdan es la siguiente.

Cómputo forense se divide en cuatro pasos principales: Identificación, Preservación, Análisis y Presentación.

- **Identificación**

En este paso, es necesario poder identificar lo que se tiene que investigar, desde computadoras, CDROM's, memorias, e incluso papeles que pudieran estar cerca de la computadora. Muchas veces en esos papeles se puede encontrar información que puede llegar a servir para poder completar ciertos procesos de investigación.

En algunos casos, no es necesario ir hasta la escena del crimen, dado a que la misma escena es únicamente la computadora, por lo cual es necesario obtener la computadora.

Si la computadora fue asignada a una persona diferente una vez que se cometió el delito y la otra persona hace uso de la computadora por un período de tiempo, no es posible regresar o poder hacer la comprobación de que la información contenida en esa máquina fue de esa persona.

Es por ello que es muy importante que una vez que se detecta el fraude o el posible delito, aislar la máquina para que el investigador la pueda obtener sin ninguna alteración.

- **Preservación**

Es uno de los pasos clave dentro de la investigación. Como se comentó anteriormente, es necesario mantener la integridad de la evidencia digital, y para ello se usan varios mecanismos que van desde generar un "clon" del disco, llamado "Imagen Forense" para poder trabajar sobre él y no sobre la evidencia original. Pero aún así, hay una pregunta clave: ¿cómo se puede asegurar que lo que se recolectó como evidencia digital es exactamente igual a lo que se analiza y a lo que se entrega al finalizar el proceso?

Por medio de una función matemática, se puede generar algo muy parecido a una huella digital de un disco duro. Si un bit[33] es alterado, entonces la huella digital del disco duro cambiará.

METODOLOGÍA PARA LLEVAR A CABO LA PRESERVACIÓN Y MUESTREO DE PRUEBAS

En este apartado se ven las reglas y pasos que se deben seguir en la obtención de información, así como del muestreo que posteriormente será objeto de análisis en una presunta investigación forense.

- Limitar el acceso al área donde se encuentra el equipo que evidentemente fue dañado. Evitar que gente ajena a la investigación tenga acceso a los equipos en donde hay mucha probabilidad de encontrar evidencia del delito, ya que hay que asegurar que no será ningún dato contenido dentro de los equipos, pues al ser manipulados los equipos por otra persona pueden alterar los registros que más adelante servirán para determinar como se llevo acabo el delito.

- Hacer un estudio preliminar sobre el tipo de caso que se va a investigar. Para evaluar el tipo de caso que se va a manejar se debe platicar con otras personas involucradas en el caso y hacerles preguntas relacionadas con el incidente. Preguntas tales como, ¿cuál es el equipo involucrado, computadoras, discos y Otros dispositivos?, su localización y ¿cómo acceder a este equipo?, investigar que personal tiene acceso al mismo y cuál es la función del equipo dañado.

- Hacer un enfoque preliminar sobre el caso a estudiar. Determinar los pasos generales que se necesitan seguir para investigar el caso. Si el sospechoso es un empleado, es necesario incautar su computadora, averiguar cuando se puede tomar posesión de ella, durante horas de trabajo o si hay que esperar después de las horas de oficina o hasta el fin de semana. Esto es porque aún es sospechoso y no se ha encontrado prueba de que él sea responsable, además se debe procurar en todo momento no interrumpir los tiempos de producción de la empresa que ha solicitado la investigación.

- Crear un diseño detallado. Refinar las líneas generales de la investigación, creando una lista detallada, de los pasos que se necesitan seguir y el tiempo estimado que será necesario para cada uno de ellos. Esto sirve para saber en que punto se encuentra la investigación, durante el proceso de la misma, además de manejar adecuadamente los tiempos.

[33] Se define como la mínima expresión de almacenamiento en medios magnéticos.

- Identificar la evidencia digital: Este es el primer paso en todo el proceso forense. Hay que saber qué evidencia se tiene, dónde y cómo se guarda. Es muy importante determinar los procesos que se llevarán a cabo para la recuperación de la evidencia. Aunque existe la idea de que sólo las computadoras personales son estudiadas por la informática forense, la realidad es que el concepto se puede extender a todo dispositivo electrónico que tenga la capacidad de almacenar información, como son las agendas electrónicas, las tarjetas inteligentes, los teléfonos celulares, entre muchos otros.[34] La tarea de aquel que examina la información almacenada en algún dispositivo es identificarla, y hacer un análisis en busca de pruebas, que determinen el problema y el responsable, así como conocer el formato en que se guarda la evidencia digital para poder extraerla con la tecnología apropiada.

- Obtener y copiar los discos donde se encuentra la posible evidencia. En algunos casos será necesario hacer más de una copia de los dispositivos de almacenamiento donde se encuentra la evidencia y no sólo en discos duros, hay otros formatos que es necesario tomar en cuenta como discos Zip[35], Jaz[36], Discos Compactos y otras unidades de almacenamiento removible.

- Preservación de la evidencia digital: Este es un punto en el que se debe tener especial atención para el proceso forense, ya que los datos deben ser examinados con mucha cautela en un juzgado por personal capacitado. Es muy importante que cualquier análisis en el proceso de la búsqueda de evidencia se haga evitando la alteración de los datos originalmente almacenados en el dispositivo en cuestión. Posiblemente en algunas ocasiones no será posible conservar la evidencia en su estado original, pero aún así es preciso que los cambios que se hagan a la evidencia sean los menores posibles. Cuando el cambio es inevitable tiene que haber algún justificante para la aplicación del mismo y debe ser notificado ante un notario o la autoridad pertinente. Esto no sólo se aplica a cambios hechos en los datos, también incluye los cambios físicos que se hagan al dispositivo en estudio o investigación, en caso de ser equipo de cómputo a cualquier parte del hardware donde se lleven acabo cambios.

- Identificar los riesgos. Hacer una lista de problemas y solución, frente a los diferentes casos que se van investigando y en especial del que se tiene en este momento. Esto sirve para hacer una lista estándar de los problemas que con mayor frecuencia se pueden ir presentando.

[34] Debra Littlejohn Zinder, Scene Of The –Cybercrime Computer Forensic, HandBook, p 11
[35] ZIP o zip es un formato de almacenamiento muy utilizado para la compresión de datos como imágenes, música, programas o documentos.
[36] Jaz: La unidad Iomega Jaz es una unidad de disco extraíble cuyos discos tienen una capacidad de 1021 megabytes. Esta actualmente disponible en configuraciones SCSI externas e internas. Iomega planea sacar al mercado una versión IDE interna.

- Eliminar o minimizar los riesgos. Encontrar la forma en la que se pueden minimizar los riesgos, por ejemplo si hay que trabajar con una computadora que está protegida con contraseñas. Se deben hacer varias copias del disco original antes de comenzar a examinarlo. Es posible que se dañaran más de una copia durante la investigación.

- Verificando el esquema de la investigación. Revisar las decisiones que se han tomado y los pasos que han sido completados.

Análisis

Una vez que se generó la imagen forense de los medios de almacenamiento se procede a realizar la investigación, la cual puede llegar a ser tan cansado como el mismo caso. Hay casos que se resuelven en una semana y algunas veces se realizan hasta seis u ocho meses de trabajo en un solo caso. Imagine que tiene una computadora normal, que tiene 60 GB[37] de disco duro, eso es aproximadamente, haciendo una analogía con papel, como 51 millones y medio de hojas de papel impresas.

En esta etapa, se utilizan diferentes mecanismos y metodologías para poder llegar a obtener evidencia, por ejemplo, si alguna persona guardó un archivo en una memoria externa de USB[38] o si alguien mandó un correo (aunque haya sido borrado).

- Es necesario conocer a la victima
- Analizar la información sin modificarla
- Identificar los archivos en la evidencia: normales, borrados, pedazos, protegidos, encriptados.
- Recuperar posibles datos relevantes, como: archivos borrados, archivos ocultos
- Revelar el contenido de archivos ocultos, temporales, swap[39], encriptados o con password.

[37] Unidad de almacenamiento. Existen dos visiones distintas de gigabyte (GB) dependiendo de la exactitud que se desee. Un gigabyte, en sentido amplio, son 1.000.000.000 bytes (mil millones de bytes), ó también, cambiando la unidad, 1.000 megas (MB o megabytes). Pero para más exactitud, 1 GB son 1.073.741.824 bytes ó 1.024 MB.
[38] USB-Universal Serial Bus
[39] Swap (Paginación): Técnica que permite que una computadora simule más memoria principal de la que posee. La técnica es usada por la mayoría de los sistemas operativos actuales. Ver memoria virtual.

Tres tipos de datos:

Datos activos
Datos almacenados
Datos latentes

Donde buscar:

Correos electrónicos
Directorios Temporales
RecycleBin
RecentFiles Spoolfiles
Historial de acceso a Internet
MyDocuments
Favorites/ Bookmarks
/etc
/bin, /sbin, /usr/bin, /usr/sbin
/var/[spool|log|adm|www|…]
/home
suid,
.*, ..*
/proc, /tmp, /dev

La recuperación de los archivos borrados dentro de la computadora es un elemento clave dentro de la investigación. Ya que normalmente pensamos como usuarios que el borrar o "formatear" la computadora va a evitar que los demás accedan a la información. Esto es completamente falso, ya que al borrar un archivo simplemente quitamos el índice donde se encontraba, pero el archivo sigue en la computadora y es completamente recuperable. La única manera de no recuperar el archivo es si es sobrescrito ya sea por un proceso o por otro archivo que se alojará en el mismo espacio.

Se puede llegar en algunos casos hasta obtener todas las acciones que el usuario de la máquina ejecutó en los últimos días, como por ejemplo, las acciones en Internet, los archivos de sonido, los correos electrónicos, etc.

Reporte

Es una de las partes más difíciles que se puede llegar a enfrentar como investigador, y esto sucede porque al generar un reporte para poder explicar qué fue lo que pasó dentro de la computadora, normalmente estos reportes llegan a personas que no conocen de

computadoras y es por ello que hay que realizarlo en un lenguaje coloquial, sin hacer uso de tecnicismos.

Por medio de este disciplina se han podido resolver casos como la identificación y comprobación de personal que esta realizando fraudes internos, personas que han atacado a sistemas federales, pedófilos que venden fotografías por medio de Internet, e incluso identificar cuando los bancos son defraudados por medio de Internet.

Una parte fundamental del cómputo forense es el establecer la cadena de custodia, un procedimiento para poder comprobar todo lo que el examinador o investigador ha realizado a la evidencia desde el momento en que identificó la evidencia hasta su presentación. Esta cadena de custodia permite que si es necesario que otro investigador realice el mismo proceso, debe llegar al mismo resultado.

ESTRATEGIAS BÁSICAS EN INFORMÁTICA FORENSE

Cuando se comienza con una investigación forense lo primero que se tiene que hacer es identificar el equipo dañado, asegurarlo y hacer un estudio, antes de mover cualquier cosa hay que tomar fotografías de todo el lugar donde se llevó acabo el delito para su ulterior consulta, no permitir el acceso a gente no autorizada la cual podría eliminar evidencia y perjudicar el proceso de la investigación, identificar el o los equipos que han sido atacados.

- Debe ser muy meticuloso y trabajar con guantes especiales de látex en todo momento para evitar mezclar sus huellas digitales con otras que posiblemente se encuentren en los equipos a estudiar.

- Llevar anotaciones puntuales de todo lo que se va haciendo, un control y bitácora de trabajo.

- Identificar si la Computadora esta trabajando y tiene algún proceso en marcha, es decir, si la máquina esta en hibernación, bastará sólo con mover el mouse, para restablecer la actividad del monitor.

- No tocar el teclado por ningún motivo pues esto puede alterar o truncar el proceso que se este llevando a cabo y la finalidad es que el monitor muestre en que esta trabajando la computadora en ese momento, una vez que el monitor muestra la actividad que se está realizando, tomar fotografías de la pantalla para conservar la imagen del momento en que se intervino y conservarla como evidencia.

- Desconectar la computadora de la corriente, es muy importante hacer notar que la computadora no debe ser apagada de forma normal (esto es apagar desde el Sistema Operativo), pues al hacer este proceso se descarga la memoria y junto con ella todos los procesos que se tenia en ese momento, también es posible que se haya dejado un programa con código malicioso y se active al querer apagar la computadora, de forma tal que se puede perder evidencia muy importante; lo que se tiene que hacer es desconectar el cable

de corriente directamente de la Unidad Central de Procesamiento, simplemente aún cuando la computadora este en pleno proceso hay que jalar el cable de corriente y también desconectar de cualquier conexión de red.

- Hacer una revisión de la estructura del sistema

Antes de pasar a examinar los registros de las computadoras a investigar, el investigador debe lograr una comprensión básica de la arquitectura informática de la organización, de la infraestructura de la red y de los componentes generales del ambiente informático, incluyendo los controles existentes de seguridad de la información. Las preguntas más frecuentes por hacer incluye:

1. ¿Cómo son autenticados los usuarios ante los servidores del sistema informático donde ocurrió el fraude u otro delito?
2. Alguna forma de estar seguros de que cada usuario es realmente el individuo que se conecta al sistema y no otro que se ha hecho de su clave.
3. Se rastrean los acontecimientos de acceso y cómo se almacenan los registros para consultas posteriores
4. Es el proceso de verificación de las transacciones de información.
5. Se controlan y anotan los cambios del sistema.

- La estructura del sistema de correo electrónico, incluyendo tipos de servidores, localización física, software usado, el número de usuarios, la localización de los archivos de correo, y la contraseña del administrador.

- Estructura de la red, incluyendo la configuración de los servidores de red y las estaciones de trabajo, la marca, versión y número del sistema operativo de red que esta en uso. En caso de que se cuente con una Zona desmilitarizada, investigar como es que esta configurada.

- Identificar el Software usado. Esto incluye la aplicación del software en, proyectos administrativos, cuentas, procesadores de texto y administradores de bases de datos. También incluir programas industriales específicos, propietario de los programas, software de encriptación y programas de utilerías. Cuando se pregunta acerca del software hay que incluir la pregunta de cuándo se instaló y cuándo fue la última vez que se actualizó.

- Identificar al personal responsable de la operación, mantenimiento y expansión de la red. El personal responsable de la administración de los sistemas de correo electrónico y, el personal responsable del mantenimiento de las computadoras, que probablemente generan reportes del comportamiento o rendimiento de los equipos de cómputo.

- Investigar y verificar el procedimiento utilizado por los usuarios del sistema para acceder a su computadora y a la red. Esto incluye el uso de sistemas de seguridad físico, passwords y cualquier otra medida de seguridad usada para acceder al Sistema.

Información de accesos, lista de control que identifica que usuario tiene acceso y a que tipo de archivos. Cómo se distribuyen los archivos, la estructura y nombre del sistema.

- La información guardada por el usuario en disquetes u otras unidades portátiles de almacenamiento es otra probable fuente de evidencia. Los usuarios guardan información en estos dispositivos por muchas razones. En primer lugar, porque hacen sus respaldos de algunos archivos, por si es necesario usarlos debido a la pérdida de algún documento o archivo de gran importancia, también guardan archivos de correo electrónico, ya que hay servidores de correo que están programados para realizar la depuración de las bandejas de entrada cada cierto periodo, finalmente algunos usuarios guardan información en dispositivos removibles porque no tienen permiso de almacenar información personal en el disco duro de la computadora. Existen disquetes con información intacta. Recolectar y examinar los disquetes es un paso esencial durante el proceso de recabar evidencia digital.

- Interrogar a todos los usuarios: Adicionalmente a lo descubierto desde el sistema de la computadora, todos los testigos deben ser interrogados. Se debe preguntar quién usa la computadora de qué manera y cómo organiza y archiva los datos, tal vez así se obtenga información que no seria revelada por los datos proporcionados directamente del sistema. Para completar esta información, hay que entrevistar a las secretarias y otros asistentes que son testigos del movimiento generado en torno al equipo en cuestión.

- Hay información que el usuario lleva de casa a la oficina y viceversa, una opción es que los datos pueden ser transferidos desde el lugar de trabajo en dispositivos de almacenamiento portátil, puede ser que algún empleado tenga acceso a la red de la compañía desde su casa. En esta situación la computadora de casa actúa exactamente igual que si estuviera en la oficina. Pero como sea que se hayan transferido los datos, el punto crítico radica en encontrar a la persona que actúa desde afuera, transfiriendo y jalando datos desde la computadora de la empresa.

- Productos como Palmtop[40] y computadoras portátiles son otro buen recurso de evidencia. Las Palmtop incluyen agendas electrónicas con direcciones convirtiéndose en un aparato más poderosos incluso que las 3 Com's PaIm Pilot y Apple's Newton. Adicionalmente almacena calendario e información de contactos, muchos de estos dispositivos almacenan notas de lo que el usuario hace como citas, agenda y el uso del correo electrónico. Arriba de esta escala de aparatos portátiles se tiene a las computadoras personales o Laptop's, que ofrecen la posibilidad de identificar específicamente a los usuarios. La computadora personal puede considerarse un recurso de recolección de evidencia bastante productivo pues tiene una gran diversidad de registros que pueden ser examinados. Pero aquí al igual que las computadoras de casa se debe preguntar, ¿cómo las Palmtop y computadoras portátiles son usadas y que datos son los que contienen?

- Proteger contra escritura y revisar que estén libres de virus una vez que se han recolectado los dispositivos de almacenamiento con los datos entre los cuales se tienen:

[40] Palmtop (handheld): Computadora pequeña que cabe en la mano y que generalmente se maneja desde pantalla táctil. Son útiles como agendas, calendario, anotador de recordatorios, reloj, calculadora, etc.

cintas de respaldo, disquetes, CD's, y algunos otros, se debe asegurar la integridad de la evidencia que se tiene, no olvidar dos pasos muy importantes, proteger contra escritura y revisar que no contengan virus. ¿Por qué es importante la protección contra escritura? Los dispositivos de almacenamiento están expuestos a que sus datos sean modificados. La protección contra escritura asegura que la evidencia no pueda ser alterada o borrada mientras se trabaje con ella. El proceso de protección contra escritura puede variar de un dispositivo a otro, pero en general el proceso en cualquier dispositivo es muy simple, normalmente cuentan con un seguro en su superficie.

- Igualmente hay que hacer una revisión en busca de virus, para prevenir que la evidencia sea alterada. Si un virus es detectado en alguno de los dispositivos, se debe grabar toda la información acerca del virus detectado e inmediatamente identificar en que parte del dispositivo fue encontrado. Hay que verificar los procesos que lleve a cabo el antivirus, porque si repara automáticamente se pueden perder o modificar datos muy valiosos para la investigación.

- Manejo de la evidencia: En caso de que sea necesario transportar la evidencia a un laboratorio para un mejor análisis, se debe tener en cuenta que todos los medios de almacenamiento magnéticos son muy sensibles a algunos fenómenos físicos como, el calor, la exposición prolongada a la luz solar, estar cerca de otros dispositivos magnéticos, golpes, etc. El medio de transporte para trasladar la evidencia de un lugar a otro debe de cumplir con ciertos requisitos como, una buena ventilación y de preferencia aire acondicionado, espacio suficiente para acomodar la evidencia de tal forma que no se encimen ni se golpee uno contra otro.

- Preservar la evidencia. Mantener los originales de la evidencia en custodia, en un lugar seguro hasta que se presente ante las autoridades correspondientes.

Para garantizar la integridad de la evidencia es necesario hacer cumplir los siguientes dos puntos.

1. Que la información no sea alterada
2. Que todos los dispositivos de almacenamiento estén asegurados

- Una vez que se ha verificado que la evidencia no contiene virus y que esta protegida contra escritura, el siguiente paso es hacer una copia imagen de cada uno de los dispositivos recolectados. El proceso de copiado cuenta con tres características críticas. **Primero:** El proceso debe de realizarse con estándares industriales de calidad y fiabilidad; esto incluye el software que se usará para hacer la copia y el dispositivo de almacenamiento donde se grabará la misma. **Segundo:** las copias creadas deben tener la capacidad de hacer verificaciones independientes. **Tercero:** la copia creada debe ser idéntica al original aún que tenga alteraciones.
- Hacer una lista de procesos a efectuar en la evidencia.
- Asignar un número único por cada pieza de evidencia recolectada.
- Proteger contra escritura todos los dispositivos de almacenamiento recolectados.
- Revisar que ningún dispositivo recolectado contenga virus.
- Imprimir la lista de directorio para cada pieza de evidencia, con el fin de llevar un buen control.

- Asegurar que el dispositivo donde se creará el respaldo de los datos esté libre de virus y que no contenga datos anteriores.
- Restaurar cada pieza de evidencia como corresponde al número asignado cuando se realizó el análisis.
- Verificar que todos los archivos en la lista del directorio aparezca en las copias restauradas.
- Asegurar toda la evidencia

INGENIERÍA INVERSA

La ingeniería inversa, representa una técnica que puede redituar muchos beneficios en la investigación, debido al enfoque que maneja su filosofía. Por eso es importante considerarla como tal. Las tareas habituales de la Ingeniería consisten en utilizar datos técnicos para elaborar un producto determinado, por ejemplo un programa de computadora Figura 2.1.
La Ingeniería Inversa se denomina así porque avanza en dirección opuesta a esas tareas, es decir, a partir de un producto accesible al público, se obtiene información técnica detallada, con el fin de determinar de qué está hecho, qué lo hace funcionar, y cómo fue fabricado.
Aplicar Ingeniería Inversa a un producto supone profundizar en el estudio de su funcionamiento, hasta el punto de que se puede llegar a entender, modificar, y mejorar dicho funcionamiento. En general, si el producto que fue sometido a la Ingeniería Inversa fue obtenido de forma apropiada, entonces el proceso es legítimo y legal.
Los productos más comúnmente sometidos a Ingeniería Inversa son los componentes electrónicos y los programas (aunque estos últimos aún más), por los siguientes motivos:

- Por lo fácil o relativamente fácil que resulta.
- Por usar protecciones similares.
- Por no existir ninguna protección efectiva.
- Por el tamaño de la comunidad implicada.
- Por el desafío que plantea.
- Por ser didáctico.
- Por ser necesario (drivers[41]/software propietario).
- Por el ahorro económico que puede suponer, al margen de la legalidad (software propietario/videojuegos).

La forma más fácil de aplicar ingeniería inversa a un programa de computadora consiste en obtener el código fuente (o uno equivalente) a partir del cual fue generado Figura 2.2.
Para ello se suelen usar una serie de herramientas que deshacen (en orden contrario) cada una de las fases de la compilación.
El código fuente obtenido mediante este proceso rara vez será exactamente igual al código fuente original, ya que en todo caso, este código fuente generado es una interpretación por las herramientas del programa ya compilado.
Estas herramientas, además, carecen de la tabla de símbolos que fue generada durante la compilación, es decir, no sabrán cómo llamar a las variables y funciones en el código fuente generado por ellas.

[41] Driver- Manejador o controlador, software que permite el reconocimiento de determinado hardware.

Fgura 2.1 Proceso de generación de un ejecutable

Ejemplos de Ingeniería Inversa son:

- El software Samba[42], que permite a sistemas operativos UNIX compartir archivos con sistemas Windows. El proyecto Samba tuvo que averiguar información clasificada sobre los aspectos técnicos relacionados con el intercambio de archivos de Windows.
- El software WINE[43], que implementa las API[44] de Windows para poder ejecutar software de Windows desde sistemas UNIX.
- OpenOffice.Org, para comprender los formatos propios de Microsoft Office.
- El módulo de NTFS[45] de Linux, para entender la estructura del sistema de archivos NTFS.
- La videoconsola PSP[46].

[42] Samba es un software libre, reimplementación del protocolo de red Microsoft Windows Network (antes llamado SMB/CIFS), realizado bajo licencia GNU GPL. El nombre "samba", proviene de la inserción de dos vocales en el nombre original del protocolo "SMB". Samba se ejecuta en la mayoría de los sistemas Unix y basados en Unix, como Linux, Solaris y los BSD, incluyendo el Mac OS X Server de Apple.

[43] WINE (acrónimo recursivo que en inglés significa Wine Is Not an Emulator "Wine no es un emulador") es una reimplementación de la API de Win16 y Win32 para sistemas operativos basados en Unix bajo plataformas Intel. Permite la ejecución de programas para MS-DOS, Windows 3.11, Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP y Windows Vista. El nombre Wine empezó como un acrónimo para Windows Emulator, pero a lo largo de sus versiones fue evolucionando y ahora corre nativamente los programas para Windows.

[44] API(Application Programming Interface: Interfaz de Programación de Aplicaciones). Grupo de rutinas (conformando una interfaz) que provee un sistema operativo, una aplicación o una biblioteca, que definen cómo invocar desde un programa un servicio que éstos prestan. En otras palabras, una API representa un interfaz de comunicación entre componentes software.

[45] NTFS (New Technology File System): Es un sistema de archivos diseñado específicamente para Windows NT, y utilizado por las versiones recientes del sistema operativo Windows. Ha reemplazado al sistema FAT utilizado en versiones antiguas de Windows y en DOS.

[46] La PlayStation Portable o PSP (en español Estación de Juego Portátil) es una videoconsola portátil de la compañía japonesa Sony Computer Entertainment. Tercera consola de la línea PlayStation y primera

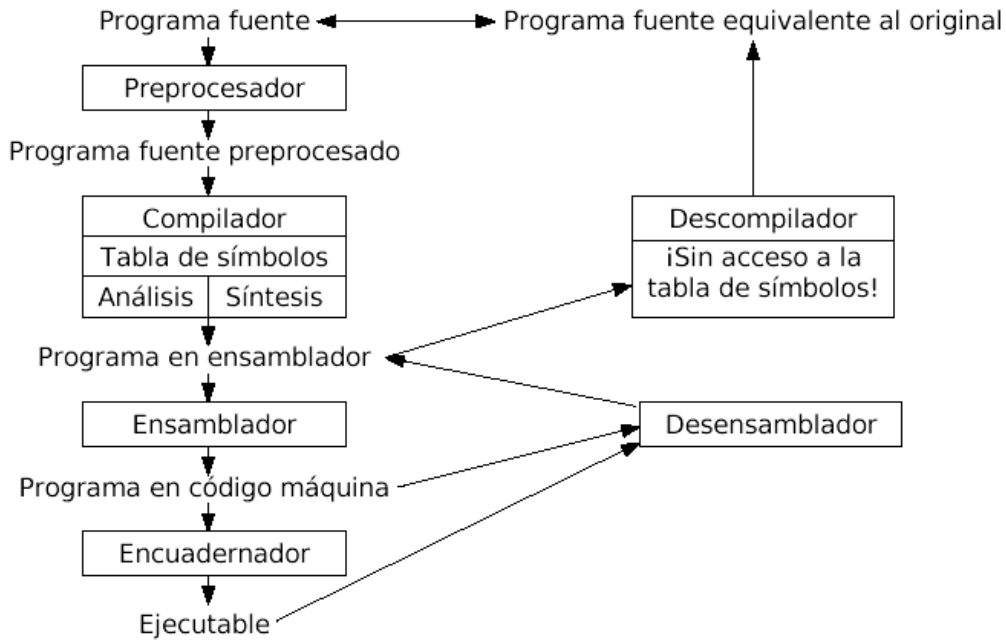

Figura 2.2. Obtención del código fuente a partir del ejecutable.

2.3. HERRAMIENTAS EN CÓMPUTO FORENSE

Para lograr la elaboración consistente de un informe y llegar a un buen termino de una investigación, es importante considerar y seleccionar el conjunto de herramientas que más se acoplen a las necesidades que plantea la situación, tales herramientas son muy diversas y se tienen desde aquellas proporcionadas por el mismísimo sistema operativo, hasta las más sofisticadas. Recordar y jamás perder de vista que el daño puede ser ocasionado por usuarios expertos o por aquellos que no tienen tanto conocimiento en el tema, por lo tanto también se debe reflejar esa consideración en las herramientas, tomando desde las más simples, hasta las más sofisticadas. Todo debe ser considerado con la proporcionalidad necesaria, para poder lograr mejores resultados y mejorar tiempos.

incursión de Sony en el mercado de las portátiles, fue presentada oficialmente en la Electronic Entertainment Expo el 13 de mayo de 2003.

HERRAMIENTAS BÁSICAS DEL CÓMPUTO FORENSE

Existen múltiples herramientas que pueden ser usabas para la investigación y la elaboración de documentos. Entre estas están varias que merecen ser mencionadas y consisten en aquellas que se puede proporcionar el sistema operativo por si solo con su conjunto de registros e historiales. Estos deben ser clasificados de diversas formas, para la buena recopilación de pruebas.

Rastreo de Sitios de Web Visitados

Mediante las siguientes utilerías de las que esta dotada cualquier sistema operativo se puede hacer un buen rastreo de las actividades que fueron realizadas en la Internet. Este tipo de recursos están a la disposición de cualquier usuario, lo cual hace de estas un conjunto de herramientas potenciales para el mejor conocimiento de las actividades de un usuario malicioso.

- **Cookies**

Las cookies constituyen una potente herramienta empleada por los servidores Web para almacenar y recuperar información acerca de sus visitantes. Dado que el Protocolo de Transferencia de Hiper Texto (HTTP) es un protocolo sin estados (no almacena el estado de la sesión entre peticiones sucesivas), las cookies proporcionan una manera de conservar información entre peticiones del cliente, extendiendo significativamente las capacidades de las aplicaciones cliente/servidor basadas en la Web. Mediante el uso de cookies se permite al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc.

Una cookie no es más que un fichero de texto que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, con información acerca de lo que hemos estado haciendo por sus páginas.

Entre las mayores ventajas de las cookies se cuenta el hecho de ser almacenadas en el disco duro del usuario, liberando así al servidor de una importante sobrecarga. Es el propio cliente el que almacena la información y quien se la devolverá posteriormente al servidor cuando éste la solicite. Además, las cookies poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión hasta una fecha futura especificada, a partir de la cual dejan de ser operativas[47].

[47] http://www.iec.csic.es/criptonomicon/cookies/queson.html

Netscape Navigator para Windows

Ver "cookies.txt" en C:\Program Files\Netscape\Navigator folder (en la carpeta de Navigator)

Netscape Communicator para Windows

Ver "cookies.txt" en C:\Program Files\Netscape\Users\

Netscape para Macintosh

Usa un archivo que se llama "MagicCookie" que se encuentra en la carpeta de Netscape dentro de la carpeta de Preferencias de la Carpeta de su Sistema.

Microsoft Internet Explorer

Hay un archivo separado en el directorio C:\Windows\Cookies para cada sitio que quiere grabar datos de cookies en el computador. La versión de Explorer para el Macintosh usa un archivo llamado "cookies.txt" en la sub-carpeta de memoria intermedia en la carpeta de preferencias en la carpeta del sistema.

- **Bookmarks**

Los bookmarks son accesos rápidos de Internet que los usuarios pueden salvar (ahorrar) sobre el browser de Web. Así, los usuarios no tienen que recordar o anotar (escribir) el URL o la posición de sitios de Web que ellos podrían desear visitar de nuevo en el futuro.
Casi todos los browsers de Web apoyan un rasgo o marca, que deja a usuarios salvar la dirección URL[48] de una página de Web de modo que ellos fácilmente puedan visitar de nuevo la página en un tiempo posterior.
Hay dos formas de acceder a bookmarks. Uno está en el browser de Web bajo Favoritos (Figura 2.3). La otra está sobre C:\Documents and Settings\Administrador\Favoritos (Figura 2.4).

[48]URL (Uniform Resource Locutor) - Localizador Uniforme de Recursos). Forma de organizar la información en la web.

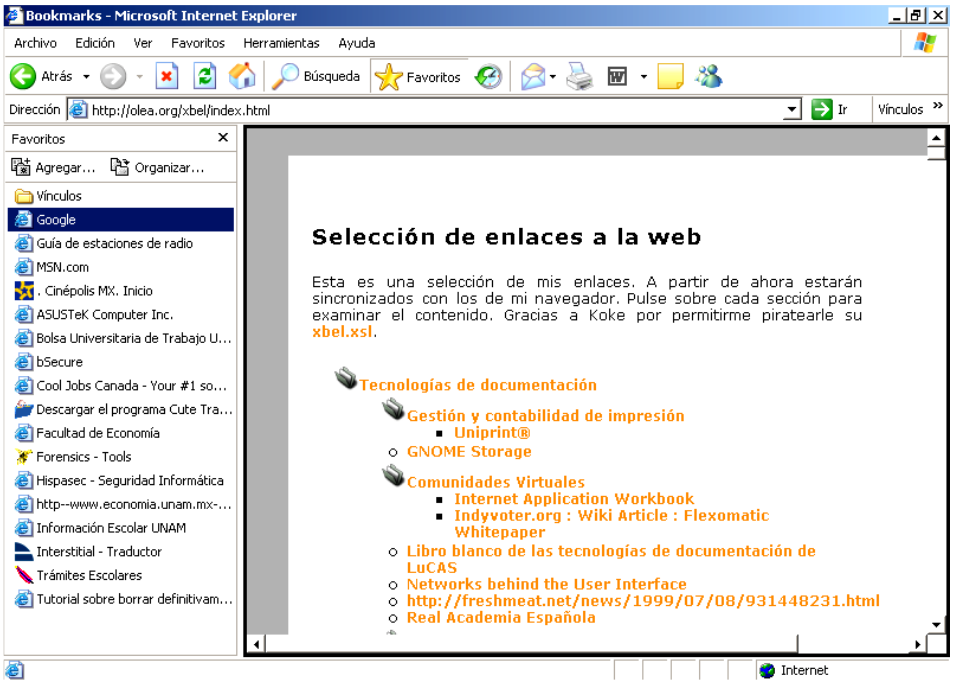

Figura 2.3 Acceso rápido a bookmarks

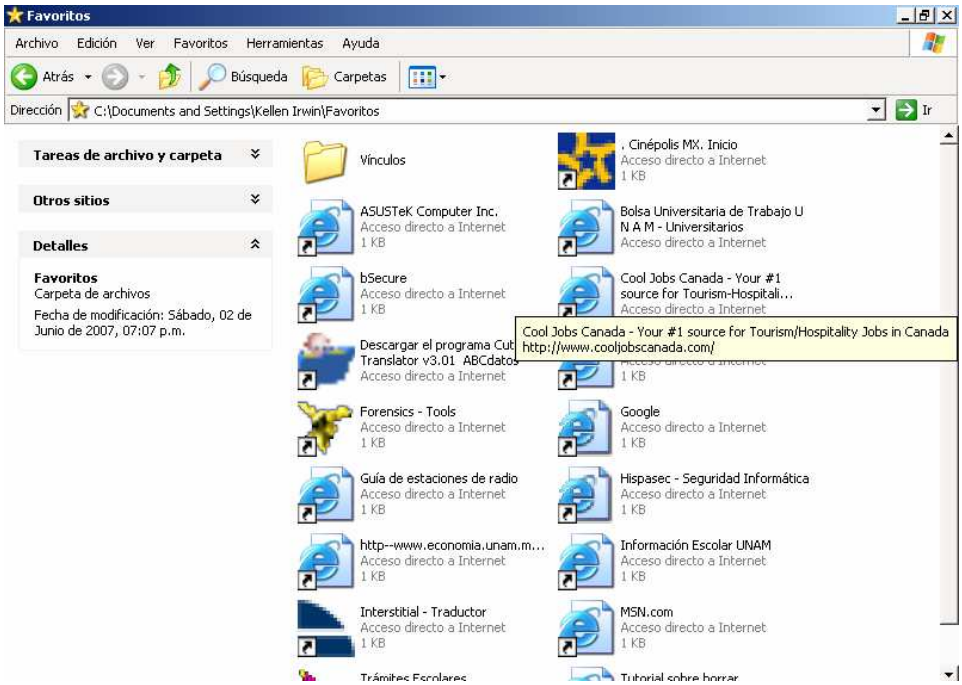

Figura 2.4 Acceso indirecto, por medio de ubicación en sub-directorio.

- **History Buffer**

Un History Buffer, es un área de almacenaje temporal, por lo general en la RAM[49]. El objetivo de la mayor parte del **history buffer** es de interpretar como un área de propiedad, el permiso la CPU[50] de manipular datos antes de la transferencia de ello a un dispositivo (por ejemplo, una impresora, el dispositivo externo, etc.).

Como los procesos de lectura y escritura de datos a un disco son relativamente lentos, muchos programas guardan (mantienen) la pista de cambios de datos de un history buffer y luego copian el history buffer a un disco. Por ejemplo, los procesadores emplean un buffer para mantener la pista de cambios a archivos. Entonces cuando se salva el archivo, el procesador de texto pone al día el archivo de disco con el contenido del buffer. Esto es mucho más eficiente que el tener acceso al archivo sobre el disco cada vez que se hace un cambio al archivo.

Así los cambios al principio son almacenados en un buffer, no sobre el disco, todos los cambios serán perdidos si hay alguna falla durante una sesión. Por esta razón, esto es una buena idea salvar el archivo de vez en cuando. La mayor parte de procesadores de texto automáticamente salvan archivos a intervalos regulares.
Por otra parte, un history buffer es un área de almacenaje sobre el navegador de Web de sitios de URL. Lo que el history buffer muestra, desde el punto de vista del Navegador de Web, es que URLS o sitios han sido visitados de día y que pantallas han sido abiertas bajo cada URL
Para encontrar en History Buffer, vaya al navegador de Web. Sobre la barra de instrumento hay un icono llamado Historial.

El history buffer puede ser limpiado por el usuario por simplemente destacando y suprimiendo los artículos en la lista. El contenido suprimido de esta lista no es almacenado en ninguna parte en el navegador, pero ellos todavía existen en el history buffer de disco duro.

Tal información puede documentar/demostrar que un empleado (o al menos el individuo que se sentó frente al ordenador personal bajo la revisión) tenía acceso al Web: en violación de políticas de la compañía; durante horas de trabajo en vez de sólo durante veces predeterminadas aceptables (p. ej., comida, horas no laborales); los fines de semana o durante otras veces fuera de lista(programa), no normales cuando los empleados u otro personal no deberían estar en el edificio/oficina; o sitios desaprobados o no autorizados de visita ver Figura 2.5.

[49] (Random Access Memory - Memoria de acceso aleatorio). Tipo de memoria donde la computadora guarda información para que pueda ser procesada más rápidamente. En la memoria RAM se almacena toda información que está siendo usada en el momento.
[50]

Figura 2.5 History Buffer

➢ **Cache**

La memoria caché es una clase de memoria RAM estática (SRAM) de acceso aleatorio y alta velocidad, situada entre el CPU y la RAM; se presenta de forma temporal y automática para el usuario, que proporciona acceso rápido a los datos de uso más frecuente.
La ubicación de la caché entre el microprocesador y la RAM, hace que sea suficientemente rápida para almacenar y transmitir los datos que el microprocesador necesita recibir casi instantáneamente.
La memoria caché es rápida, unas 5 ó 6 veces más que la DRAM (RAM dinámica), por eso su capacidad es mucho menor. Por eso su precio es elevado, hasta 10 ó 20 veces más que la memoria principal dinámica para la misma cantidad de memoria.

La utilización de la memoria caché se describe a continuación:

1. Acelerar el procesamiento de las instrucciones de memoria en la CPU.
2. Los ordenadores tienden a utilizar las mismas instrucciones y (en menor medida), los mismos datos repetidamente, por ello la caché contiene las instrucciones más usadas.

Por lo tanto, a mayor instrucciones y datos el CPU pueda obtener directamente de la memoria caché, tanto más rápido será el funcionamiento del ordenador.

- **Archivos temporales de Internet**

La ventaja de mirar los Archivos Temporales de Internet sobre cualquier otro archivo consiste en que esto le muestra la dirección del sitio, y cuando fue su ultima modificación o acceso. Esto puede ser muy útil juntando pruebas de demasiado acceso a Internet, o el acceso a Internet inadecuado. Estos también pueden ser útiles en la confirmación (prueba) de un modelo de veces de duración y conexión.

HERRAMIENTAS ESPECIALIZADAS

Estrictamente hablando, el Análisis Forense se refiere a la recopilación de evidencias bajo notario que puedan servir como prueba judicial. Es por ello que la mayor parte de las técnicas se basan en la recuperación de información de discos duros.

- **Recuperación de evidencias en discos**

Estrictamente hablando, el Análisis Forense se refiere a la recopilación de evidencias bajo notario que puedan servir como prueba judicial. Es por ello que la mayor parte de las técnicas se basan en la recuperación de información de discos duros, ahora que comienza a decaer las técnicas denominadas **Floppy Disk Forensics**

En este sentido, el líder del mercado en entornos forenses de discos es **ENCASE**, que puede realizar duplicaciones exactas del contenido de un disco, incluso de forma remota. **SMART** es una utilidad que permite instalar en un disco las imágenes capturadas con Encase. A la sombra de esta herramienta, líder del mercado, han surgido muchas otras herramientas similares, como por ejemplo **Forensic Toolkit**

La empresa Checa LEC, dispone de dos productos de análisis forense de discos, **Disk Doubler II** (un duplicador hardware de discos) y **DiskDoubler Plus**, una aplicación de búsqueda de cadenas en los datos adquiridos.

La recuperación de ficheros borrados o no accesibles entra también dentro de este campo. Búsqueda de cadenas en los datos adquiridos. Lo más normal en caso de querer recuperar datos de un disco es intentar montar la partición con un arranque del sistema operativo **Linux. Foremost** permite extraer ficheros del interior de una imagen de disco realizada con el comando dd de Linux. Existen varias herramientas de recuperación de ficheros, como por ejemplo **CIA Unerase**, **File Recover**, **Restores 2000**, **Active@**, **R-Studio**, **Ontrack Easy Recovery y GetDataBack**, (si se han borrado particiones con fdisk). **Sleuth Kit** (web que contiene interesantes artículos sobre Forensics) y su entorno gráfico **The**

Autopsy Forensic Browser permiten visualizar el contenido de sistemas de ficheros y ficheros borrados. **NTFS Reader** es un programa windows que genera una imagen de floppy disk para arrancar en FreeDos y permite leer y copiar ficheros dentro de particiones NTFS. **Bootdisk, Winimage** o **PEBuilder** permiten crear imágenes de discos de arranque de diferentes sistemas operativos. **Wotsit Format** contiene las especificaciones de múltiples formatos de ficheros.

Drive Image o Norton Ghost, ambas de Symantec, permiten la gestión de particiones.

Por otro lado, el análisis forense también se refiere a determinar las causas del compromiso de seguridad de un sistema, es decir, la alteración de sus datos o la caída o mal funcionamiento del sistema**. Tripwire y Osiris**, son dos sistemas de control de integridad de ficheros.

- **Recuperación de contraseñas**

John the Ripper es el crackeador de contraseñas fuerza bruta más famoso, probablemente por ser gratuito y uno de los primeros. El proyecto **OpenWall** es una recopilación de recuperadores de contraseñas, al igual que **Russian Password Crackers**. Ambos incluyen crackeadores para compresores, para utilidades de cifrado, BIOS, formatos de ficheros (Office, PDF, etc.), bases de datos, Sistemas Operativos, Aplicaciones, etc. se incluyen además enlaces sobre los algoritmos y sus debilidades. **MDcrack** es capaz de romper hashes[51] MD4, MD5 y NTLM1.

Existen varias formas de recuperar o restablecer una contraseña en Windows. La página de Daniel Petri muestra algunas de ellas, como por ejemplo **el Offline NT Password Registry editor** (portado al DOS como chntpw) o pwdump3 y **Dumpsec** (para Windows 2000). **LC5** es la última versión del famoso crackeador de passwords comercial **LophtCrack**, antiguo grupo de hacking ahora reconvertido en la empresa **Stake**. Se trata de un software de recuperación de passwords por fuerza bruta y por diccionario para Microsoft Windows. Las versiones anteriores de Lophtcrack tienen el código fuente disponible. En la web puede descargarse una versión de evaluación de 15 días con el ataque por fuerza bruta deshabilitado. **Cain** es otro software muy conocido para la recuperación de password Windows.

Piero Bunari ha profundizado en la utilización y adaptación de crackeadores de contraseñas; dando como resultado las utilidades **wJohn,** el port para windows de **Lepton's Crack y WaRP**.

Más recientemente, el proyecto **Rainbowcrack** permite agilizar el cracking de contraseñas mediante precomputación de hashes. Con **Winrtgen** se puede agilizar la generación de

[51] Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

tablas para **Rainbowcrack**. Este proyecto ha tenido tanto éxito que se ha creado una página web para el cracking online de hashes. **Revelation** es una utilidad freeware para revelar las contraseñas ocultas en el GUI de Windows.

- **Detección y recuperación de Virus, Troyanos y Spyware**

Una de las mejores webs de Antivirus es el Centro de Alerta Temprana sobre Virus Informáticos, una propuesta de varios Ministerios y entidades colaboradoras públicas y privadas. Se puede encontrar tutoriales, una gran base de datos de virus, descripciones y calendarios de activación y estadísticas de infección. Existen multitud de antivirus para puestos de trabajo, pero puede ser particularmente interesante el **PC Cillin 2003** para tiempo real o el **Trend Micro System Cleaner** si se quiere escanear todo el disco duro sin instalar antivirus. Sin embargo, al parecer hay un consenso entre los creadores de virus, que consideran el **AVP Kaspersky Labs** como el mejor antivirus. **Panda Software** es la única empresa española que desarrolla actualmente software antivirus. El **EICAR** (European Institute of Computer Anti-virus Research) mantiene un fichero de prueba de antivirus, no propagable y sin un payload dañino. Es una de las mejores pruebas para ver de forma segura si un antivirus se está ejecutando o no. El **Test VEMLIE** comprueba si un sistema es vulnerable a la autoejecución de pogramas .bat en el e-mail.

Es comúnmente aceptado que **29A** es el mejor grupo de investigación de virus del mundo. Su política implica que cualquier virus desarrollado por el grupo, se confina internamente y se prohíbe su propagación. En uno de sus últimos e-zines se repasa la **virus-scene** (Situation in VX scene) y pueden encontrarse muchos links interesantes como la Reference guide to VX sites. **Mercé Molist** realizó recientemente una entrevista a VirusBuster. WinterMute mantiene en su web un Curso sobre Programación de Virus. **IKX**, menos conocido, es el otro grupo dentro de la VX Scene. **VDAT** es una web muy completa sobre colecciones de Virus. Entre los troyanos más conocidos se encuentran **Back Orifice 2000** (originario de "Cult of the Dead Cow" y de Lopht), **SubSeven, NetBus y Hack'a'tack**.

La Universidad de Calgary es la primera en incorporar a sus planes de estudio el funcionamiento y la creación de virus. Un artículo técnico de Microsof denominado Virus Hunting: Understand Common Virus Attacks Before They Strike to Better Protect Your Apps ayuda a comprender el funcionamiento de los Virus. **De entre los gusanos con mayor potencial de propagación se encuentran el SQL Slammer**, del cual se ha publicado el código fuente. Microsoft ha tomado contramedidas posteriormente. El virus de tipo gusano **Blaster** es uno de los más peligrosos últimamente. Para desinfectarse en Windows XP, es necesario dehabilitar la opción de Restaurar el sistema de forma automática, descargarse un parche y desinfectarlo con un antivirus actualizado.

The Worm FAQ es una fuente muy importante para conocerlo todo sobre los gusanos.

1. **Trend Micro PC-cillin 2003** protege de virus el puesto de trabajo en tiempo real además de filtrar POP3[52]. Es posible descargarse el software, la guía de inicio rápido y un readme.txt. Se necesita el registro para la actualización de patrones y versiones.
2. **ISS BlackICE PC Protection 3.6** es un sistema híbrido de protección de intrusiones en red, protección contra ejecución de aplicaciones y de acceso a la red y comprobación de integridad del sistema.
3. **Windows Washer** limpia el PC de ficheros temporales e históricos. La versión demo no permite realizar limpiezas programadas.
4. Entre los programas que eliminan el spyware se encuentran **Ad-aware 6.0** (el único durante mucho tiempo), **SpyBot, Search and Destroy** (uno de los mejores), **Hijack This!** (mencionado en muchos sitios) y **Spy Sweeper**. **Winpatrol** Monitoriza el PC en intervalos de tiempo detectando las diferencias.
5. Respecto a los programas que eliminan las ventanas en la navegación, los más populares son **Popup Stopper y Stopzilla**
6. **Patchfinder 2.10** es una utilidad de diagnóstico para localizar bibliotecas del sistema y compromisos del kernel por los rootkits más modernos: **Hacker Defender, APX, Vaniquish, He4Hook**, etc.
7. Los muy muy duros pueden probar la ingeniería inversa tras leerse el artículo Reverse Engineering Malware y hacer prácticas con **el IDA Pro Disassembler and Debugger**, presentándose a los retos del HoneyNet Reverse Challenge o el Reto de Análisis forense de RedIRIS (resultados).

   Ahora están de moda las bombas de descompresión, que pueden limitar el rendimiento de los antivirus que escanean en ZIP. Ejemplo:

   dd if=/dev/zero bs=1k count=10000 | gzip - > testfile.gz[53]

- **Seguridad en el correo electrónico**

La amenaza más propagada, aunque aparentemente inofensiva, son los hoaxes, mensajes de correo electrónico en los que se advierte de un virus extremadamente peligroso o de alguna otra noticia alarmista que, en realidad, no existe. Estos mensajes normalmente son reenviados por quien los recibe a toda su agenda de direcciones, como se requiere en el mensaje, ayudando a que la falsa alarma se extienda aún más. Existen varios sitios donde se puede consultar si un mensaje puede ser o no un hoax.

1. Un buen artículo introductorio sobre las técnicas filtrado de SPAM es **Fighting the Spam Monster-and Winning** . Normalmente, realizado por un robot, que recoge

[52] (Post Office Protocol 3 - Protocolo 3 de Correo). Es un protocolo estándar para recibir mensajes de e-mail. Los mensajes de e-mails enviados a un servidor, son almacenados por el servidor pop3. Cuando el usuario se conecta al mismo (sabiendo la dirección POP3, el nombre de usuario y la contraseña), puede descargar los ficheros.

[53] http://www.ausejo.net/seguridad/forense.htm

direcciones de una base de datos o recogidas de analizar las existentes en un hoax previamente lanzado. También es posible. Microsoft publica un truco para añadir simultáneamente a varios remitentes en la lista de no deseados en Microsoft Outlook 2002. SA-Proxy (ftp) es un port para Windows del SpamAssasing, un proxy local (127.0.0.1) de POP3 que filtra los mensajes y los marca como SPAM. utiliza filtros bayesianos para autoaprender del SPAM anterior. Se integra perfectamente con el cliente de correo **Bloomba** (ftp).

2. Es posible encontrar una introducción al seguimiento de emails en **Visualware. Mailtracking** es un sistema de seguimiento de emails mediante la confirmación manual de recepción del destinatario. **WMDecode** es una utilidad para extraer ficheros de un archivo **Winmail.dat de Outlook**. **Decode Shell Extension** permite extraer varios ficheros multiparte de emails en crudo en formato codificado MIME-Base64, etc.

3. Respecto al **MSN Messenger**, el protocolo utilizado está ampliamente documentado en la web del MSN Messenger Protocol; además de ser utilizado también por una versión de software libre, **amsn**.

- **Procesos en el puesto de usuario**

Con el comando msconfig, es posible en Windows XP habilitar y deshabilitar los servicios en ejecución y los elementos del inicio.

- **Anonimato**

1. **NoTrax** es un navegador de Internet diseñado para no dejar trazas de la navegación en el PC local donde se utiliza, no escribe en el registro, borra de forma segura las cookies, cachés y ficheros temporales que utiliza (los cifra con blowfich por si se cuelga), no ejecuta Spyware[54], JavaScript or ActiveX y soporta SSL[55] en un único exe

2. Se puede encontrar un interfaz web para servicios anónimos de surfing y mailing en **All-Nettools**

[54] Spyware: Los programas de espionaje de la red y su objetivo primario es conocer hábitos del usuario y bombardearlo con publicidad.

[55] (Secure Sockets Layer). Protocolo diseñado por la empresa Netscape para proveer comunicaciones encriptadas en internet.

- **Investigación de información**

Tras conseguir indicios parciales de la identidad de un atacante, es posible completar la información mediante varias formas, siendo la principal de ellas la búsqueda en Google (por ejemplo cuando se localizó el Mapa de red de la CIA). Los teléfonos se consiguen en las Páginas Blancas, las direcciones en Infobel, las fotografías de inmuebles en el Callejero Fotográfico, las fotografías de personas en Google, los Códigos Postales en Correos y los mapas en Multimap.

Existe multitud de callejeros como Páginas Amarillas, el Callejero de Terra, Arcópolis y/o Mappy; además de guías de carreteras entre dos puntos como las Guías Campsa y Michelín. Más concretamente en Madrid, hay Mapas de Zonas, Cálculo de rutas en transporte público. También es posible realizar búsquedas de vuelos (Iberia, Spanair), Hoteles (Hotelsearch y Conocemundo), empresas (Banesto Empresas, Camerdata Empresas, Yahoo! Finance y E-Informa) y países (CIA)

2.4. INSTALACIÓN DE UN SISTEMA DE SEGURIDAD

El cibercrimen es posible por que los ordenadores y las redes no disponen de la seguridad adecuada. Los agentes dedicados al cumplimiento de la ley, saben que la mayor parte de los criminales buscan presas más “fáciles”, es decir, que los carteristas por ejemplo siempre buscan victimas que no tiene un muy buen cuidado con sus respectivas carteras o bolsos, así mismo los ladrones buscan las residencias y negocios de aquellos que no han reparado demasiado en su seguridad. Todo esto nos permite llegar a un tipo de conclusión similar en el ámbito informático. En su mayoría, los ataques a las redes o sistemas informáticos encuentran la mejor oportunidad en sus debilidades. Estas muchas veces no requieren de una gran inversión de tiempo para subsanarse, tales pueden ser la instalación de parches o modificación de configuraciones. El punto preocupante radica en que la mayoría de las ocasiones los puntos débiles son muy conocidos y debido a la pobre cultura de la seguridad individual de datos, así como los sistemas que se usan, aunado a la creciente cantidad de usuarios en la red, estos alientan que fallas de seguridad tan comunes sean aun tan efectivas, aun que no sean estas las mas sofisticadas con las que se pueda vulnerar una sistema.

Factores que alientan la vulnerabilidad:

- Falta de conocimiento sobre seguridad por parte del usuario promedio.
- Poco tiempo disponible, debido a las múltiples actividades.

- Negación psicológica. No se visualizan en una situación de riesgo.

Asegurar un sistema

Se refiere al proceso de construir una barrera entre aquellos que pretenden dañar sistemas y nuestro entorno. Retomando el ejemplo que se planteó anteriormente, tenemos que hacer que nuestro equipo en vez de representar una opción prometedora para hacer daño, se presente como la última figura a considerar para vulnerar. Se debe tomar en cuenta que no hay en informática sistema completamente seguro, no se ha dado con tal formula aún. Pero lo que si se puede hacer es proveer a nuestros equipos de la mayor calidad en seguridad que se pueda, para que represente una oportunidad menos atractiva. Cabe destacar que no necesariamente tiene que ser la opción más cara.
La seguridad se puede resumir como una constante mejora, que requiere la búsqueda continua de la perfección, no es estática, de su dinamismo depende su confiabilidad.
La seguridad no se debe limitar solamente a ordenadores, también se debe extender a todos los dispositivos que interactúan con el dentro de una red o fuera de ella, como los son dispositivos móviles, unidades de almacenamiento, sistemas operativos, redes, protocolos, personas, etc.

Elementos de un Sistema de Seguridad

Un sistema de seguridad hace referencia no solo a la protección contra usuarios malintencionados, también se ocupa de otos puntos como lo son el acceso a usuarios autorizados, el mantenimiento de la integridad de datos así como de infraestructura. Estos puntos se describen bajo cuatro términos, los cuales son: autentificación, confidencialidad, integridad y disponibilidad. De no ser considerados con seriedad cada uno de los puntos mencionados anteriormente, el administrador de una infraestructura IT, fallara en su labor de mantener la seguridad. Es muy difícil abarcar toso los conceptos que se requieren para hablar de una buena seguridad, tomando en cuenta también el hecho de que a diario se generan nuevas tecnologías y conocimientos, así que se tratara de dar un vistazo a los elementos de seguridad requeridos:

Instalación de medidas de seguridad para Banda Ancha

Una “banda ancha” hace referencia a una tecnología de conexión que utiliza muchas frecuencias sobre un medio de rehabitual (como un cable coaxial usado para la televisión por cable o CATV) para aprovechar todo el ancho de banda disponible. Con ellos se consigue que todos los datos estén multiplexados[56], de forma que puedan viajar a diferentes

[56] Multiplexación: Es la combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación. Un concepto muy similar es el de control de acceso al medio.

frecuencias (o canales) simultáneamente y que puedan transmitir datos en un periodo de tiempo concreto que con tecnologías de banda ancha base (un canal) como Ethernet[57]. La banda ancha (broadband) también se llama wideband en algunas ocasiones.

Problemas de seguridad de la banda ancha

En el pasado los usuarios de modem, solían desconectarse de internet cuando habían completado su sesión, lo que sacaba a sus ordenadores de la red y evitaba que los crackers accedieran a sus sistemas o pudieran atacarlos. Con las conexiones de banda ancha que permanecen conectadas veinticuatro horas al día, siete días a la semana y se reconectan automáticamente cuando se interrumpe la conexión, los ordenadores están disponibles para ser atacados continuamente.
Otro aspecto de desventaja, lo representa la dirección IP asignada al sistema. Con una conexión de banda ancha se suele asignar una dirección IP fija o son capaces de renovar constantemente las direcciones IP DHCP asignada de forma que sus identificadores de línea permanezcan constantes durante una largo tiempo si no es que indefinidamente, lo que hace que el seguimiento de los sistemas sea extremadamente sencillo y por tanto es mas vulnerable a los ataques por la fuerza y el escaneo de puertos.

Estrategias de reducción de riesgos para una conexión de banda ancha.

Instalación de un Software Antivirus: Una amenaza seria y constante a considerar consiste en la destrucción o alteración de información por causa de un virus. Una conexión de banda ancha es tan buena para un contagio de virus, como lo puede ser un vínculo LAN[58] o una conexión de acceso telefónico, No importando la forma en que el quipo se conecta, este debe ser protegido contra virus. Tratándose de este rubro, se deben tomar en cuenta las siguientes consideraciones:

- La reputación de la compañía que lo fabrica.
- Debe ser capaz de actualizarse de forma automática respecto a las definiciones de virus.
- Debe ser capaz de escasear archivos almacenados, memoria RAM, medios extraíbles correo electrónico y datos transmitidos por la Web.
- Capacidad para limpiar y poner en estado de cuarentena los archivos infectados.
- Se recomienda también instalar dos o más aplicaciones antivirus en un sistema para que trabajen en un sistema por capas. En cambio, no se recomienda la utilización de más de una de estas aplicaciones en un mismo ordenador, esto debido a que tiende a producir fallas o comportamiento errático.

[57] Ethernet: Ethernet es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.
[58] LAN: Una red de área local, conocida por sus siglas en inglés LAN (Local Area Network).

- Definición de contraseñas fuertes: Se tiene que tomar en cuenta que son requeridos tan solo dos elementos para el acceso a la mayor parte de los sistemas informáticos y esto son: una identidad de usuario (nombre de usuario) y su contraseña (password). La primera es fácil y no suele tener carácter privado, dedo a esto es la segunda (contraseña) quien proporciona el acceso, debido a esto es que la contraseña debe ser realmente compleja, para brindar un buen nivel de seguridad
- Establecer permisos de acceso: Es importante considerar la capacidad cantidad de privilegios que se otorgan a un aulario. Es un factor que bien controlado y debidamente supervisado, trae como resultado un fortalecimiento de seguridad. Mediante la asignación de privilegios, podemos controlas las acciones que pueden ser llevada a cabo por un usuario malintencionado, debido a esto es mucho mas recomendable asignar permisos de acceso de modo personalizado que la creación de grupos, debido a que estos representan una posible vulnerabilidad de acceso a recursos que tal vez no todos aquellos miembros de un grupo usaran con prudencia, es más conveniente limitar que permitir (prevenir que lamentar).

- Uso de NAT[59]: Entre los beneficios que proporciona están el ocultar la dirección IP y el diseño de la red interna de Internet, lo cual permite evitar que los intrusos rebusquen la información y la aprovechen para acceder a la red. Permite que a los clientes utilizar direcciones IP no enrutables, como las direcciones IP privadas, pero continua permitiéndoles el acceso a Internet.

- Instalación de un Firewall: Es un producto cuyo principal fin es filtrar el tráfico que cruza los limites de una red (Banda Ancha, LAN, WAN[60], telefónica o cualquier otro sistema).

- Desactivación de los servicios innecesarios: La desactivación de servicios que muchas veces se proveen en una instalación no personalizada o completa, muchas veces pueden representar un camino más para los intrusos o personas malintencionadas. Se deben cerrar accesos a información que no sean utilizados realmente. Tal ejemplo de este tipo de aplicaciones de da en muchas versiones de Windows instalan automáticamente un servidor Web durante la instalación del sistema operativo, lo recomendado es que si no se planea usar como un servidor Web, se desactiven estas utilerías.

- Configuración de la auditoria del sistema: Comprende básicamente tareas de control para detectar la aparición de actividades anormales, esto explotando las capacidades de auditoria que ya incluyen los sistemas operativos, tales como Windows NT Workstation, Windows 2000 y Windows XP Professional, los cuales proporcionan controles gracias las herramientas administrativas en el visor de sucesos, además de la capacidad de un administrador de controlar privilegios en las cuentas, los cuales constituyen una brecha de seguridad muy explotada por los intrusos. De requerirse un control mayor, debido al gran volumen de información, podemos utilizar herramientas especializadas para ayudarnos a mantener la integridad de nuestra información y sistemas. IDS[61] Es un sistema de detección

[59] Network Ardes Translation: Traducción de direcciones de red.
[60] Una Red de Área Amplia (Wide Area Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente.
[61] IDS: Intrusión Detection System.

de intrusiones, muy conveniente para resguardar la información en ambientes empresariales. Automatiza la parte más pesada de la búsqueda de actividades anormales o sospechosas de un sistema utilizando patrones de reconocimiento y aprendizaje heurístico[62] para detectar las actividades anormales o sospechosas de las cuentas de usuario autorizadas y de los usuarios eternos malintencionados.

Instalación de medidas de seguridad para navegadores de correo electrónico

Independientemente de el tipo de conexión de la que se este haciendo uso, se debe considerar el hecho de que hay debilidades que pueden afectar nuestros ordenadores por medio de navegadores Web. Un buena cantidad de clientes de programas de software para servicios de Internet más utilizados, como exploradores Web y las utilidades de correo electrónico, son vulnerables ante una serie en incremento de ataques malintencionados, viéndose estos favorecidos por las capacidades dinámicas y automatizadas que han recibido todas estas aplicaciones con la evolución de los servicios durante el transcurso del tiempo.
La mayoría de las áreas de oportunidad encontradas en los clientes de correo electrónico y la Web se relacionan con errores de sobrecarga del buffer o la ejecución arbitraria de código. Ambas situaciones, permiten a un sistema remoto ya sea un sitio Web o el emisor de un mensaje de correo electrónico, ejecute códigos malintencionados en un ordenador.

Códigos Peligrosos

En los siguientes puntos se observan las tecnologías más populares que crean puntos de riesgo tanto para el correo electrónico, como para páginas Web.
Java Script: Lenguaje de scripting desarrollado por Netscape para la ejecución de códigos incluidos en las páginas Web. Principalmente se puede utilizar malintencionadamente para engañar a los navegantes de la Web, para que hagan algo que normalmente no harían[63].
Active X: Tecnología de incrustación de códigos desarrollada por Microsoft.
Java:

- Hacer a los navegadores y los clientes de correo más seguros.

Podemos, pese a las vulnerabilidades implícitas dentro de los paquetes que utilizamos, Internet, navegadores y clientes, fortalecer nuestro sistema para que pueda tener una menos probabilidad de ser violentado por este medio de acceso.

[62] Se denomina heurística a la capacidad de un sistema para realizar de forma inmediata innovaciones positivas para sus fines. La capacidad heurística es un rasgo característico de los humanos, desde cuyo punto de vista puede describirse como el arte y la ciencia del descubrimiento y de la invención o de resolver problemas mediante la creatividad y el pensamiento lateral o pensamiento divergente.
[63] Java Script for Beginners en http://polaris.umuc.edu/~mgaylor/Issues.html.

- Restricción de lenguajes de programación: La mayor parte de los exploradores disponen de opciones de configuración que permiten a sus usuarios restrinjan o anulen el uso de los lenguajes de programación basados en Web. La restricción de todos los códigos ejecutables en un sitio Web o al menos forzar a que sea el usuario sea el que decida cada vez que se descarga uno de ellos , permite limitar el acceso a códigos o aplicaciones malintencionados. Además de que al estar activa esta opción, también se aplica para el acceso a correo electrónico, lo que limita de la misma forma el contenido malintencionado de correo malintencionado que puede ser ejecutado por el usuario sin percatarse.
- Mantener actualizado el sistema descargando parches de seguridad: Es un punto muy importante y que requiere muy poco tiempo, se puede configurar de modo automático. Permite al sistema estar al día respecto a las nuevas vulnerabilidades que puedan haberse detectado. Con esto se busca resolver el hueco de seguridad antes que sea aprovechado por usuarios malintencionados.

- Conocimiento de los Cookies: Funciona como un testigo o mensaje que entrega un sitio Web a un explorador Web para ayudar a realizar un seguimiento a los visitantes, y que el navegador se encarga de almacenar en el disco duro de los usuarios, en un archivo de texto. El archivo contiene información que identifica las preferencias del usuario o sus actividades previas en el sitio Web, de forma que, si el usuario vuelve a visitar el mismo sitio, el navegador del usuario envía el cookie de vuelta al servidor Web. Son extremadamente útiles. Del mismo modo que los lenguajes de programación, podemos desactivar hacer lo mismo con las cookies.

Instalación de medidas de seguridad para los servidores Web

La instalación de medidas de seguridad, implica no una ventaja en estos tiempos, implica una necesidad y refiriéndonos al tema de servidores Web, evidentemente es un punto crucial, debido a que son estos quienes también interactúan de manera muy intensa con el exterior, lo cual los hace blancos muy apetecibles para ser blanco de ataques malintencionados. Entre los puntos principales que se deben cuidar respecto a servidores Web tenemos:

- Se debe de bloquear el sistema operativo subyacente, proceso que incluye la practica de actualizaciones y parches, así como la eliminación de protocolos y servicios innecesarios, además de la configuración de controles nativos
- Situar el servidor tras una barrera firewall o proxy inverso, representando estos un fuerte punto de control y filtro de tráfico en un servidor Web.
- Asegurar el servidor Web en si mismo: Consiste en una serie de facetas que se describen a continuación:

1. Filosofías usadas en seguridad de servidores Web. Existen dos líneas de pensamiento o filosofías que hacen referencia a servidores Web. La primera de ellas DMZ[64] implica el asumir que el servidor Web se va a ver comprometido, lo cual

[64] DMZ (Demilitrized Zone): Zona desmilitarizada

implica hacer planes a futuro en función de ello. Consiste en una zona de red en que el servidor Web se asegura ante los puntos débiles mas conocidos pero que se sabe es inseguro en algún punto. Consiste en asumir que el tiempo y el dinero necesarios para asegurar la red contra cualquier ataque posible, es un gasto demasiado grande, que llega a superar el valor de los datos almacenados en el servidor Web. La segunda Stronghold[65] tiene la visión de intentar evitar cualquier ataque sea cual sea su coste. Este tipo de configuración suele aplicarse a empresas en las que la integridad y disponibilidad de la información de sus servidores Web se considera esenciales para la realización de sus actividades, tales como sitios de comercio electrónico. Asume que los datos almacenados son lo suficientemente valiosos como para no reparar en gastos en un aspecto como lo es su protección.

2. Aislar el servidor Web: Con el fin de evitar comprometer la red LAN, este debería estar separado del servidor Web, así de verse comprometido este, se evitara comprometer a toda la red. Dentro de este punto se puede realizar de distintas maneras el aislamiento tales como crear un dominio separado solo para el servicio Web y sus servicios de soporte, Usar una solución que no tenga otra función que el servicio de páginas Web, situar los servidores Web en un ISP[66], externalizar los servicios Web a un ISP o un tercero.

3. Bloqueo del servidor Web: Aplicando los últimos parches y actualizaciones del fabricante. Una vez cumplido esto, el administrador debe seguir las recomendaciones del fabricante para configura para configurar adecuadamente los servicios Web.

4. Servidores Web ocultos: También llamados (rouge), los cuales pueden representar una de las perores situaciones para una administrador de un servidor Web. Es posible que un usuario con bastantes conocimientos y este pueda configurar servicios Web en su ordenador, pero lo más habitual es que se instalen sin intención. Muchos sistemas operativos incluyen software para servidores Web sin ni siquiera darse cuenta y cuando un servidor Web esta presente en una red sin que el administrador lo sepa, nadie toma las precauciones de seguridad necesarias para asegurar el sistema, haciendo que el sistema sea vulnerable a cualquier ataque a ese servidor Web. Para comprobar un sistema en busca de un servidor Web que no se conocía, se puede utilizar el explorador y acceder a http://localhost/. Si no hay ningún servidor Deneb aparecerá un mensaje de error indicando la imposibilidad de acceder al servidor. De lo contrario si aparece cualquier otro mensaje se tendrán que considerar las medidas adecuadas.

[65] Stronghold: Fortaleza
[66] ISP (Internet Service Provider): Proveedor de Servicios de Internet.

2.5 DISCO DURO

Hasta este punto se puede tener una panorámica de las posibilidades de recuperación reinformación, mediante una serie de técnicas y herramientas que no sólo permiten obtener información de un equipo que ha sido usado o que es el directamente afectado. En este aparatado, se tratara brevemente la constitución física de un disco duro, como principal fuente de pruebas y como el cuerpo del que más información se puede obtener en caso de perdida de información. Por lo tanto, se debe conocer bien como funciona esta pieza fundamental para realizar cualquier investigación.

Conceptos generales de un disco duro

Por ultimo, en este apartado se hace referencia a la constitución física de un disco duro, esto es debido a que durante los bloques anteriores se habló de las formas de recuperación de información por medio de algunas técnicas y herramientas, estas permitirán recuperar información, pero en el caso particular de un daño físico del disco duro, el enfoque tiene que cambiar, debido a que al menos todos los programas descritos anteriormente, sólo se aplican en casos en los cuales se puede acceder a un disco duro sin daño físico. Se tiene que pensar en la posibilidad, debido a que el mal uso o eliminación de información, no sólo se limitan a un borrado de archivos, se podría hablar también de un atentado a la información de un modo más drástico y tal es el caso de una destrucción o daño físico. Esta modalidad del delito, lo pone en otra rama muy interesante del cómputo forense, debido a que también hay las técnicas para la recuperación total o parcial de información. Por eso es que se requiere un conocimiento básico no sólo sobre sistemas operativos y programas, también se requiere una formación en el aspecto de dónde acudir, para hacer una recuperación física.
Actualmente hay muchas empresas que realizan esta labor, debido esto no sólo a que hay quien quiere hacer daño a la información, también existen aquellos casos en que se provocan daños que no son debidos a un intento de perjudicar a una institución o persona. Así que esta resulta un área de oportunidad muy redituable para el sector privado.

Composición mecánica de un disco duro:

El disco duro esta compuesto por varios discos o platos apilados distantes de una carcasa impermeable al aire y al polvo Figura 2.6.

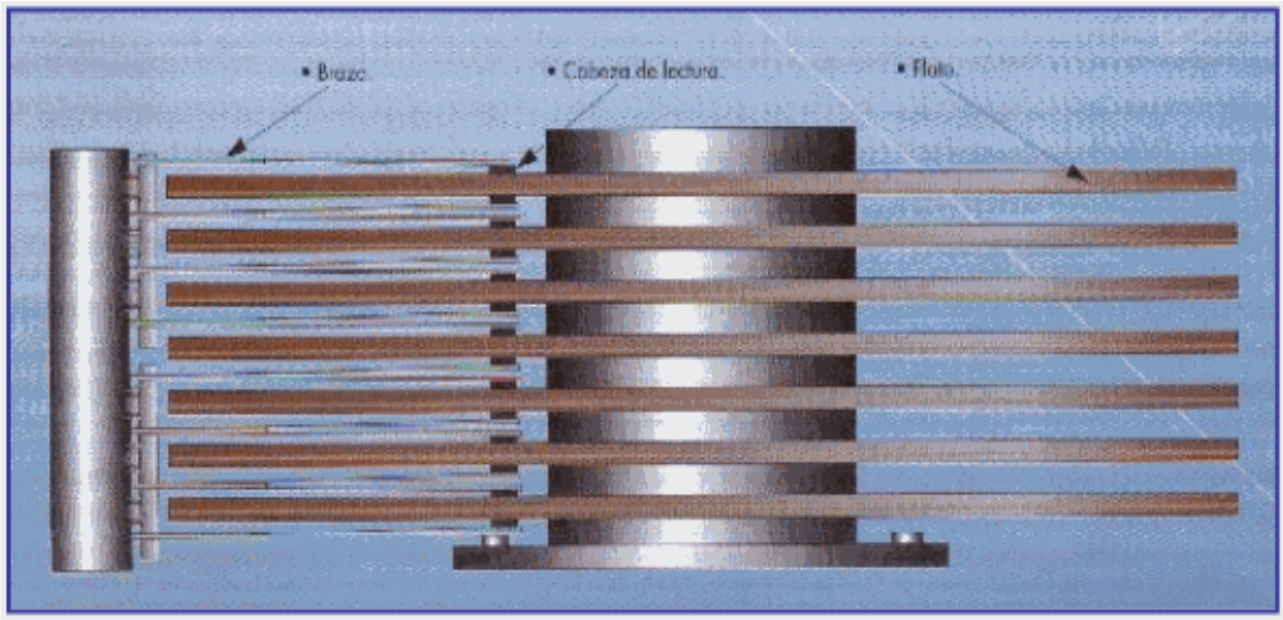

Figura 2.6 Estructura interna del disco duro.

Piezas de un disco duro:

Como se puede apreciar en la figura 2.7 un disco duro esta contenido de diferentes piezas que se van a mencionar a continuación:

- Platos o discos donde se graban los datos.
- El cabezal de lectura/escritura.
- El impulsor de cabezal (motor).
- Electroimán que es el que mueve el cabezal.
- Un circuito electrónico de control lo cual contiene, la interfaz con el resto de los componentes de computadora, memoria caché.
- Una caja que protege al disco duro de la suciedad o polvo del medio.
- Una bolsita desecante con lo cual se evita la humedad.
- Tornillos que son especiales.

Figura 2.7 Partes que componen a un disco duro.

Estructura física de un disco duro:
El disco duro esta compuesto por las siguientes estructuras:

Platos:
También llamados discos. Estos discos están elaborados de aluminio o vidrio recubiertos en su superficie por un material ferromagnético apilados alrededor de un eje que gira gracias a un motor, a una velocidad muy rápida. El diámetro de los platos oscila entre los 5cm y 13 cm. Ver figura 2.8.

Cabezal de lectura/escritura:
Es la parte del disco duro que lee y escribe los datos del disco. Ver figura 2.8. La mayoría de los discos duros incluyen una cabeza de lectura/escritura a cada lado del plato o disco, pero hay algunos discos de alto desempeño que tienen dos o más cabezas sobre cada superficie, esto de manera que cada cabeza atienda la mitad del disco reduciendo la distancia del desplazamiento radial.

Impulsor de Cabezal:
Es un motor que mueve los cabezales sobre el disco hasta llegar a la pista adecuada, donde esperan que los sectores correspondientes giren bajo ellos para ejecutar de manera efectiva la lectura/escritura. Figuras 2.8 y 2.9.

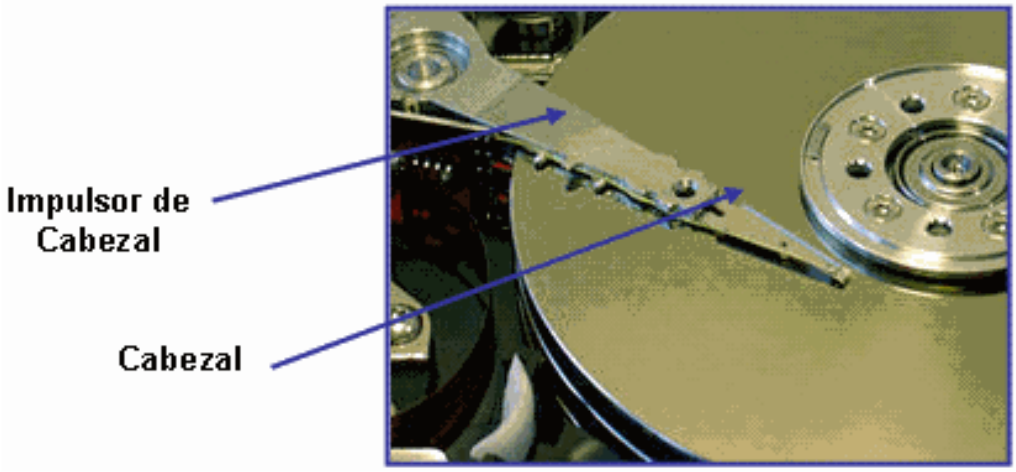

Figura 2.8 Estructura interna del disco duro impulsor de cabezal, cabezal y platos (discos).

Pistas:
La superficie de un disco esta dividida en unos elementos llamadas pistas concéntricas, donde se almacena la información. Ver figura 2.9. Las pistas están numeradas desde la parte exterior comenzando por el 0. Las cabezas se mueven entre la pista 0 a la pista más interna.

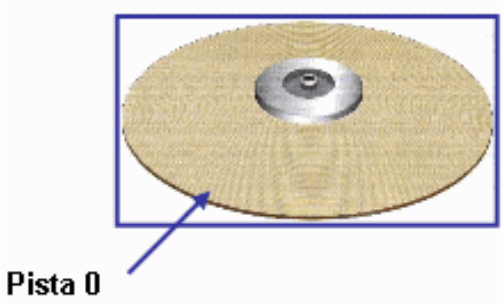

Figura 2.9 Estructura interna del disco duro. Plato (disco)

Cilindro:
Es el conjunto de pistas concéntricas de cada cara de cada plato, los cuales están situadas unas encima de las otras. Lo que se logra con esto es que la cabeza no tiene que moverse para poder acceder a las diferentes pistas de un mismo cilindro. Dado que las cabezas de lectura/escritura están alineadas unas con otras, la controladora de disco duro puede escribir en todas las pistas del cilindro sin mover el rotor. Cada pista esta formada por uno o más cluster.

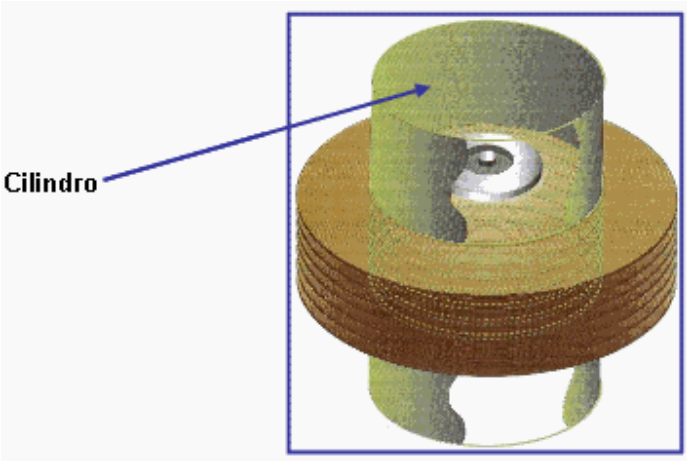

Figura 2.10 Estructura interna del disco duro. Representación física de un cilindro

Sector:

Las pistas están divididas en sectores, el número de sectores es variable. Un sector es la unidad básica de almacenamiento de datos sobre los discos duros. Ver figura 2.11. Los discos duros almacenan los datos en pedazos gruesos llamados sectores, la mayoría de los discos duros usan sectores de 512 bytes cada uno. Comúnmente es la controladora del disco duro quien determina el tamaño de un sector en el momento en que el disco es formateado, en cambio en algunos modelos de disco duro se permite especificar el tamaño de un sector.

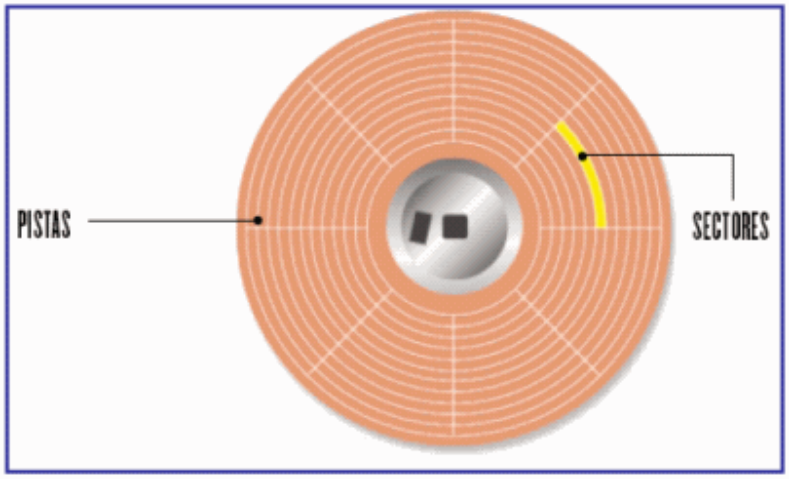

Figura 2.11 Representación física de un sector en un disco duro.

Cluster:

Es un grupo de sectores, cuyo tamaño depende de la capacidad del disco. Ver tabla 2.1

Tamaño del Driver	**Tipo de FAT (bits)**	**Sectores por cluster**	**Tamaño del Cluster (kb)**
0-15	12	8	4
16-127	16	4	2

128-255	16	8	4
256-511	16	16	8
512-1023	16	32	16
1024-2048	16	64	32

Tabla 2.1 Proporciones del cluster respecto al tamaño del disco.

Geometría del disco duro:

Ahora se vera la organización electrónica de cualquier disco duro según el número físico real de platos, cabezas, pistas y sectores:

Se sabe que el disco duro tiene una cabeza de lectura/escritura para cada cara de un plato, entonces si se sabe el número de cabezas que hay en un disco duro automáticamente se sabe el número de platos que contiene y viceversa.

Ejemplo: Si se tiene 5 platos entonces se tiene 10 cabezas de lectura/escritura.
El número de pistas varia según el tipo de disco duro, para los discos duros antiguos el numero de pista era de 305 en cambio los discos duros más nuevos pueden tener 16000 pistas o más.

El número de pistas por superficie es igual al número de cilindros. Al multiplicar el número de cabezas con el número de cilindros se sabe el número de pistas del disco.

El número de sectores varía según el tipo de disco duro, para los discos duros antiguos el número de sectores era de 8 en cambio para los discos duros más modernos es de 60 sectores o más.

Estructura lógica de un disco duro:

La estructura lógica de un disco duro esta formado por:

1. Sector de arranque.
2. Espacio particionado.
3. Espacio sin particionar.

Sector de arranque: Es el primer sector de un disco duro en él se almacena la tabla de particiones y un programa pequeño llamado Master Boot. Este programa se encarga de leer la tabla de particiones y ceder el control al sector de arranque de la partición activa, en caso de que no existiese partición activa mostraría un mensaje de error.

Espacio particionado: Es el espacio del disco que ha sido asignado a alguna partición.

Espacio sin particionar: Es el espacio del disco que no ha sido asignado a ninguna partición.

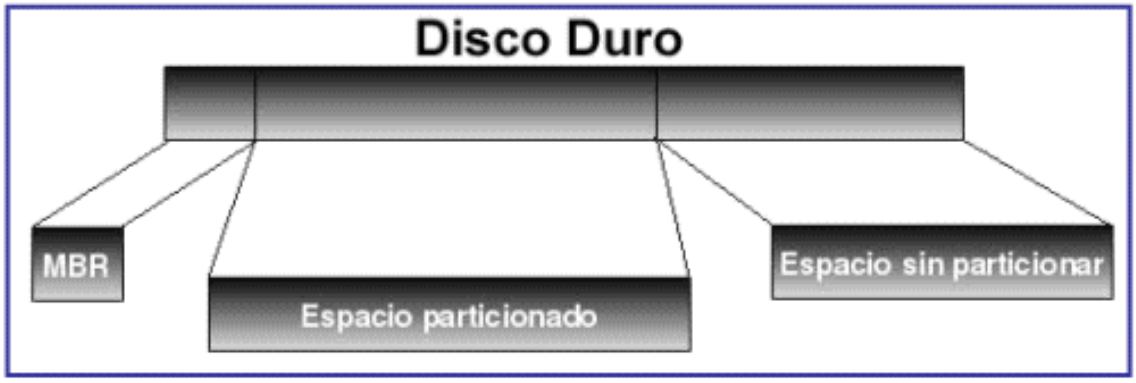

Figura 2.12 Representación de la estructura lógica de un disco duro.

A su vez la estructura lógica de los discos duros internamente se pueden dividir en varios volúmenes homogéneos dentro de cada volumen se encuentran una estructura que bajo el sistema operativo MS-DOS. Ver tabla 2.2.

Sector de arranque (BOOT).
Tabla de asignación de ficheros (FAT)
Una o más copias de la FAT
Directorio raíz.
Zona de datos para archivos y subdirectorios.

Tabla 2.2 Estructura lógica de cada volumen.

Cada zona del volumen acoge estructuras de datos del sistema de archivos y también los diferentes archivos y subdirectorios. No es posible decir el tamaño de las diferentes estructuras ya que se adaptan al tamaño del volumen correspondiente.

A continuación vamos a definir cada una de las estructuras mostrada en el cuadro.

1.-Sector de arranque (BOOT): En el sector de arranque se encuentra la información hacerca de la estructura de volumen y sobre todo del BOOTSTRAP-LOADER, mediante el cual se puede arrancar el PC desde el DOS. Al formatear un volumen el BOOT se crea siempre como primer sector del volumen para que sea fácil su localización por el DOS.

2.-Tabla de asignación de ficheros (FAT): La FAT se encarga de informar al DOS que sectores del volumen quedan libres, esto es por si el DOS quiere crear nuevos archivos o ampliar archivos que ya existen. Cada entrada a la tabla se corresponde con un número determinado de sectores que son adyacentes lógicamente en el volumen.

3.-Uno o más copias de la FAT: El DOS permite a los programas que hacen el formateo crear una o varias copias idénticas de la FAT, esto va a ofrecer la ventaja de que se pueda sustituir la FAT primaria en caso de que una de sus copias este defectuosa y así poder evitar la perdida de datos.
4.-Directorio Raíz: El directorio raíz representa una estructura de datos estática, es decir, no crece aún si se guardan más archivos o subdirectorios. El tamaño del directorio raíz esta en relación al volumen, es por eso que la cantidad máxima de entradas se limita por el tamaño del directorio raíz que se fija en el sector de arranque.
5.-Zona de datos para archivos y subdirectorios: Es la parte del disco duro donde se almacenan los datos de un archivo. Esta zona depende casi en su totalidad de las interrelaciones entre las estructuras de datos que forman el sistema de archivos del DOS y del camino que se lleva desde la FAT hacia los diferentes sectores de un archivo[67].

Arreglar un disco duro deteriorado por un accidente
Si se ha tenido algún accidente (golpe, cortocircuito) y el disco duro ha sido dañado físicamente, entonces **recuperar la información** se vuelve más complejo. En estos casos es necesario acudir a empresas especializadas que disponen del hardware necesario para acceder a los diferentes platos del disco duro, extraer la información digital, y posteriormente trabajar como los programas anteriormente descritos.

[67] http://es.wikipedia.org/wiki/Disco duro

CONCLUSIONES

El tema que se trató de abordar en forma general, representa una gran oportunidad, para muchos ingenieros e interesados en un área de oportunidad de tremendo futuro. Estas áreas de oportunidad tan grandes del ramo computacional, representan grandes retos y abren la puerta a muchas nuevas posibilidades, ya que así como el Cómputo forense tomo importancias años después de la creación de las computadoras, esta misma situación, puede desencadenar nuevas ramas del área se Seguridad, que vengan a satisfacer nuevas necesidades creadas por el avance tan imponente del cómputo y las comunicaciones.

El cómputo forense resulta un tema muy diverso y muy amplio, debe ser considerado como un fuerte punto en todas las instituciones de educación y privadas. Dado el actual avance de la tecnología, la escala de integración creciente en los medios de almacenamiento y procesadores, están creando un punto muy importante y es que mientras más capacidad se tiene, se puede estar expuesto a fallas y estas no podrán ser tan fácilmente evitadas aún con el mejor de los controles de calidad. Esto nos lleva a estar expuesto a pérdidas grandes de información, así que por consecuencia estamos mas expuestos cada día a perder nuestra información, la cual en un mundo que se domina por la misma, hace candidatos potenciales para requerir del Cómputo forense.

Se tiene que pensar seriamente en que la escala de integración en los componentes de hardware y los nuevos programas con mayor capacidad nos harían, si no hay cuidado, aumentar la escala de perdida de información y por tanto aumentar la misma escala de perdidas económicas.

Este trabajo en lo personal me deja una gran enseñanza, debido a que este campo es increíble y apasionante, creo y espero que a muchas personas más les sirva, para darse cuenta del alcance de todo esto, que propicie que más emprendedores se dediquen a la investigación, desarrollo o crear empresas que brinden servicios forenses en México, ya contamos con algunas empresas, pero es un mercado muy cautivo aún.

BIBLIOGRAFÍA

ALAN E. BRILL,FLETCHER N. BALDWIN, AND ROBERT JOHN MUNRO, Cybercrime and Security, OCEANA, Publications, September 1998.

ALBERT J. MARCELLA, Ph.D, Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, ROBERT S. GREENFIELD Editors, United States of America.

ALBERT J. MARCELLA, ROBERT S. GREENFIELD, Cyber Forensics, a Field Manual for Collecting, Examining, and Preserving Evidence of Computer, AUERBAC PUBLICATIONS, United States of America, 2001

ANONYMOUS, Maximum Security, A Hacker´s Guide to Protecting Your Computer System and Networks, SAMS PUBLISHING, United State of America, 2003.

BILL NELSON, AMELIA PHILIPS, FRANK ENFIGER, CHRIS STEUART. Computer Forensics and Investigations, THOMSOM COUSE TECHNOLOGY, United State of America, 2004.

BRIAN CARRIER, File System Forensic Analysis, ADDISON WESLEY PROFESSIONAL, United States of America 2005.

DEBRA LITTLEJOHN. Scene of the Cybercryme Comptuter Forensics Handbook, SYNGRESS SHINDER BOOKS, United State of America, 2002.

Electronic Crime Scene Investigation, A Guide for Forst Responders, NATIONAL INSTITUTE OF JUSTICE. United State of America, 2001.

EOGHAN CASEY, Digital Evidence and Computer Crime, ACADEMIC PRESS, United State of America, 2003.

FRED CHRIS SMITH, REBECCA GURLEY BACE, A guide to forensic testimony : the art and practice of presenting testimony as an expert technical witness. ADDISON-WESLEY, United States of America, 2002.

FRED CHRIS SMITH, REBECCA GURLEY BACE. A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as and Expert Technical Witnes. ADDISON WESLEY, United State of America, 2003.

ROBERT JONES, Internet Forensics, O'REILLY, United State of America 2005

HARLAN CARVEY, "windows Forensics and Incident Recovery", ADDISON WESLEY, United State of America, 2005.

JONH R. VACCA, Computer Forensics. Computer Crime Scene Investigation, CHRALES IVER MEDIA, INC., United State of America, 2002.

JULIO TÉLLEZ VALDÉS. Derecho Informático. Mc. GRAW-HILL Interamericana, México, 2002.

LAUDON C., KENNETH y LAUDON P., JANE. Sistemas de información gerencial. Organización y tecnologia de la empresa conectada en Red. PEARSON EDUCACION, Mexico, 2002.

M. FARÍAS-ELINOS, V. BÁTIZ-ÁLVAREZ LIDETEA /Escuela de Ingeniería / Facultad de Derecho Coordinación General de Investigación Universidad La Salle Grupo de Seguridad de Red CUDI, Internet-2 México.

WARREN G. KRUSE II, JAY G. HEISER, Computer Forensics. Incident Response Essential. ADISSON-WESLEY. United State of America, 2003.