UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INFORMÁTICA FORENSE COMO MÉTODO DE INVESTIGACIÓN EN LOS DELITOS INFORMÁTICOS

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

MARCOS ARTURO ROSALES GARCIA

FES Aragón

ASESOR: ING. RODOLFO VÁZQEZ MORALES

ASESOR EXTERNO: M. en C. RUBÉN VÁZQUEZ MEDINA

MÉXICO, D.F. **JULIO 2005**

A mis padres, Francisco y Concepción quienes me han brindado todo su amor, apoyo y confianza, esperando ser motivo de orgullo para ellos...

A mis queridos hermanos, Cynthia, Paco, Alfredo y Fernando, por siempre alentarme a seguir adelante...

A mi abuelita que tanto quiero, quien es un ejemplo de fortaleza y amor...

A Susana y familia por su cariño y apoyo en todo momento...

A mis tíos Ernesto y Estela, al igual que a mis primos por abrirme las puertas de su hogar ...

A mis familiares, especialmente a Teresa, Gaby, Laura, Beto, Erick, Ludwin, Juan, y mi finado tío Enrique.

A mis amigos, con quienes he compartido buenos y malos ratos ...

Finalmente a Rodolfo y Rubén, por su asesoría y valiosa colaboración en la elaboración de esta tesis.

INDICE

INDICE DE TABLAS Y FIGURAS

OBJETIVO

A partir de la revisión de los fundamentos de la informática forense, sus alcances y campos de acción, en esta tesis se proponen las prácticas que deben tenerse en cuenta para iniciar una investigación forense, las cuales habrán de conformar una guía que permita elaborar un informe claro y objetivo para proceder legalmente.

JUSTIFICACIÓN

La informática forense está adquiriendo mucha importancia dentro del medio de las tecnologías de la información, ya que cada vez es más importante la información que manejan empresas u organizaciones públicas y privadas. Esta información se almacena y procesa por computadoras y otros medios electrónicos, así que cuando se comete un delito, muchas veces la información con la cual se puede identificar el problema queda almacenada en forma digital. Es aquí donde entra la informática forense para hacer un análisis de la evidencia en forma tal que pueda usarse como prueba para dar paso a un proceso judicial. Poco a poco los delitos informáticos, así como su prevención, ha tenido mayor trascendencia e importancia a nivel mundial, siendo también el caso en México, quien se ha visto en la necesidad de crear cuerpos especializados dentro de la misma policía, tal es el caso de la Policía Federal Preventiva (PFP) quien cuenta con una división encargada de la investigación de delitos informáticos llamada policía cibernética.[1] El aumento que han tenido los delitos informáticos se pueden verificar en la página de unas de las organizaciones más importantes dedicadas a la investigación de seguridad en cómputo como lo es el CERT (Computer Emergency Responce Team) con sede en los Estados Unidos de Norte América, pero que genera evaluaciones de los incidentes a nivel mundial.[2] En las siguientes tablas se muestran las vulnerabilidades y el número de incidentes reportados en los últimos años, estas sólo para Estados Unidos de Norteamérica.

[1] http://www.ssp.gob.mx/application?pageid=pcibernetica
[2] http://www.cert.org/stats/cert_stats.html

2000-2003

Año	2000	2001	2002	2003
No Incidentes Reportados	21,756	52,658	82,094	137,529

Figura 1.Tabla tomada de la página del CERT (Computer Emergency Responce Team)[3]

Alrededor del mundo existen muchas organizaciones dedicadas a la informática forense como, tal es el caso de COMPUTER FORENSICS INC., fundada en 1994 y con sede en Seattle Washington, Estados Unidos de Norte América. Esta Empresa es una de las organizaciones precursoras en el estudio forense a equipos de cómputo; dentro de los servicios que ofrecen se encuentra la recuperación de información, reparación del daño ocasionado por el ataque informático o la intrusión de extraños sin autorización y el seguimiento judicial en contra de los responsables del daño. También cuentan con abogados expertos en las tecnologías de la información y comunicación.[4]

Otra empresa es Eviddence Matters Ltd., fundada en 1996 y ofrece servicios en el Reino Unido e Irlanda, cuenta con especialistas en informática forense. Los servicios se ofrecen a través de un grupo de abogados, especialistas en delitos informáticos, que buscan llevar ante la corte a los responsables de los ataque cometidos en contra de sus clientes.[5]

LC Technology Internacional, Inc. fundada en 1997 en Clearwater Florida, Estados Unidos, cuenta con oficinas en muchos países alrededor del mundo y las que se encargan de ofrecer los servicios de recuperación de datos y archivos digitales, pero desde el año 2001 cuenta con los servicios de informática forense.[6]

New Technologies Inc. fundada en 1996 por especialistas en el área de la informática forense, y en general por expertos en seguridad informática, tiene sus oficinas

[3] http://www.cert.org/stats/cert_stats.html
[4] http://www.forensics.org
[5] http://www.evidence-matters.com/
[6] http://www.lc-tech.com/aboutus.htm

centrales en Gresham Oregon, Estados Unidos. Ofrece servicios de seguridad en cómputo, informática forense y también ofrecen cursos para quien tiene interés en aprender las técnicas de la informática forense.[7]

Control Risk, fundado en 1975 es una organización internacional, cuenta con oficinas en la ciudad de México desde 1999. Dentro de los servicios que ofrece se encuentra, el análisis y políticas de seguridad, auditorias de seguridad, y realizar investigación contra fraudes cometidos electrónicamente, pero esto último solo desde 1995.[8]

Laboratorio de Informática Forense GC, es un equipo que se especializa en la investigación a equipos de cómputo, sus oficinas se encuentran en la ciudad de México. Ofrece servicios de análisis forense, análisis y diagnostico de vulnerabilidades, comparecencia de expertos ante instancias administrativas y judiciales, análisis técnico-jurídico respecto de la evidencia obtenida.[9]

Seguridad en la Información S.A. de C.V., es otra empresa localizada en la ciudad de México dedicada a la implementación de sistemas de seguridad informática, dentro de los servicios que ofrecen se encuentra entre otros el de Informática Forense.[10]

En México, la informática forense es una ciencia relativamente nueva y desconocida para muchos sectores, aún del mismo medio dedicado a las tecnologías de la información. Esta tesis tiene por objetivo servir como guía a todas las personas interesadas en introducirse al medio de la Investigación forense referente a equipos de cómputo, estudiando todos los puntos técnicos que envuelven a la informática forense, desde los aspectos más básicos, todo el proceso de una investigación forense y llegando hasta el análisis de un caso específico, así como también revisar la legislación en materia

[7] http://www.forensics-intl.com/index.html(12/01/05)
[8] http://www.crg.com/html/service_level1.php?service_level=4&service_path(12/01/05)
[9] http://www.lif-gc.com(12/01/05)
[10] http://www.seginf.com(18/05/05)

de informática para determinar los alcances legales con los que se cuenta actualmente en México.

INTRODUCCIÓN

En los últimos años las tecnologías de la información han tenido un avance espectacular; hoy día existen cosas que antes sólo se veían en películas de ciencia ficción, tales como enviar imágenes o ver televisión por medio del teléfono celular, pero la realidad ha superado a la ficción. Actualmente, cualquier persona que tenga una computadora y una conexión a Internet puede saber lo que está pasando en otro lado del mundo. Puede platicar con alguien en un lugar remoto sin tener que pagar una cantidad extra a su servicio de Internet, puede hacer compras en línea, pago de servicios, transacciones bancarias, enviar imágenes, datos y sonido, consultar casi cualquier información en Internet. En fin, las tecnologías de la información son indispensables para cualquier sociedad moderna que pretenda competir en el acelerado mercado de los negocios y servicios. Por ejemplo, un Banco debe de contar con bases de datos, sistemas automatizados y servicios en línea.

El gran avance en la tecnología no sólo ha sido alentador, sino que también ha traído nuevos problemas en muchos ámbitos sociales, principalmente se encuentran conductas antisociales y delictivas que antes era imposible imaginar. Este avance en la tecnología también ofrece a los delincuentes una forma de cometer delitos tradicionales en forma no tradicional, ya que se pueden cometer delitos tal como el robo de un banco, la alteración de información para obtener beneficios personales, o simplemente irrumpir en alguna empresa con el fin de dañar o extraer información. Pero también, las tecnologías de la información sirven de herramienta para aquellos que buscan delinquir con ella. Por ejemplo, en marzo de 1997, en Massachussets un joven atacó un aeropuerto. Durante este ataque deshabilitó la torre de control y todos los sistemas de comunicación dentro del aeropuerto por un espacio de seis horas, impidiendo que los

aviones aterrizaran hasta que usaron plantas eléctricas alternas para encender las luces de aterrizaje. [11]

Otro ejemplo es el ocurrido en Santiago de Chile el 25 de abril del 2002, cuando las computadoras del control de tráfico fueron apagadas durante tres días. Estas computadoras quedaron fuera de servicio por un ataque físico al lugar donde se encontraban. Como resultado tuvieron lugar varios accidentes y se imposibilitó la llegada de los servicios de emergencia al lugar de los hechos.[12]

El 23 de abril del 2003 se capturó a Khalid /heikh Mohammad en Pakistán sospechoso del atentado del 11 de septiembre del 2001 en las torres gemelas de Nueva York, Estados Unidos. En el arresto se le encontró una computadora personal, la cual contenía en su disco duro datos sustanciales e información financiera de la red terrorista Al-Qaeda. Esta información pudo ser sustraída de la metabase gracias a un software especializado de informática forense y un análisis hecho por especialistas en la materia.[13]

El 22 de Febrero de 2005 se detiene a Carlos Luna Cabrera y Edgar Ignacio Armendáriz Bautista en la ciudad de México quienes aprovechando su especialidad de asesoramiento en una empresa de computación que hace trabajos externos para bancos, cometieron fraude al desviar electrónicamente dinero de una cuenta empresarial para su propio beneficio. Estos individuos trabajaban para la empresa denominada CABSAT, (Computación a Bordo Vía Satélite) y se encargaban de brindar apoyo externo a Banco Nacional de México, especialmente a clientes que solicitaban asistencia y acceso al sistema Bancanet Empresarial (banco en línea). Esta actividad les permitía enterarse de claves, números de identificación personalizada y saldos de cuentas de activos de empresas. Con esta información consultaban saldos y determinaban la cantidad que se podían transferir.[14]

---

[11] Anonymous, *MAXIMUM SECURITY*, Sams Publishing, EUA. P.39
[12] Anonymous, *MAXIMUM SECURITY*, Sams Publishing, EUA. P.35
[13] www.forensics.com(10/10/04)
[14] www.eluniversal.com.mx(23/02/05)

En nuestro país, la mayoría de las empresas o gente vinculada con la informática desconoce la magnitud del riesgo, y generalmente no se invierte ni en recursos humanos ni tecnológicos, lo cual lleva a las empresas u organizaciones a ser blancos fáciles de ataques que se reflejan en la pérdida de información, prestigio y dinero.

Muchas empresas aún no visualizan a la seguridad informática y su entorno como una inversión, más bien lo ven como un gasto innecesario que no les reditúa ninguna ganancia. El echo es que creen estar lejos de ser blanco de algún delito informático la mayoría de las veces, cuando las empresas son blanco de ataques, las perdidas materiales sufridas son mayores que si hubiesen invertido en equipo de seguridad informática. Pero la realidad es otra, la seguridad informática busca prevenir cualquier tipo de intrusión en cualquier sistema, para que la empresa pueda brindar a sus clientes disponibilidad de sus recursos en todo momento, confiabilidad de que se le esta brindando el mejor servicio e integridad en toda la información que se maneja. Estos tres puntos, la disponibilidad, confidencialidad e integridad, son el fin de cualquier administrador de las tecnologías de la información.

Es evidente que se necesita seguridad en cada momento. Desde los primeros tiempos del hombre se vieron en la necesidad de resguardarse de las inclemencias del tiempo, de los animales salvajes y de otros hombres. Es decir, sentirse seguros; de forma que construyó guaridas, más tarde construyó murallas, luego castillos. Conforme fue evolucionando vio la necesidad de otras formas de seguridad, por ejemplo la escrita, así se inventó el cifrado, los primeros en usarla fueron la civilización Egipcia, la Mesopotámica, la India y la China. Los Espartanos ya usaban el cifrado 400 años a.C. pues utilizaban un sistema secreto de escritura, el cual consistía en enrollar un papiro en un objeto tubular y escribir sobre él. Entonces cuando llegaba al destinatario sólo podía ser leído si se enrollaba en un objeto tubular de las mismas medidas que en el que se había escrito, de no ser así sólo se verían fragmentos de letras.[15]

[15] http://www.delitosinformaticos.com/especial/seguridad/principio.shtml

Los primeros indicios de seguridad moderna se originan en la segunda mitad del siglo XVIII en la revolución industrial para combatir delitos y movimientos laborales que eran muy comunes en aquella época, ya que las máquinas comenzaban a desplazar a los obreros y estos no estaban muy contentos. Finalmente, Henry Fayol en 1919 identifica a la seguridad como una de las funciones empresariales, después de las funciones técnicas, comerciales, contables y administrativas.

Cuando Fayol define la seguridad la define de esta forma "salvaguardar propiedades y personas contra el robo, fuego, huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso del negocio". Las medidas de seguridad a las que Fayol se refería eran exclusivamente físicas, de instalación, pues los activos más importantes de las empresas eran las máquinas.[16]

Pero en la actualidad el activo más importante de las empresas es la información que manejan, por lo que es imprescindible su protección. Existe información de uso público, como la información que provee en México el INEGI (Instituto Nacional de Estadística y Geografía) que puede consultarse por todos los mexicanos y el resto del mundo. Pero también existe cierta información que es muy sensible y exclusiva, la cual está disponible sólo para grupos muy reducidos. Esta información debe de permanecer íntegra, sin ninguna alteración causada por un virus, o programa con código malicioso; o tal vez por un extraño que ha entrado al sistema. Esta información debe estar disponible en cualquier momento que sea requerida y debe poseer la confiabilidad de ser información fidedigna. Así que se tiene que invertir en seguridad informática, tanto lógica como física. La inversión que se haga en sistemas de seguridad y capacitación del personal depende directamente de que tan importante y confidencial sea la información que se está resguardando, siempre atendiendo el sentido común en términos de la relación costo beneficio.

Es preciso decir que no existe sistema completamente seguro. Se dice que la computadora más segura es aquella que está resguardada en una bóveda, desconectada de

[16] http://www.calidad.org/public/arti2000/0962913184_alexis.htm (19 julio 2004)

cualquier tipo de línea tanto eléctrica como de red. Pero también es verdad que una computadora con éstas características es inútil. Las computadoras, y todas las tecnologías de la información, se han creado para facilitar las comunicaciones, y a su vez agilizar cualquier tipo de operación e intercambio de información, pero esto a su vez expone y pone en riesgo los sistemas, cuando se conectan a la red mundial. Existe una gran diversidad de ataques que pueden recibir los sistemas desde la Internet;[17] sólo por mencionar algunos se encuentran los virus, caballos de Troya, gusanos, crackers.

Pero, ¿Qué pasa cuando, aunque se haya contado con sistemas de seguridad, una empresa ha sido vulnerada y la información dañada o alterada? Una vez que los sistemas de prevención de ataques han fallado es necesaria otra etapa que también es parte de la seguridad informática, y se denomina Informática forense, la informática forense se encarga de estudiar el delito y el daño ocasionado a los sistemas de la empresa que ha sido blanco del ataque, investiga el objetivo del atacante, los procesos llevados acabo y las vulnerabilidades presentadas en el sistema dañado, además de identificar al delincuente y apegado a derecho llevarlo ante las autoridades para que pague por sus delitos, en el capítulo dos de la presente tesis se estudia detalladamente el procesos y los puntos ha tomar en cuenta durante la investigación de un delito informático, y en el capítulo cuarto se muestra la forma en que se debe acoplar la investigación para que sea legalmente valida. A continuación se presentan algunas definiciones de informática forense.

Según Computer Forensic and Investigation, la informática forense envuelve la obtención y análisis de la evidencia digital para usarse como evidencia en casos civiles, criminales, o administrativos.[18]

De acuerdo con el DIBS USA. Inc. Corporativo privado especialista en informática forense, la informática forense examina y analiza científicamente datos

[17] http://webs.ono.com/usr026/Agika2/3internet/ataques.htm
[18] Computer Forensic and Investigation, Hill Nelson, Amelia Phillips, Frank Enfinger, Cris Steuart Edit. THOMSON Pg 2

almacenados en medios de cómputo, para que esos datos puedan usarse como evidencia en una corte.[19]

La definición que da el FBI (Federal Bureau of Investigation, dependencia de los Estados Unidos de Norte América), es la siguiente. "La computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional".

Intemet Solutions, socio de Check Point[20], con sede en Bogota Colombia, define a la "investigación forense en computación" como el conjunto de herramientas y técnicas que son necesarias para encontrar, preservar y analizar pruebas digitales frágiles, que son susceptibles de ser borradas o sufrir alteración de muchos niveles. Quienes la practican reúnen esos datos y crean una prueba de auditoria para juicios penales, buscan información que puede estar almacenada en registros de acceso, registros específicos, modificación de archivos intencionalmente, eliminación de archivos y otras pistas que puede dejar un atacante a su paso.[21]

Después de buscar en Internet, en libros y revistas que tratan sobre la informática forense, se puede decir que la informática forense estudia todo tipo de delito en donde se relacionen sistemas digitales o tecnologías informáticas. Su labor es todo un proceso que va desde la recolección análisis de las pistas, hasta seguir el proceso legal en contra de quien o quienes resulten responsables del daño ocasionado. En la presente tesis se estudia el entorno que envuelve a la informática forense y su campo de acción.

[19] http://www.dibsusa.com(28/12/2004)
[20] http://www.checkpoint.com(29/03/2005)
[21] http://www.internet-solutions.com.co/forense.html (09/11/04)

Capítulo I. Informática Forense

I. INFORMÁTICA FORENSE

En este primer capítulo se revisan conceptos fundamentales de la informática forense, el proceso tecnológico que ha incitado a nuevas formas de cometer delitos, la evolución de los "hackers" y los más destacados de ellos. Se revisa quien trabaja en informática forense alrededor del mundo, cuándo y cómo surge, en dónde, y también se ve quién hace informática forense en nuestro país.

1.1 LA IMPORTANCIA Y DEBILIDADES DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

La revolución de la informática en la administración y los negocios ha tenido gran impacto a nivel mundial, la globalización del comercio, la aparición de economías de información y el crecimiento de Internet y algunas otras redes de comunicaciones globales han transformado el rol de los sistemas de información en la administración de los negocios. Internet se ha constituido como una plataforma mundial para comprar y vender productos, crea nuevas oportunidades para la innovación en las organizaciones, estos avances tecnológicos han cambiado la forma de ver las cosas. En la actualidad, la evolución en las tecnologías de la información, que abarcan los equipos y aplicaciones teleinformáticas, ha tenido un gran impacto en la sociedad a nivel mundial. Tres importantes cambios a nivel mundial han alterado el entorno de los negocios. El primer cambio fue el surgimiento y fortalecimiento de la economía global. El segundo cambio fue la transformación de las economías y las sociedades industriales en economías de servicio basadas en los conocimientos y la información. El tercero fue la transformación de la empresa de negocios, que se veía en la necesidad de un fuerte intercambio de información.

Transformación de las economías.

Estados Unidos, Japón, Alemania y otras potencias industriales se están transformando de economías industriales en economías de servicios basadas en conocimiento e información, en tanto que la fabricación se está desplazando a los países con salarios bajos. En una economía basada en los conocimientos y la información, tanto los conocimientos como la información son ingredientes clave para crear riqueza. La revolución de los conocimientos y la información se inició a principios del siglo XX y se ha acelerado gradualmente. Para 1976, el número de trabajadores de "Cuello Blanco" empleados en oficinas sobrepasó al número de trabajadores de la granja, trabajadores de servicio y obreros, empleados en la fabricación. Hoy día, la mayoría de las personas ya no trabajan en el campo ni en las fábricas, sino que se les encuentra en las áreas de ventas, educación, cuidado de la salud, bancos compañías de seguros y bufetes de abogados. Estos trabajos implican primordialmente el manejo, la distribución o creación del conocimiento e información. De hecho, el trabajo con conocimiento e información representaba en el año 2002 aproximadamente un importante 60% del producto interno bruto de los Estados Unidos y ocupaba casi el 55% de la fuerza laboral. [22]

En definitiva, resulta fundamental contar con la información oportuna para tomar las mejores decisiones en el momento adecuado. En esta situación las nuevas tecnologías de la información son muy relevantes. Permiten obtener y procesar mucha más información que los medios manuales. Así que las empresas invierten en ellas.

Sin embargo, como cualquier tecnología, hay que tener presente que las Tecnologías de la Información son sólo un instrumento para la gestión de las empresas.

Riesgos en las tecnologías de la información.

Las tecnologías de la información son indispensables casi en cualquier empresa, ya que ofrecen una gran versatilidad en el intercambio de información, pero la misma necesidad por intercambiar grandes cantidades de información, genera riesgos y vulnerabilidades

[22] Kenneth C. Laudon, Jane P. Laudon, *"Sistemas de información gerencial", Prentice Hall, Sexta edición, 2002, pp 6.*

que exponen los sistemas y pueden ser explotadas por gente con la intención de dañar, modificar o destruir la información contenida en ellos, a este tipo de actos se les ha dado el nombre de delitos informáticos (en el capitulo III de esta tesis se definen los delitos informáticos), existe una gran variedad de ellos pero en general el objetivo de todos estos delitos es el mismo, dañar, robar o modificar información contenida en medios electrónicos es la finalidad de alguien que comete un delito informático.

Los delitos Informáticos se acrecientan día a día pues resultan muy atractivos para la gente que tiene la posibilidad u oportunidad de cometerlo, son atractivos para llevarse acabo por las siguientes razones:

- No es necesario portar un arma de fuego ni cargar con grandes cantidades de dinero.

- No hay ningún tipo de contacto físico con alguna otra persona, lo cual asegura el anonimato del delincuente.

- Lograr exitosamente un delito informático puede generar grandes sumas de dinero para el delincuente.

No cualquier persona puede cometer un delito informático, para llevar a cabo uno, es necesario, que quien pretenda cometerlo cuente con fuertes y profundos conocimientos técnicos, al menos de los sistemas en los que desea llevar acabo el delito. En algunas revistas y sitios de la Internet se dice, que los requisitos técnicos para llevar acabo un delito informático son:

- Conocimientos en diversos sistemas operativos, Windows, Unix, Mac OS, etc.

- Conocimiento en sistemas de seguridad perimetral de redes, como lo es el firewall, detector de intrusos, honey pots, etc.

- Conocimiento en redes, protocolos de comunicación, routers, etc.

- Conocimientos en lenguajes de programación, C, Java, Html, perl, etc.

- Conocimiento en bases de datos.

Los delitos informático generalmente tienen como objeto, empresas u organizaciones que le pueden retribuir algún beneficio al delincuente, este tipo de delitos se puede realizar ya sea entro de la red a dañar o en forma remota, desde dentro de la misma red que se atacara y que en la mayoría de los casos ha resultado que se trata de algún empleado con privilegios en los sistemas, que vio la oportunidad de cometer un delito informático y lo llevo acabo, y la otra forma es desde afuera de la red, esto es en forma remota, puede ser cualquier persona, a continuación se muestra una gráfica donde se ve a un individuo tratando de acceder en forma remota a una red de datos privada.

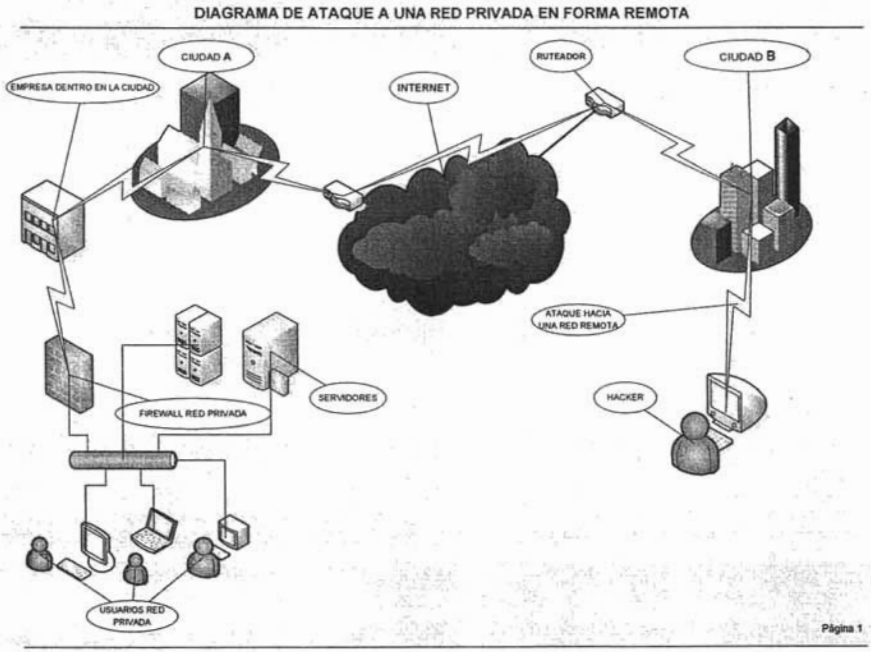

Figura 1.

1.2 DELITOS INFORMÁTICOS

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 computadoras, 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"[23]. 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. Los 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.[24]

El Hacking se considera una ofensa o ataque al Derecho de la gente, y no tanto un delito contra un Estado en concreto, sino más bien contra la humanidad o por lo menos todas las personas que tienen contacto con las tecnologías de la información, pues todos estamos expuestos ha ser victimas del hacking. Los Hackers son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo.

---

[23] La corriente yippie fue un *movimiento hippy anarquista particularmente oscuro. Los yippies tomaron su nombre de un partido de ficción el "Youth International Party", que llevaron a cabo una política escandalosa y surrealista de subversión surrealista y una maldad política desproporcionada.*

[24] http://www.monografias.com/trabajos12/hacking/hacking.shtml

En los últimos tiempos la comunidad hacker en la Internet, dice no ser responsable de actos ilícitos y describen la esencia de un hacker como alguien que simplemente tiene un gusto enorme por la investigación de los sistemas de computo, se dicen curiosos pero no con malos propósitos.

En 1961 la Bell Telephone denuncio el primer robo de servicio telefónico, había detectado llamadas con mucho tiempo de duración a un número de información de una zona aledaña. La investigación llevó a los inspectores hacia el State College de Washington, donde encontraron una caja extraña que denominaron Blue Box (caja azul) y que reproducía los tonos multifrecuencias de la compañía. Eran doce combinaciones de seis tonos maestros y se suponía que eran secretos. Pero en 1954, la compañía telefónica había publicado las claves en una revista que se distribuía entre su personal. Tarde se dieron cuenta de que la leían todos los estudiantes y egresados de ingeniería electrónica. Los alumnos llamaban al número de información, y una vez comunicados entraba en acción la Blue Box, que emitía una señal para indicar a la central telefónica que ambos aparatos estaban en línea mientras los muchachos derivaban la llamada a un número de larga distancia. Agencias gubernamentales de los Estados Unidos hicieron algunos arrestos de "phreackers"[25] por manipular sistemas telefónicos. En la década de los 80's, el FBI (Federal Boreua of Investigations) hizo algunos de los primeros arrestos de "hackers" en computadoras más activos de la época (incluyendo a Kevin Mitnick, quien sería algo así como el máximo representante de la comunidad "hacker"). Películas como "WarGames" en los 80's y "Lain Softley's" en los 90's buscaban el concepto de lo que en esencia es la personalidad o perfil de un "hacker" y muestran a una persona brillante y romántica, quien rompe las leyes (pero sólo eventualmente y lo hace con propósitos nobles).[26]

En la actualidad el término "hacker" se aplica sólo a aquellos que irrumpen en un sistema, usualmente en forma remota, obviamente con acceso a una red de computadoras.

[25] *Los phreackers es gente que trata de hacer uso de las líneas telefónicas sin tener que pagar por los servicios.*
[26] Debra Littlejohn Shinder. *SCENE OF the Cybercrime computer forensics handbook (pp 51-62)*

El primer "hacker" electrónico irrumpió en los sistemas telefónicos y su objetivo fue hacer llamadas telefónicas de larga distancia sin tener que pagar por ello. Estos "hackers" de las redes telefónicas se conocieron como "phreackers"[27]. Hay otro término que se origina durante los primeros años de las comunicaciones electrónicas, este es "cracker", 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.

El comienzo de la cultura "hacker", tal como la conocemos actualmente, se puede fechar con seguridad en 1961, año en que el MIT (Massachussets Institute of Technology) adquirió la primera PDP-1 (Programmed Data Processor 1). El comité de "Señales y Energía" del Tech Model Railroad Club adoptó la computadora como su juguete tecnológico preferido e inventó herramientas de programación, un argot y toda una cultura que giraba en torno a ella, aún hoy puede reconocerse entre las tecnologías de la información actual.

La cultura en torno a las computadoras del MIT parece haber sido la primera en adoptar el término "hacker". Los "hackers" del Tech Model Railroad Club se convirtieron en el núcleo del Laboratorio de Inteligencia Artificial del MIT, el centro más destacado de investigación sobre Inteligencia Artificial de todo el mundo a principios de los 80's. Su influencia se extendió por todas partes a partir de 1969, año de la creación de ARPANET.

Estos son algunos de los más famosos "hackers" de los últimos tiempos:

En 1990, Kevin Poulsen, "Dark Dante", tomó el control de todas las líneas telefónicas de la estación de radio KIIS-FM, de la ciudad de Los Ángeles, asegurándose de ser la llamada número 102 para ganar un concurso que llevaba a cabo la estación. Poulsen ganó un auto, Porshe 944 S2. Poulsen forzó la caja telefónica donde se

[27] http://www.geocities.com/Area51/Orion/4015/llaneros.htm

encontraba la línea de la estación de radio y la pinchó para ser el único que pudiese tener contacto con la estación de radio. Acepto ser culpable por penetrar a computadoras en búsqueda de operaciones encubiertas del FBI. Después de que el mismo FBI lo rastreo durante mucho tiempo, fue hasta que su caso apareció en el programa de televisión llamado, misterios sin resolver, así una persona lo reconoció y delato. Fue detenido y sentenciado a tres años de prisión y tres más sin autorización de acercarse a cualquier equipo de computo, actualmente trabaja para la empresa en seguridad informática, Security Focus.[28]

Julf Johan Helsingius, mejor conocido como "Julf", operaba el re-envío de correos electrónicos anónimos más popular del mundo, llamado planet.fi, hasta que tuvo que cerrarlo en septiembre de 1996. Sus problemas empezaron cuando fue acusado ante la policía finlandesa por "Church of Scientology" (un grupo religioso), pues un cliente de planet.fi divulgaba sus secretos en Internet. Julf debió desmantelar planet.fi cuando la policía lo obligó a revelar el correo electrónico del cliente, Actualmente Julf trabaja como consultor de seguridad a empresas de todo el mundo.[29]

Vladimir Levin, graduado de matemáticas en la Universidad de San Petersburgo, saltó a la fama mundial al robar 10 millones de dólares de Citibank desde su país natal, Rusia. Para ingresar a las computadoras de Citibank en Nueva York, Levin utilizó las computadoras de la compañía donde trabajaba, AO Saturn, en San Petersburgo. Fue arrestado en el aeropuerto Heathrow de Londres por la Interpol en 1995 y fue extraditado a los Estados Unidos, donde le hicieron juicio el cual perdió y fue sentenciado a tres años de prisión. Durante su proceso legal declaró que uno de sus abogados defensores era agente del FBI.

Kevin David Mitnick es quizás el más famoso "hacker" de los últimos tiempos. Nacido el 6 de agosto de 1963 en Van Nuts, California, se dice que desde muy niño sintió curiosidad por los sistemas de comunicación electrónica y fue auto cultivando un

[28] http://tlc.discovery.com/convergence/hackers/bio/bio_07.html
[29] http://tlc.discovery.com/convergence/hackers/bio/bio_08.html

obsesivo deseo por investigar cosas y lograr objetivos aparentemente imposibles, hasta llegar a poseer una genial habilidad para ingresar a servidores sin autorización, robar información, interceptar teléfonos, crear virus, etc.

Cuando el gobierno de los Estados Unidos acusó a Mitnick de haber sustraído información del FBI relacionada con la investigaciones del FBI y de haber penetrado en computadoras militares, en 1992, decidió defenderse en la clandestinidad, convirtiéndose en un fugitivo de la justicia durante casi tres años. Mitnick fue arrestado por el FBI en Raleigh, Carolina del Norte, el 15 de febrero de 1995. Mitnick descubrió y reveló información de alta seguridad perteneciente al FBI, incluyendo cintas del consulado de Israel, en Los Ángeles. Sus incursiones costaron millones de dólares al FBI y al gobierno norteamericano y obligó a este departamento policial a mudar sus centros de comunicación secreta a sitios inaccesibles. Mitnick, quién fue liberado en enero del 2000, después de permanecer casi 5 años en una prisión federal, según reportes del FBI le costó al estado norteamericano y a empresas privadas, cerca de 80 millones de dólares al ser responsable del robo de software, de información y alteración de datos. Entre los afectados además del FBI, el Pentágono y la Universidad del Sur de California, también se incluyen corporaciones tales como Motorola, Novell, Nokia y Sun Microsystems.

Mitnick se convirtió en el máximo exponente de la comunidad internacional de "hackers". Después de que el FBI lo investigó y persiguió infructuosamente durante tres años, su captura se produjo en 1995, cuando los investigadores rastrearon sus huellas hasta llegar a un departamento en Raleigh, Carolina del Norte, fue liberado en el año 2000. Actualmente Kevin Mitnick trabaja como consultor de seguridad para varias empresas.

¿Cómo se dan los delitos informáticos?

En el año 1962, Vyssotsvy, McIlroy y Morris, empleados de la compañía Bell Telephone Laboratories de Estados Unidos de Norteamérica, crearon un juego llamado "Darwin". Este consistía en la creación de programas que se reproducen en la memoria de la

computadora luchando entre sí con el fin de apoderarse de la misma, sin saberlo inventaron la base de los virus informáticos.

En los inicios de los años 80 comenzó la propagación de las computadoras personales apareciendo en los años 1981-1982 el virus Elkcloner destinado a infectarla.

En mayo de 1984, aparece una variante simplificada del juego "Darwin" llamado "Core War" en el que los jugadores escriben programas en lenguaje ensamblador, una vez que están siendo ejecutados en memoria luchan entre sí con el objetivo de bloquearse.

A partir de 1985 salio al mercado la computadora personal IBM con sistema operativo DOS la que, por el gran desarrollo en su producción, provocó una reducción de los precios permitiendo así su amplia distribución en el mundo. De esta manera aumentó la cantidad de personas ocupadas en su programación. Esto, junto con el desarrollo de las redes de comunicación, permitió que la computadora no sólo fuera utilizada en los trabajos sino también en los hogares. Además, el hecho de ser el DOS un sistema operativo sumamente amigable, poco protegido, bastante documentado, al cual los fabricantes de dichas computadoras, incluyendo sus clones, contribuyendo a estandarizar, el proceso de inicialización de las mismas, tabla de vectores de interrupción, rutinas del BIOS y localizaciones de memoria provocó la creación de una enorme plataforma común para la propagación de los virus de computadoras.

En 1986 con la creación del virus Brain comenzó lo que se ha dado en llamar la segunda etapa en el desarrollo de los programas malignos. Este virus fue construido en Pakistán por dos hermanos que vendían software, lo crearon pensando en castigar a los turistas norteamericanos que compraban en ese país copias ilegales de software a un precio muy económico.

En noviembre de 1987 fue detectado en EEUU el virus LEHIGH que sólo infectaba al archivo COMMAND.COM y que una vez que realizaba 4 infecciones destruía la información contenida en los discos. Otros virus creados este mismo año fueron: Viena, Jerusalem, Stoned (primer virus que infectó al sector de particiones de los discos rígidos y el sector de arranque de los disquetes), Italian o Ping-Pong, Cascade

(utilizaba una nueva idea, que era la de cifrar el código del virus con el fin de que varíe de un archivo infectado a otro).

En el año 1988 se tuvo una amplia propagación de los virus Stoned, Cascade, Jerusalem, Italian y Brain, lo que conllevó a la creación de los primeros antivirus.

En marzo de 1989 fue detectado el virus DATACRIME, elaborado en Holanda, el cual se propagó ampliamente; este virus, destruía la información de los discos rígidos formateando el cilindro 0 de los mismos.[30]

Una historia de hackers.

Hablando de hackers, en el año de 1986 Peter Kahl tenía treinta y cinco años de edad. Trabajaba como crupier en un casino de Hannover, él ignoraba todo sobre computación, todo excepto la existencia y el accionar de los hackers. Había asistido a una reunión en Hannover y allí comenzó a diseñar un plan para salir de su actual vida. El plan era simple, quería armar a un grupo de hackers que consiguiera información de la industria militar y defensiva del Occidente para vendérsela a la Unión Soviética.
Karl Koch había gastado la herencia de sus padres comprando drogas, un día, después de leer la trilogía Illuminatus! , de Robert Shea y Robert Anton Wilson decidió que su alias seria Hagbard, convencido que las conspiraciones dominaban el mundo. Además de las drogas se interesaba sólo en el hacking.

Los primeros dólares que ganó como hacker los gano vendiendo software de dominio público y programas que había copiado sin costo de los sistemas a los que tenía acceso. Pero los soviéticos para los que trabajaba le pidieron un trabajo de un mayor grado de dificultad, el cual consistía en ingresar a sistemas diversos, en los cuales se incluían organismos de defensa nacional y empresas, como las que se presentan a continuación.

[30] Roberti Raquel / Bonsembiante Fernando, LLANEROS SOLITARIOS, HACKERS, LA GUERRILLA INFORMATICA pp.52-57

El pentágono[31], la NORAD[32], el MIT (Massachussets Institute of Technology), la NASA[33] y también Philips[34] France. Esta es una lista de sistemas en los cuales la KGB[35] tenía interés, y le solicitaron a Hagbard que se infiltrara en ellos.

Pero Hagbard se encontró con un problema, todos esos sistemas tenían VAX[36] y él no tenia suficientes conocimientos para entrar. Hagbard necesitaba ayuda y decidió visitar el congreso anual que organizaban los del Chaos[37] de Hamburgo. Allí estaba Pengo en realidad Hans Hubner, un adolescente de dieciséis años que conocía todos los

[31] El Pentágono es la sede del departamento de Defensa de los Estado Unidos de Norte América. El edificio donde se encuentran las oficinas centrales tiene forma de pentágono y por eso el nombre, es el hogar de aproximadamente 23.000 empleados militares y civiles, y cerca de 3000 de personal de apoyo, situado en Arlington, Virginia. Tiene cinco pisos y cada piso tiene cinco corredores. El Pentágono fue inaugurado el 15 de enero de 1943 y continúa siendo el edificio de oficinas más grande del mundo.

[32] El Comando Aeroespacial Norteamericano de la Defensa (NORAD) es una organización militar binacional establecida formalmente en 1958 por Canadá y los Estados Unidos para supervisar y defender el espacio aéreo norteamericano. Usando datos de satélite y de tierra bajo radar, NORAD supervisa, valida y advierte de ataque contra Norteamérica en avión, misiles o vehículos de espacio. NORAD también proporciona vigilancia y el control del espacio aéreo de Canadá y de los Estados Unidos. http://www.norad.mil/&prev=/search%3Fq%3DNORAD%26hl%3Des%26lr%3D

[33]NASA (National Aeronautics and Space Administration) El 29 de julio de 1958, el Presidente de los Estado Unidos de Norte América Eisenhower firmó el Acta que funda la NASA que empezó a funcionar el 1 de octubre de 1958 con cuatro laboratorios y unos 8.000 empleados. Los primeros programas de la NASA fueron tendentes a poner una nave tripulada en órbita y ello se hizo bajo la presión de la competición entre los EE.UU. y la entonces URSS en la denominada, Carrera espacial que se produjo durante la Guerra Fría. http://es.wikipedia.org/wiki/NASA#Historia

[34]Philips es una de las mayores compañías de electrónica del mundo, tiene sus inicios en 1891 cuando Gerard Philips creó una empresa en Eindhoven, Holanda para "fabricar lámparas incandescentes y otros productos eléctricos'', actualmente tiene presencia a nivel mundial. http://www.philips.com.mx/about/company/global/history/index.html

[35] La KGB (en ruso Комитет Государственной Безопасности, Komitet Gosudárstvennoi Bezopásnosti, traducido como "Comité para la Seguridad de Estado") fue el nombre de la agencia de inteligencia Rusa, desde el 13 de marzo de 1954 al 6 de noviembre de 1991. El dominio de la KGB fue aproximadamente el mismo que el de la CIA o la división de contrainteligencia del FBI en Estados Unidos.

[36] Nombre original era VAX-11 (Virtual Address Extended PDP-11). Lanzada el 25 de octubre de 1977 por la compañía Digital Equipment Corporation, fue la primera máquina comercial de arquitectura de 32 bits, lo que la convierte en un hito destacable en la historia de la computación. La primera VAX-11/780 fue instalada en Carnegie Mellon University Estados Unidos. Los últimos modelos nuevos de VAXen (modelos 7000 y 10000) fueron lanzados en 1992, aunque se introdujeron cambios hasta 1997. La línea se descontinuó en 1999, y en ese entonces se rumoreaba que todas las unidades remanentes habían sido adquiridas por Intel. http://es.wikipedia.org/wiki/VAX

[37] Organización internacional de carácter inconformista cuyos integrantes se definen como portavoces de los piratas informáticos (hackers) de todo el mundo y demandan una sociedad con libertad ilimitada y flujos de información sin censuras. Organizan anualmente en Hamburgo, Alemania, un conocido encuentro de sus partidarios. http://www.glosarium.com/term/3520,7,xhtml

defectos del VAX y con quien Hagbard compartía el gusto por las drogas. Unas pocas palabras bastaron para integrarlo a la sociedad aportando un programa, cedido por Steffen Weihruch, renombrado como "el genio de los VAX" y asiduo asistente a las reuniones del Chaos que capturaba login y passwords de los sistemas VMS[38]. UNIX es un sistema operativo que funciona en casi todas las computadoras y por entonces estaba en auge, aun para las VAX. Hagbard no tuvo mas remedio que concurrir a las reuniones del Chaos y esta vez se acercó a Marcus Hess, empleado de una empresa especialista en UNIX. Marcus no opuso demasiada resistencia y pasó a formar parte del grupo. Con su incorporación y los datos que brindó, los nuevos espías ganaron dos mil quinientos dólares, toda una fortuna para esa banda de delincuentes informáticos. Mientras Hagbard y compañía hackeaban para la KGB, Bach y Handel, dos adolescentes identificados como VAXbusters (rompe-VAX), descubrieron tres máquinas de ese tipo en red instaladas por SCICON, que era una de las compañías de software más importantes de Alemania. Cuando intentaron entrar teclearon lo primero que se les ocurrió ante el pedido de identificación y un mensaje de "error" apareció en la pantalla.

- Dale enter- sugirió Bach -quizás nos deja intentar de nuevo.

- Ok. que?!- exclamó Handel -nos dio paso, mira! Ahora nos pide el password.

- Dale enter otra vez! Es un aujero, seguro.

Bach tenía razón. La máquina tenía un error de configuración un bug (un hueco de seguridad) en la jerga. Los VAXbusters estaban dentro del sistema. Steffen Weihruch, espías y adolescentes eran demasiadas personas dentro del sistema y las investigaciones comenzaron. La primera pista surgió en 1986 en los laboratorios de investigación espacial de Lawrence Berkeley, California. Clifford Stoll, astrónomo empleado de los laboratorios, denunció que personas no autorizadas habían intentado obtener datos con códigos tales como nuclear, ICBM, Starwars o SDI. En 1987 Roy Omond, director de un sistema VAX en Heidelberg, descubrió los verdaderos nombres de los VAXbusters y los

[38] Virtual Memory System, "Sistema de Memoria Virtual" es un método de administración de la memoria que ejecuta el Sistema Operativo, consiste en desocupar localidades en el módulo RAM para escribirlos en un archivo dinámico en el disco duro. Los programas y aplicaciones del usuario pueden disponer así de grandes montos de memoria para sus procesos. A esta dinámica de intercambio de espacios RAM/Disco, se

publicó en un mensaje al resto de los usuarios de la red europea SPAN. Cuando Bach y Handel se vieron descubiertos les ganó el miedo y recurrieron al consejo de los miembros del Chaos, de quienes eran amigos. Por intermedio de un tercero, los hackers profesionales consiguieron que los servicios secretos alemanes en conjunción con los técnicos de la Digital Equipment acordaran una entrevista con los chicos bajo promesa de no tomar represarías legales. Los VAXbusters prepararon un informe minucioso con todas las cerraduras que estaban en su poder: habían entrado en diecinueve centros de la NASA a través de SPAN, entre los que Philips no figuraba. Ya en la reunión demostraron ante cámaras como lo hacían e instalaron un "parche" para arreglar el agujero de seguridad. El video se difundió por la televisión y la investigación quedo prácticamente cerrada. Pero Philips de Francia estaba dispuesta a perseguirlos (también a los del Chaos), convencida que eran los responsables del espionaje en la empresa. En SECURICOM, la feria internacional de seguridad en comunicaciones que se realiza en Francia, detuvieron a Steffen Wernery, quien se había ofrecido para conferenciar, y lo mantuvieron encarcelado tres meses, tiempo que demoraron las autoridades francesas en aceptar su declaración de inocencia. La confusión de Phillips era comprensible. Tanto los VAX busters como Weihruch y el grupo de espías usaban las mismas técnicas para hackear, en tanto Wernery sólo había sido mediador y quien dio la cara a las explicaciones televisivas después de la conmoción que causó el caso de Bach y Handel. Mientras Wernery sufría cárcel en Francia, los responsables del espionaje seguían en Alemania, sanos y salvos de la legislación francesa, pero preocupados por los allanamientos y arrestos de miembros del Chaos y por la creciente presión de la KGB, que se endurecía en los pedidos y plazos.

En el verano de 1988, Pengo y Hagbarg pensaron sacar provecho de una amnistía en la ley de espionaje para aquellos que colaboraran con los investigadores y no registraran antecedentes. Amparados en ella se declararon espías y fueron testigos de cargo en el juicio contra Hess y Kahl. Alexander Prechtel, quien era portavoz de la fiscalía federal alemana, confirmo a través de la cadena de radio y TV NDR "el

le denomina "Swapping". En el entorno Windows, el archivo dinámico se llama win386.swp http://es.wikipedia.org/wiki/VMS

desmantelamiento de la red" y anuncio la "detención de tres de sus miembros que operaban en la RFA (República Federal de Alemania) y eran coordinados por dos agentes de la KGB". Hess fue condenado a veinte meses de prisión y una multa de diez mil marcos; Kahl a dos años y tres mil marcos, pero ambas sentencias se sustituyeron por libertad condicional. Dos meses después del juicio el cuerpo de Hagbard apareció carbonizado. El hecho nunca pudo aclararse y fue cerrado como suicidio.[39]

Los delitos informáticos se incrementan en medida a las posibilidades de las personas de adquirir computadoras y otras tecnologías, mientras más bajan los costos de computadoras mayor cantidad de gente se incorpora al uso de las nuevas tecnologías. Los países industrializados tiene pleno acceso a la tecnología de las computadoras, los niños comienzan su aprendizaje del uso de las PC en la escuela primara, y la gente tiene acceso gratis a computadoras en librerías o universidades, también pueden rentar una computadora en un café Internet, la mayoría de la gente sabe como enviar un correo o como descargar un archivo de otra computadora a través de la Internet, esto no requiere tener grandes conocimientos en el uso de las computadoras. 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.

Como lo han hecho ya desde hace nueve años, el Computer Security Institute y el FBI hacen un estudio en la seguridad de las nuevas tecnologías de empresas en los Estados Unidos. A través de una gran encuesta se ha podido extraer interesante información acerca de las tendencias de la seguridad informática con los años. La encuesta realizada entre casi 500 empresas estadounidenses representativas de todos los sectores, se toma como punto de referencia ante la seguridad informática y las empresas. A lo largo de casi una década cada documento ha sido testigo de un cambio de actitud hacia el problema que supone una Internet cada vez más hostil, y hoy en día

[39] Roberti Raquel, Bonsembiante Fernando, *LLANEROS SOLITARIOS, HACKERS, LA GUERRILLA INFORMATICA*, pp.45-50

revela que la seguridad es una parte prioritaria del presupuesto de toda compañía. Por ello en el 2004 vuelve a bajar el índice de ataques exitosos, que viene descendiendo desde 2001. Aun así, el 53% de los encuestados declara haber sufrido un acceso no autorizado a sus sistemas. El cambio más sorprendente se observa en el número de ataques provenientes del exterior e interior de la red corporativa, que si bien en el año 2003 correspondían al 20 y al 80% respectivamente, en el año 2004 prácticamente se igualan.

Los virus suponen el problema más común, afectando al 78% de los encuestados. De hecho este problema es el que más cuesta a las compañías, seguido del robo de información confidencial, abusos desde el interior y las brechas en redes inalámbricas. Del estudio también se desprende que los ataques DoS (denegación de servicio o "denial of service") siguen siendo de los ataques más dañinos económicamente para muchas de las empresas que se incluyeron en esta encuesta. La encuesta también quería saber si las compañías realizaban una investigación proactiva para la búsqueda de vulnerabilidades antes de que fuesen descubiertas por otros, a través de auditorias de seguridad. El 82% ya realizaba este tipo de ejercicios.[40]

1.3 SITUACIÓN ACTUAL

El avance que tuvo la tecnología de la información a finales del siglo pasado y la que ha desarrollado en los primeros años de éste, ha sido impresionante, los dispositivos de comunicación son cada vez más potentes, más pequeños y más económicos. La mayoría de las profesiones han tenido que adaptarse al uso de estas tecnologías de la era digital, ya que resulta una herramienta indispensable para la competitividad de las empresas, pero también la policía se tiene que actualizar, dado que las nuevas tecnologías de comunicación han traído consigo formas de cometer delitos, las cuales antes eran inimaginables.

[40] http://www.it-analysis.com/article.php?articleid=12122 (12/08/04)

Como se muestra en las siguientes tablas tomadas de la página del CERT, cada vez son mayores los delitos cometidos usando las tecnologías informáticas.

1988-1989

Año	1988	1989
Número de incidentes reportados	6	132

Tabla 2. Tomada de la página del CERT

1990-1999

Año	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidentes Reportados	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

Tabla 3. Tomada de la página del CERT

2000-2003

Año	2000	2001	2002	2003
Incidentes reportados	21,756	52,658	82,094	137,529

Tabla 4. Tomada de la página del CERT

Estos datos nos arrojan un total de 319,992 incidentes reportados al CERT desde el año de 1988 hasta el 2003.

Las pérdidas económicas que han dejado estos delitos sólo en el año del 2003 se calculan en 660 millones de dólares, según la CSO (Chief Security Officer) que es una empresa encargada de la seguridad en las tecnologías de la información a grandes empresas en los Estados Unidos, en cooperación con el Servicio Secreto de los Estados Unidos y el CERT realizaron una investigación, y obtuvieron los siguientes datos, reportan un incremento muy importante de delitos por medios electrónico, realizaron una

encuesta a empresas de Estados Unidos en el año 2003, el 43% de los encuestados, reportan un incremento en los delitos informáticos y las intrusiones, en comparación con el año 2002, el 70% de los encuestados reporta haber sufrido algún tipo de delito informático o intrusión, y solo el 30% dice no haber sufrido ningún tipo de incidente. Cuando se les preguntó a las empresas que tipo de perdidas habían sufrido a causa de los ataques por medios electrónicos durante el año 2003, el 56% reportó perdidas operacionales, el 25% perdida en los estados financieros y el 12% dijo haber tenido otro tipo de problemas. Pero el 41% de los encuestados dijo que no contaban con un plan formal de respuesta a incidentes y tampoco para reportar con las autoridades en caso de sufrir un ataque.

Dentro de la encuesta realizada, se les preguntó únicamente a las empresas que fueron victimas de algún delito informático, si los ataques recibidos se llevaron acabo desde dentro de la misma empresa o desde afuera, el 30% dijo no saber si los ataques se habían llevado a cabo desde adentro o fuera de la empresa, de los que si sabían quien los había atacado el 71% dice que los ataques fueron perpetrados desde afuera de la empresa y sólo el 29% dice que los ataques se llevaron acabo desde adentro, lo cual nos muestra el incremento de los ataques llevados acabo en forma remota.[41]

El investigar estos delitos, que día a día son más sofisticados, y recolectar toda la evidencia necesaria para presentar el caso ante las autoridades correspondientes, tiene que ser la tarea de policías completamente capacitados en el área, con los suficientes conocimientos para presentar evidencia contundente, pero desafortunadamente, en México, los cuerpos policiales no cuentan con la suficiente capacidad para atacar este tipo de problemas, existen algunas divisiones dedicadas a investigar este tipo de delitos, como lo es la policía cibernética, está es una división perteneciente a la PFP (Policía Federal Preventiva), la PGR (Procuraduría General de Justicia) cuenta con un cuerpo de peritos forenses en informática, de los cuales hablaremos más adelante en este mismo capituló, pero el apoyo que tienen los mismo y el alcance legal que tienen los mantiene muy limitados, además de que el número de integrantes en estas áreas es muy reducido.

[41] http://www.cert.org/about/ecrime.html

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 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 requería el FBI para hacer sus investigaciones[42], la informática forense tiene como objetivo identificar, preservar, analizar y presentar toda evidencia digital de manera que sirva para seguir un proceso judicial.

La informática forense forma parte de la seguridad en cómputo, la seguridad en computo 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 computo busca prevenir cualquier ataque o intrusión no autorizada a un sistema de computo, hay dos diferentes formas de accionar 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 computo, 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 quien y como 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.

[42] http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm#Examining%20Computer%20Evidence

¿Cuándo surge la informática forense?

En 1984 el FBI crea el "Computer Analysis and Responce Team" (CART) para recuperar evidencia desde las computadoras. Pero es hasta 1991 que el CART comienza a operar completamente.[43]

Desde 1984, el laboratorio del FBI y otras agencias gubernamentales de los Estados Unidos, que siguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional, desde 1998 cuentan con un sistema llamado "Carnivore", este sistema se encarga de analizar la Internet en busca de actos terrositas, hackers, espionaje, pornografía infantil y fraudes en línea, y actualmente no requieren de ningún permiso legal, apoyándose en la Ley de Procedimientos relacionados con Información Clasificada, puede ser usado en la investigación de alguien en concreto, con este sistema pueden ver lo que un sujeto hace en la Internet, pueden leer su correo electrónico y también interceptar su Chat, sin que el investigado se de cuenta.

La NW3C (Nacional White Collar Crime Center) creado en 1980 por el gobierno de los Estados Unidos de Norteamérica, auxilia a otras agencias como el FBI, en la investigación de fraudes financieros y delitos donde se involucra la tecnología, pero es hasta el año 2000 que comienza a tener mayor presencia en los delitos electrónicos, cuentan con un laboratorio de informática forense que a la vez funciona como escuela o centro de capacitación.[44]

También hay otra agencia que trabaja conjuntamente con el FBI y la NW3C es la IFCC (Internet Fraud Complaint Center) se encarga de trabajar con victimas y fraudes en Internet, cuentan con un sistema para levantar reportes en línea y ellos hacen la investigación en base a los datos entregados por la victima

[43] http://www.fbi.gov/libref/historic/history/rise.htm(09/08/04)
[44] http://www.nw3c.org

Es precisamente Estados Unidos quien empieza a detectar los primeros delitos informáticos, ya que es en este país donde las computadoras tienen su mayor auge, es por ello que se ven en la necesidad de invertir en investigación que los ayude a frenar estas actividades delictivas.

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

El 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.[45] 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 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.[46]

[45] http://www.dcfl.gov/dc3/dc3.htm(15/09/04)
[46] http://sanfrancisco.fbi.gov/pressrel/2005/svrcfl010505.htm

También existen en los Estado Unidos otras agencias como, The Defense Cyber Cryme Institute (DCCI), Major crimes and Safety (DCFL) y The Defense Computer Investigations Training Program (DCITP).[47]

Además de los organismos ya mencionados existen alrededor del mundo diversas organizaciones dedicadas a la investigación de informática forense como son:
European Network of Forensic Science Institute http://www.enfsi.org/aboutenfsi/
National Institute of Forensic Science (Australia) comienza a operar en febrero de 1998 en Melbourne http://www.nifs.com.au/
National Institute of Justice/UCF (USA) Ubicado en la Universidad Central de Florida http://ncfs.ucf.edu/home.html
Information Security and Forensics Society (HK) fundada en Mayo del 2000 en Hong Kong http://www.isfs.org.hk/

Finalidad de la informática forense

La informática forense tiene por objetivo 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.

Se puede decir que la informática forense se compone de la obtención, análisis y procesamiento de la información digital para que pueda ser usada como evidencia en

[47] http://www.dcfl.gov/dc3/home.htm(15/09/04)

juicios civiles, criminales o administrativos. Actualmente casi ningún abogado usa evidencia digital en las cortes porque no la ven como una evidencia tangible, pero este tipo de evidencia puede ser crucial en muchos casos legales.

1.4 DELITOS INFORMÁTICOS E INFORMÁTICA FORENSE 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.[48]

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.

[48] http://www.ssp.gob.mx/application?pageid=pcibernetica (18/12/2004)

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 ciberterrorismo 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 18 sitios relacionados con el robo o alteración de información, 163 de fraudes, dos de clonación de señal satelital, dos de tarjetas de crédito y siete de ciber-terrorismo, estos datos se pueden verificar en la siguiente dirección de Internet http://ventana.presidencia.gob.mx/9/tranquilidad.php.

La misión de la policía cibernética de la PFP 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 la policía cibernética de la PFP, es rrealizar 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.[49]

La PGR (Procuraduría General de La República) 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.[50]

[49]http://www.ssp.gob.mx/application?pageid=pcibernetica_sub_2&docName=¿Qué%20hacemos?&docId=419 (10/08/04)

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.

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.[51]

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 la recopilación de evidencia digital. LIF ofrece servicios de análisis, investigación y prevención de conductas delictivas o irregulares en 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.[52]

1.5 PERFIL DE UN INFORMÁTICO FORENSE.

Después de revisar información en Internet y libros especializados en informática forense, se puede decir que la base del informático forense se fundamenta en la aplicación de conocimientos técnicos y procedimientos legales, en las situaciones donde

[50] http://wwwhtm.pgr.gob.mx/homepage.htm(13/09/04)
[51] http://www.state.gov/p/wha/rls/rpt/26214.htm (18 /08/04)

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.

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[53]:

- 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 investigación.
- 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.

[52] http://www.lif-gc.com/(13/09/2004)
[53] Debra Littlejohn, *Scene of the Cybercrime*, Syngress 2002,pp 136-139.

- 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.

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: solo 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, conocer las debilidades de estos mismos.

La informática forense es una ciencia relativamente nueva, y los esfuerzos por profesionalizar esta rama a llevado a asociaciones internacionales como lo son la IACIS

International Association of Computer Investigative Specialist, y la High Technology Crime Netwok, ubicadas en Estados Unidos, a desarrollar programas de capacitación, especialización y certificación para informáticos forenses, son programas que buscan la estandarización internacional de este tipo de investigaciones forenses, ya que los sistemas informáticos funcionan igual en todo el mundo, con algunas pequeñas diferencias pero en general son iguales.

La IACIS ofrece la certificación internacional denominada CFEC - Computer Forensic External Certification, la cual exige que el aspirante a obtener la certificación tenga que realizar un examen mostrando los siguientes conocimientos.[54]

- Identificación y recolección de evidencia en medios magnéticos
- Comprensión y práctica en procedimientos de revisión y análisis forenses
- Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática
- Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.
- Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación.
- Comprensión de los diferentes sistemas de archivos asociados con sistemas operacionales, particularmente FAT de Microsoft.
- Conducir de manera detallada recuperación de datos de todas las porciones de un disco.
- Comprensión de como tener acceso a los archivos temporales, de caché, de correo electrónico, de web, etc.
- Comprensión de los aspectos básicos de Internet.
- Comprensión de técnicas de rompimiento de contraseñas.
- Comprensión general de los temas relacionados con investigaciones forenses.

[54] http://www.cops.org/External%20Certification.htm(05/04/2005)

Un documento publicado por la IOCE (International Organization on computer Evidence)[55] y elaborado por el Dr. L.W. Russell, secretario de la IOCE, dice que para la especialización de informática forense se deben de contemplar los siguientes conocimientos[56]:

- Procesamiento AVI (Audio, Video e Imágenes)
- Funcionamiento de PDA (Personal Digital Assistant) como Palm´s Pilot y teléfonos celulares.
- Conocimientos en criptografía, la criptografía es el arte y ciencia de cifrar y descifrar datos.
- Ocultación de datos, como la esteganografia, es una rama de la criptografía que trata la ocultación de mensajes, para evitar que se perciba que existe algún tipo de mensaje.
- Conocimiento en Redes, tecnologías inalámbricas y seguridad en redes.
- Tecnologías emergentes, como sistemas biométricos, capaces de censar parámetros físicos.
- Manejar ampliamente varios sistemas operativos como, Mac OS, Windows, Linux, Unix, Etc.
- Fundamentos en procedimientos legales.
- Destreza para el análisis y presentación técnica.
- Capacidad de mostrar la evidencia ante un Juez.

En este capítulo hemos revisado como es que nace la informática forense, la necesidad que llevó a crear un cuerpo especializado dentro del FBI dedicado a investigar los delitos informáticos en la década de los 80´s, quienes han sido los más destacados exponentes de la corriente hacker a causa de los cuales se ha tenido la necesidad de crear sistemas de seguridad para proteger las redes y salvaguardar la información de empresas y algunos otros organismos, todo esto a llevado a crear una rama de estudio dentro de la computación llamada seguridad informática la cual se subdivide en varias líneas de

[55] www.ioce.org (05/04/2005)
[56] www.ioce.org/2002/ioce_tksa.html(05/04/2005)

especialización y es donde encontramos la informática forense, además de que grupos policiales de nuestro país se han visto en la necesidad de incorporar dentro de sus organizaciones a equipos especializados en este tipo de delitos y a los cuales les llaman perito informáticos, es evidente que el mundo tecnológico que estamos viviendo trae muchas comodidades pero también trae consigo muchas responsabilidades las cuales hay que tratar antes de que se conviertan en un problema.

Capítulo II. Investigación Forense

II. INVESTIGACIÓN FORENSE

En este capítulo estudiaremos el objetivo de la informática forense. Revisaremos cómo se lleva a cabo una Investigación forense, los puntos que se deben de tomar en cuenta al iniciar una investigación y procesos a seguir en la búsqueda de evidencia digital. Estudiaremos algunos programas que se utilizan en la investigación forense de los sistemas de cómputo.

2.1 COMO HACER UNA INVESTIGACIÓN EN INFORMÁTICA FORENSE

La función del informático forense es recolectar evidencia en medios digitales y determinar si el sospechoso cometió un delito o violó las políticas de la empresa. Si la evidencia apunta a que el sospechoso cometió un delito, es hora de prepara una demanda en su contra. Debemos tener en cuenta al realizar una investigación, que lo que estamos buscando es evidencia digital, que sirva como prueba en un proceso judicial, por esta misma razón debemos ser muy cuidadosos con la información que estamos manejando, ya que puede ser determinante para inculpar al sospechoso.

Antes de comenzar la investigación es recomendable elaborar un plan de trabajo, en el cual se deben incluir los pasos a seguir durante la investigación, siempre buscando obtener resultados favorables, teniendo en cuenta, que pueden presentarse situaciones imprevistas durante el proceso de la investigación, las cuales requerirán ajustar el plan, una vez conceptualizado y elaborado el plan de trabajo, podremos desarrollar nuestra búsqueda de evidencia con un seguimiento lógico y estructurado, evitando así perder el objetivo durante todo el proceso de la investigación, un plan de trabajo puede ser generalmente como el que sigue, aunque en algunas ocasiones puede variar por los requerimientos y necesidades del mismo caso a investigar.

La siguiente tabla muestra la metodología propuesta en esta tesis para llevar acabo una investigación de informática forense, cabe señalar que la siguiente es una metodología general y puede ser acoplada para casos específicos. En la siguiente tabla solo se ve una breve explicación de lo que se pretende conseguir en cada punto de la metodología, más adelante se explica a detalle el objetivo de lo siguiente.

Metodología	Objetivo a cumplir
Limitar el acceso al área donde se encuentra el equipo que evidentemente fue dañado.	Evitar que gente ajena a la investigación, pueda alterar el equipo involucrado
Hacer un estudio preliminar del caso que se va a investigar	Tener un panorama general del medio en el que se va a trabajar
Hacer un enfoque preliminar sobre el caso a estudiar	Conceptualizar la orientación que se le dará a la investigación
Crear un diseño detallado	Diseñar una lista detallada de los pasos a seguir durante la investigación y calcular tiempos de ejecución de cada uno
Identificar la evidencia digital	Saber que equipos se encuentran involucrados en el delito, los cuales serán analizados
Obtener y copiar los discos donde se encuentra la posible evidencia	Tener los respaldos suficientes para analizar y no dañar ni alterar los dispositivos originales
Preservación de la evidencia digital	Buscar que la evidencia sea valida en un proceso legal, demostrando que no se ha alterado la información original
Identificar los riesgos	Poder generar una lista en base a anteriores investigaciones realizadas, que ayude a una mejor fluidez de próximas investigaciones
Eliminar o minimizar los riesgos	Prever los posibles problemas que se pueden presentar y buscar la solución
Verificando el esquema de la investigación	Analizar las decisiones que se han tomado y los pasos que han sido completados
Analizar y recuperar la evidencia digital	Determinar el equipo y técnicas a emplear para extraer la información contenida en medios digitales
Investigar los datos recuperados	Analizar los datos recuperados en busca de evidencia para determinar los hechos y el

	culpable
Hacer un reporte del caso	Elaborar un reporte detallado de lo que se hizo y obtuvo en la investigación
Criticar la investigación	Determinar si las decisiones tomadas en la investigación fueron las correctas.
Presentación de la evidencia digital	Que el reporte que entregamos sea claro y contundente para el proceso judicial.

Tabla 5.

- **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 tenemos que asegurar que no será modificado 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.

- **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[57]. 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, Jaz, 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

[57] Debra Littlejohn Zinder, *Scene Of The Cybercrime Computer Forensic,* HandDbook , p.11

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 aun 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 computo 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 tenemos en este momento. Esto sirve para hacer una lista estándar de los problemas que con mayor frecuencia se pueden ir presentando.

- **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.

- **Analizar y recuperar la evidencia digital.** Usando software especializado, herramientas y cualquier otro recurso que sea necesario para superar los riesgos y obstáculos que se presenten al examinar el disco y demás dispositivos en búsqueda de la evidencia digital.

- **Investigar los datos recuperados.** Analizar la información recuperada desde el disco, incluyendo archivos existentes, archivos borrados y el correo electrónico,

organizar la información obtenida de tal forma que nos ayude a probar la inocencia o culpabilidad del sospechoso. El análisis de la evidencia digital, la obtención, procesamiento e interpretación de los datos son considerados como las partes clave en una investigación de la informática forense. Una vez obtenida la evidencia digital, se lleva a cabo un proceso para depurar la información, que sea clara y comprensible al presentarla ante un juez o simplemente para la persona que haya contratado los servicios de informática forense, esto es un reporte escrito de todo el proceso de investigación que se llevó a cabo y con las respectivas conclusiones, en las cuales se debe incluir recomendaciones para evitar futuros problemas por la misma situación.

- **Hacer un reporte del caso.** Escribir un reporte completo y detallado de lo que se hizo y lo que se encontró durante la investigación.

- **Criticar la investigación.** Hacer una auto evaluación, esto es un punto que deben tener todos los profesionales. Después de completar la investigación, hay que conceptualizarla, identificando las decisiones y acciones correctas que se tomaron, de que forma pudo ser mejor y como calificamos nuestra participación en el caso.

- **Presentación de la evidencia digital:** Este paso consiste en presentar la evidencia de la mejor manera, esto es que a la vista de los evaluadores de la evidencia, no llegue a ser dudosa la integridad de lo que se les presenta, asimismo las evaluaciones del perito y la autenticidad de los procesos empleados en la obtención de la evidencia se presentaran ante la autoridad legal correspondiente. Algo que diferencia a la informática forense de cualquier otra especialización de tecnologías de la información, como pueden ser las telecomunicaciones, es cumplir que el proceso y desarrollo que nos lleve al final de la investigación debe derivarse de un proceso que sea legalmente aceptable. Por esto mismo, se debe tener claro cuáles son los procesos o requisitos

necesarios que exige la ley para hacer válida la evidencia recolectada durante el proceso de investigación y peritaje. De no hacerlo así, ó no estar conciente de ello, puede hacer que la evidencia obtenida se considere inadmisible, ó en el mejor de los casos, con poca credibilidad.

El contar con un plan de trabajo sistematizado muchas veces facilita el descubrir la información que es crucial para el caso. Eventualmente si no se cuenta con un esquema de trabajo sistematizado se puede llegar a sentir que se cuenta con demasiada información, especialmente sino esta organizada lógicamente.

2.2 ESTRATEGIA DE UN INVESTIGADOR 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 cosas 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.

El informático Forense 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 nos muestre en que esta trabajando la computadora en ese momento, una vez que

el monitor nos 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 tenía 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 aun 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, ¿Cómo son autenticados los usuarios ante los servidores del sistema informático donde ocurrió el fraude u otro delito?¿Hay 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?¿Cómo se rastrean los acontecimientos de acceso y cómo se almacenan los registros para consultas posteriores?¿Cuál es el proceso de verificación de las transacciones de información?¿Cómo 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 encrypcion 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.

Recolección de evidencia

Una vez que el investigador conoce los aspectos generales del ambiente informático de la empresa en cuestión, puede comenzar la investigación. El objetivo del investigador, es descubrir evidencia que puede ser usada para convencer a un jurado o al juzgador, que para cometer el delito, sólo el sospechoso podría haber utilizado la combinación de contraseñas, identificación de usuario y otros elementos como el registro de acceso. El primer paso para esa finalidad es que la investigación tenga una base forense sólida, lo cual significa que los pasos de la investigación deben estar bien documentados y de ser

necesario se deben poder repetir. El investigador se debe asegurar que la evidencia sea conservada integra en su condición original.

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 sería 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 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 Palm 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 tenemos 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 debemos preguntarnos, ¿cómo las Palmtop y computadoras portátiles son usadas y que datos son los que contienen?

Hacer una lista de los archivos y dispositivos que deben ser analizados

Archivos de datos:

- Computadora personal de la oficina o estación de trabajo.
- Computadora portátil.
- Computadora de casa.
- Computadora del asistente personal, secretaria o ayudantes.
- Organizador personal.
- Servidores de la red/ mainframes/ mini-computadoras.

Cintas de respaldo:

- Respaldos del sistema (mensual, semanal y los más actuales).Respaldos de recuperación para desastres (almacenados en el site).
- Respaldos personales (revisar disquetes y otros dispositivos portátiles).

Otros recursos de almacenamiento de datos:

- Cintas de archivos.
- Remplazó o cambio de unidades de almacenamiento.

- Discos floppy y cualquier otro dispositivo portátil de almacenamiento (CDs, Zip cartuchos).

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 tendremos: cintas de respaldo, disquetes, CD's, y algunos otros. Debemos asegurar la integridad de la evidencia que tenemos, 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 nos 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, debemos 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.

2.3 MANEJO DE LA EVIDENCIA DIGITAL

En caso de que sea necesario transportar la evidencia a un laboratorio para un mejor análisis, debemos 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.

- Que la información no sea alterada
- 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 criticas. 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. Y tercero, la copia creada debe ser idéntica al original sin 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 corresponda al número asignado cuando se realizó el análisis.
- Verificar que todos los archivos en la lista del directorio aparezcan en las copias restauradas.
- Asegurar toda la evidencia

2.4 HERRAMIENTAS DE ANÁLISIS FORENSE

Existe en el mercado software especializado en el análisis forense de computadoras, a continuación nombraremos algunos de estos programas y su aplicación, posteriormente se describirá a detalle el funcionamiento de algunos de ellos.

- **AIDA32,** analiza el sistema, trabaja sobre plataformas Windows y soporta los siguientes sistemas operativos: Windows 98, Millenium, 2000 y XP.[58]
- **Encase** es un programa de análisis forense de datos diseñado para Windows. Es una buena herramienta que permite hacer una búsqueda de datos de forma simple y versátil, mantiene de forma íntegra todos los datos que se están analizando sin corromperlos.
- **Handy Recovery,** es un programa de recuperación de datos que han sido borrados de medios magnéticos.
- **The Coroner´s Toolkit,** es una suite de aplicaciones que contiene la captura de inores, recuperación de archivos, visualiza ficheros y directorios, en general se puede hacer una autopsia de equipos dañados, esta orientada a sistemas Unix.
- **Visual Route,** este programa sirve para rastrear direcciones IP, URL´s y también de correo electronico.
- **Pasco**, este programa sirve para analizar la actividad que ha tenido el explorador de Internet de la computadora ha investigar.

[58] Este software se puede descargar desde la siguiente liga
http://www.softonic.com/file.phtml?&id_file=23346&action=view&view=downloads

- **Vision V1**, es un programa que analiza todos los puertos de la computadora, te dice cuales estan trabajando y que procesos esta llevando acabo.
- **Show in 2.0,** este programa sirve para mostrar claves y contraseñas del sistema.

AIDA32

Es una herramienta de análisis del sistema que busca en las mismas entrañas de la computadora todos sus componentes sin excepción, tanto de hardware como de software, así como los periféricos instalados en la misma. AIDA32 arroja una gran cantidad de información detallada tras el análisis del equipo el cual dura apenas unos cuantos segundos y sirve para identificar los componentes que constituyen el equipo en el cual se trabaja. El tipo de información que arroja es la siguiente, Sistema Operativo, plataforma, versión, service pack, actualizaciones, propietario, licencia, usuarios. Todo el software instalado, incluyendo versión, fecha de instalación, actualización y licencia. Controladores de los dispositivos como tarjeta de video, de sonido, etc. Hace un análisis a todos los componentes electrónicos (Hardware) del equipo donde da toda la información sobre el tipo de placa madre, procesador, memorias, discos duros, unidades de lectura y almacenamiento, periféricos, etc.

De igual forma, no sólo muestra información sobre los elementos de la computadora sino que además, facilita enlaces a la página Web del fabricante para mayor información, o a la página de descarga de controladores.

Figura 2.

AIDA32 trabaja sobre plataformas Windows y soporta los siguientes sistemas operativos: Windows 98, Millenium, 2000 y XP.[59]

Encase

Encase es un programa de análisis forense de datos diseñado para Windows. Aún cuando soporta otras plataformas como UNIX, está basado completamente en plataforma Windows, es una buena herramienta que permite hacer una búsqueda de datos de forma simple y versátil, mantiene de forma íntegra todos los datos que se están analizando sin corromperlos. Desde 1998 este software ha auxiliado a muchos profesionales de la Investigación en la resolución de muchos delitos informáticos, obteniendo la evidencia que ayuda a identificar a quien sea el responsable de cometer el delito, así como también establecer normas en base a la investigación realizada que eviten en el futuro ser blanco del mismo tipo de ataque.

[59] Este software se puede descargar desde la siguiente liga
http://www.softonic.com/file.phtml?&id_file=23346&action=view&view=downloads

Encase usa el algoritmo MD5[60] (Message Digest 5) para hacer una comparación de ficheros[61] y comprobar la integridad de los mismos. MD5 es un algoritmo que se suele utilizar para realizar la comprobación de la integridad de ficheros binarios, por eso se ha establecido como el algoritmo de comprobación estándar en el mundo forense de la computación. Con este algoritmo podemos tener la certeza de que la información que estamos manejando es exactamente igual a la del original y que los ficheros no han sido modificados ni corrompidos en ningún momento, ya que al crear la imagen hace una comprobación directa de los datos copiados. El algoritmo hash MD5 fue creado en 1991 por el profesor Ronal Rivest, y es usado para crear firmas digitales. Encase usa también el CRC (Cyclical Redundancy Checksum) para verificar la integridad de cada bloque de datos. El CRC es una variación del Checksum[62] estándar y trabajan de una forma prácticamente similar, corroborando que los bloques recibidos o copiados, son exactamente iguales a los originales.

El proceso más rápido para copiar la información de un disco es "disco a disco". Para este proceso es necesario tener conectados dos discos duros a la misma tarjeta

[60] MD5 es un algoritmo de cifrado que toma como entrada un mensaje de longitud arbitraria y produce como salida una "fingerprint" (firma digital, huella dactilar digital) o un "message digest" (compendio de mensajes) de 128 bits. El algoritmo MD5 se utiliza para aplicaciones de firma digital, donde un gran fichero debe ser comprimido de manera segura antes de ser cifrado con una clave privada (secreta) bajo un sistema de cifrado de clave pública tal como RSA. En resumen, MD5 es una manera de verificar la integridad de los datos.

[61] Un sistema de ficheros es un conjunto de programas que prestan servicio a los usuarios finales. Cada programa define y maneja sus propios datos. Los sistemas de ficheros surgieron al tratar de informatizar el manejo de los archivadores manuales con objeto de proporcionar un acceso más eficiente a los datos.

[62] Una checksum o función CRC es un mecanismo no criptográfico para detectar errores en las transmisiones y tiene las siguientes características:

- Producir números pseudo aleatorios no criptográficamente seguros.
- Comprobar si un mensaje se corrompió durante la transmisión. Observe que esto se hace como una comprobación extra además de cualquier método criptográficamente seguro de detección de errores. La función de checksum se utiliza sólo en áreas que no requieren criptografía fuerte.

madre, obviamente uno debe ser el disco de donde se quiere sacar la información y el otro debe ser un disco similar sin ninguna informaron almacenada, también es necesario tener un disco de inicio hecho con Encase en un disco 3.5, esté nos ayudara para hacer la imagen del disco.

El proceso para recuperar la información es el siguiente:

- Hacer una conexión IDE al disco duro donde se copiará la información del disco original.
- Iniciar la computadora con el disco de inicio de Encase dentro de la unidad de 3.5.
- Desbloquear todas las unidades instaladas en la computadora, ya que viene bloqueadas de fábrica.
- Oprimir la tecla "A" de adquirir. Seleccionar el disco físico del que deseamos extraer la información.

Figura 3.

1) Escribir la dirección en donde se quiere guardar la información copiada.

Figura 4.

2) Encase te da la opción de llevar un control de los casos que se estudian, así que te pide el número de caso de la nueva investigación, el número de caso lo determina el investigador.

Figura 5.

3) Escribir el nombre del examinador o investigador que llevará acabo toda la búsqueda de evidencia.

Figura 6.

4) Muchos investigadores asignan un número o código a cada pieza de evidencia y lo etiquetan.

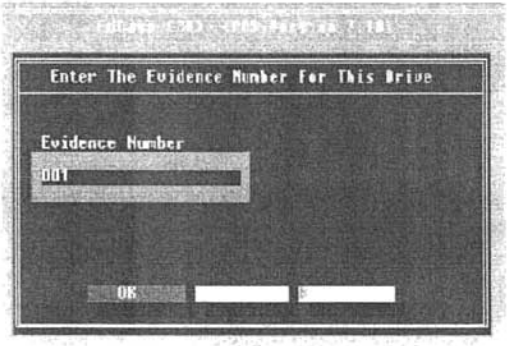

Figura 7.

5) Escribir una pequeña descripción para saber de que se trata, una computadora de escritorio, computadora portátil o diferenciar por nombre de sistema operativo, número de serie, etc.

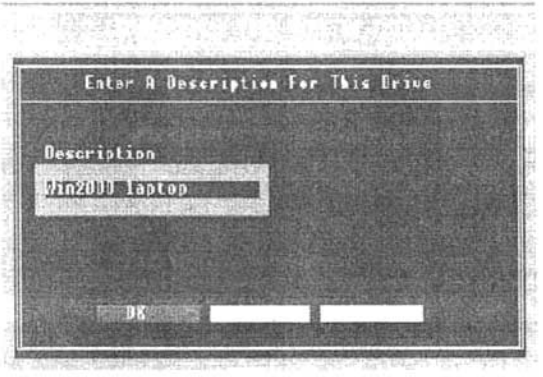

Figura 8.

6) Encase muestra la hora del sistema, para llevar un control en la investigación y saber a qué hora se realizó algún estudio.

Figura 9.

7) La opción de notas sirve para hacer una breve descripción del estado en el que se encontró el objeto de estudio al llegar a la escena del delito.

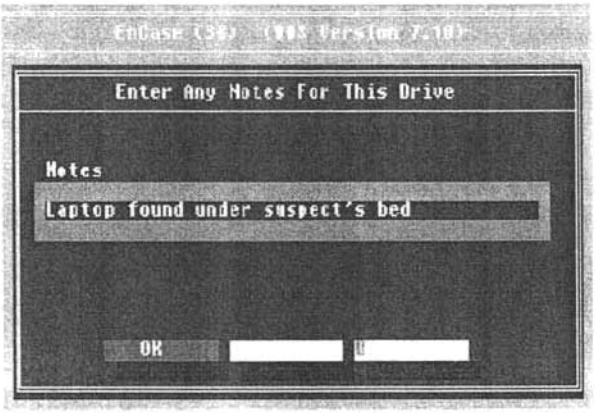

Figura 10.

8) Seleccionar la opción "Yes" si se quiere que los archivos de la evidencia sean comprimidos. La compresión no afecta la evidencia, pero el tiempo que tarda en hacer la copia del original será mucho mayor, aproximadamente cinco veces más.

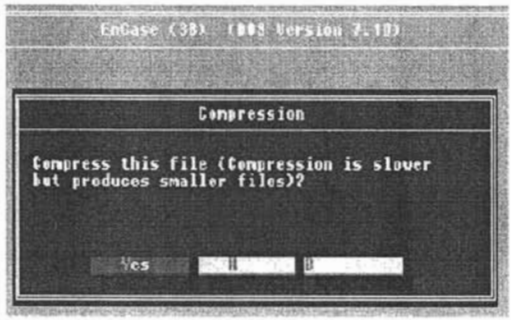

Figura 11.

9) En la siguiente ventana pregunta si se quieres que efectué una función hash MD5 para evaluar los datos durante el proceso para adquirir la evidencia, (es muy recomendable decirle que si, esto le dará mayor integridad a la información).

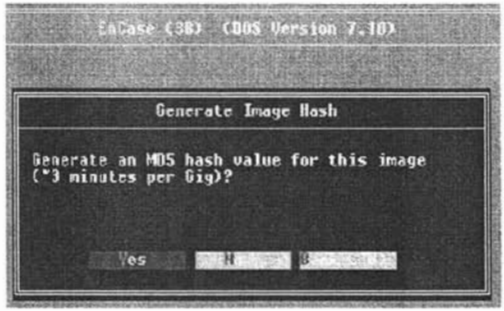

Figura 12.

10) También está la opción de ponerle una contraseña al archivo donde se tiene guardada la evidencia, así, la evidencia será inaccesible por algún otro usuario que no cuente con la contraseña, pero debe recordarse de sólo poner una contraseña que se esté seguro no olvidar.

Figura 13.

11) En esta ventana tenemos que determinar el tamaño que queremos para los bloques de archivos. Encase los pone de 640 MB en automático, esto es para poderlos copiar a un disco compacto en caso de que sea necesario pero el tamaño se puede incrementar hasta 2146MB.

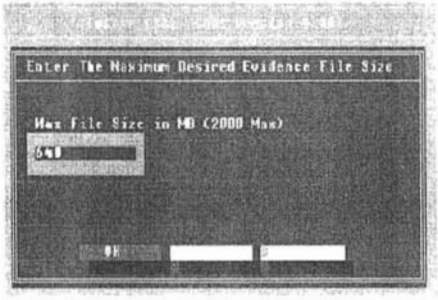

Figura 14.

12) En la siguiente pantalla se puede especificar exactamente cuantos sectores se quieren copiar. Aunque en la mayoría de los casos lo más conveniente es dejar el número de sectores que viene seleccionado en automático por el programa.

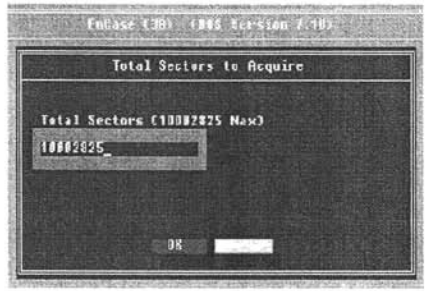

Figura 15.

13) Por último Encase muestra los datos que se vaciaron al programa, para corroborar que todo está bien y se muestra el proceso de copiado.

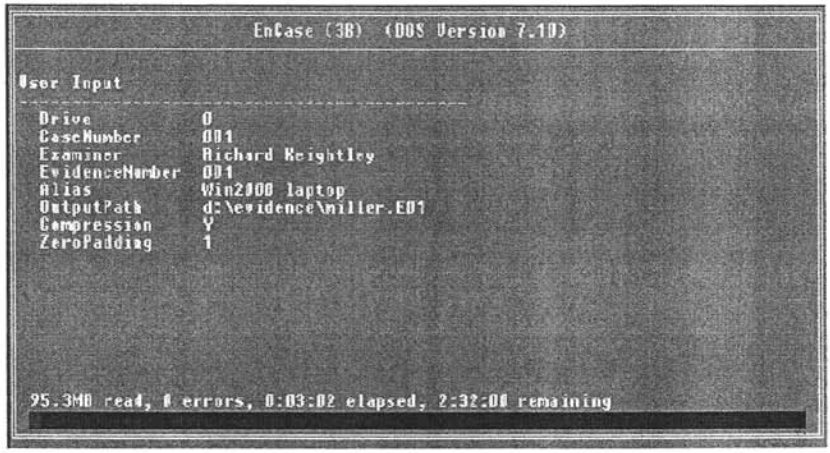

Figura 16.

El copiado de "disco a disco" que se ha explicado, es el método más rápido que hay en Encase para hacer la imagen de un disco que requiere ser analizado. Con este mismo método es posible hacer las copias en Macintosh y Unix, por medio de la conexión IDE, haciendo la conexión del disco directamente a la tarjeta madre.

Una vez terminado el proceso de copiado se debe hacer lo siguiente:

1. Apagar el equipo en donde se hizo la copia.
2. Desconectar el disco original de la computadora y guardarlo en un lugar seguro y libre de estática.
3. Sacar el disco de inicio de Encase que se insertó en la unidad de 3.5 en un principio para hacer la copia.
4. Iniciar la computadora con nuestro disco duro imagen y correr Encase para comenzar a hacer el análisis.

Handy Recovery.

Éste es un software de recuperación de datos con una interfaz de ejecución muy fácil de usar, además de ser una herramienta muy buena para recuperar datos que se hayan borrado desde medios magnéticos, obviamente siempre y cuando no se haya escrito sobre ellos.

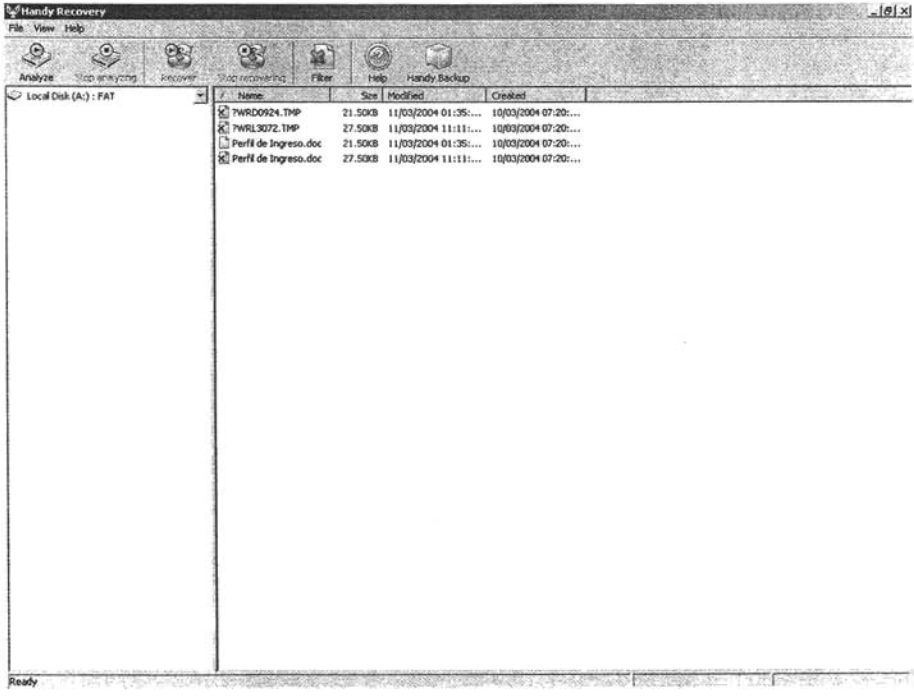

Figura 17.

The coroner's Toolkit.

Ya dijimos que la información que se pierde en una computadora puede ser recuperada. Estudios recientes sobre las implicaciones en seguridad de los "flujos de datos alternativos" en un Windows NT de Kurt Seifried, han mostrado que el sistema de ficheros Windows NTFS permite ocultar datos en "flujos de datos alternativos" conectados a ficheros. Este flujo de datos no se destruye porque proporciona utilidades de borrado de ficheros que prometen una eliminación irrecuperable de la información. Borrar un fichero significa su eliminación "de forma segura" del disco no como habitualmente se eliminan las entradas del fichero de los directorios), de forma que la restauración del archivo se vuelve extremadamente costosa o imposible.[63]

Algunas descripciones de lo que queda en el disco después de eliminar un fichero, cómo puede descubrirse y cómo puede prevenirse son proporcionadas en el artículo "Eliminado Seguro de Datos en Memorias Magnéticas y de Estado Sólido" de Peter Gutmann. El autor recomienda sobrescribir los ficheros varias veces con patrones especiales. En el caso de que se requiera contra adversarios ocasionales, simplemente se debe sobrescribir el fichero con ceros.

Linux no posee flujos de datos alternativos, pero los ficheros eliminados usando /bin/rm todavía permanecen en el disco. Muchos sistemas Linux usan el sistema de ficheros ext2. Al estudiar el diseño del sistema de ficheros ext2 se observan diversos lugares donde los datos pueden esconderse.

En general, si la recuperación se hace poco tiempo después de la eliminación del fichero y la partición es desmontada a tiempo, las posibilidades de completar satisfactoriamente la recuperación son altas. Por el contrario, si el sistema se ha usado mucho, las probabilidades de recuperarlo satisfactoriamente decrecen de forma significativa. Sin embargo, considerando el problema desde el punto de vista forense, la posibilidad de recuperar algo (como una pequeña parte de una imagen ilegal) es bastante

[63] http://his.sourceforge.net/trad/varios/chuvakin/data_hiding.html(22/09/04)

alta. Se ha llegado a encontrar partes de ficheros de años pasados que han sido recuperadas por examinadores forenses.

De tal forma, los ficheros pueden esconderse en el espacio libre. Si muchas copias de un mismo fichero son guardadas y eliminadas, aumenta la posibilidad de recuperar los contenidos usando los métodos anteriores. Sin embargo, debido a las peculiaridades del sistema de ficheros ext2, el proceso sólo puede ser automatizado de forma fiable en ficheros pequeños.

Un examen más detallado al interior del ext2 revela la existencia de espacio de poca actividad. El sistema de ficheros usa partes direccionales del disco llamadas bloques, que tienen el mismo tamaño. El sistema de ficheros ext2 habitualmente usa bloques de 1.2 o 4 Kb. Si un fichero es más pequeño que el bloque, el espacio restante se desperdicia. A esto se le llama espacio de poca actividad (espacio vago). Este es un problema que afecta mucho a los usuarios de Windows 9x con sistema de ficheros FAT16, el cual usa tamaños de bloque de hasta 32Kb, desperdiciando así gran cantidad de espacio al guardar ficheros pequeños.

En una partición Linux de 4Gb, el tamaño de bloque es normalmente de 4Kb (elegido de forma automática cuando se ejecuta la utilidad make2fs para crear un sistema de ficheros). Así se puede ocultar hasta 4Kb de datos por fichero si se usa un fichero pequeño. Los datos serán invulnerables al uso del disco, invisibles al sistema de ficheros y, lo que es más excitante para alguna gente, indetectable por los comprobadores de integridad de ficheros que usan algoritmos de sumas de comprobación y tiempos MAC. Un disquete ext2 (con un tamaño de bloque de 1Kb) permite ocultar datos de la misma forma, aunque en pedazos más pequeños.

Ocultar datos puede usarse para guardar secretos, colocar pruebas (el software forense lo encontrará, pero el sospechoso probablemente no lo hará) y puede que para ocultar herramientas de los comprobadores de integridad (si automáticamente se dividen

los ficheros largos en pedazos de tamaño vago. N del T: es decir, si el comprobador de integridad sólo tiene en cuenta el espacio que ocupa el archivo y no todo el bloque).

Ahora, es necesario descubrir qué hay en las enormes extensiones del disco. Si buscamos cadenas de texto, un simple strings /dev/hdaX | grep 'cadena que necesitamos' nos confirmará la presencia de la cadena en la partición (el proceso necesitará bastante tiempo). Usando un editor hexadecimal en la partición en bruto puede a veces aclarar los contenidos del disco, pero el proceso es extremadamente complicado. Así, el análisis nos lleva al campo del análisis forense de computadoras. Una muy buena herramienta para husmear los contenidos del disco es The Coroner's Toolkit de Dan Farmer y Wietse Venema y su conjunto de herramientas tctutils. El software proporciona funcionalidades para la recolección de datos forenses, recuperación de ficheros, análisis de los contenidos de la unidad en busca de cambios (usando marcas de tiempo en los ficheros), localización de contenidos en el disco (usando números de inodo y de bloque) y para otras tareas forenses.

The Coroner's Toolkit (TCT) es un suite de aplicaciones escritas por Dan Farmer y Wietse Venema para un curso organizado por IBM sobre un estudio forense de equipos comprometidos.

Las aplicaciones más importantes del suite son:

grave-robber - Una utilidad para capturar información sobre inodes, para que luego pueda ser procesada por el programa mactime del mismo toolkit.

unrm y lazarus - Herramientas para la recuperación de archivos borrados (logs, RAM, swap, etc.). Estas aplicaciones identifican y recuperan la información oculta en los sectores del disco duro.

mactime - El programa para visualizar los ficheros/directorios su timestamp MAC (Modification, Access, y Change).

Esta colección de programas sirve para realizar una 'autopsia' sobre sistemas UNIX después de que han 'muerto' completamente.

El funcionamiento de este software se basa principalmente en la recolección de grandes cantidades de datos para proceder a su análisis posterior. Algunos de sus componentes son herramientas como 'ladrón de tumbas' (que captura información), los programas para detectar archivos 'muertos' o 'vivos', así como 'lázaro', que restaura archivos borrados, y otras herramientas que restaura claves criptográficas desde un proceso activo o desde algún archivo.

TCT corre sobre las últimas versiones de SUN Solaris, FreeBSD, RedHat Linux, BSD/OS, OpenBSD e incluso SunOS 4.x. Requiere perl 5.004 o posterior, aunque perl 5.000 es probablemente más adecuado si se está realizando el análisis sobre una máquina diferente. [64]

VisualRoute

Ésta es una herramienta para rastrear direcciones de Internet IP (Internet Protocol), direcciones de páginas en Internet o URL (Uniform Resource Locutor), direcciones de correo electrónico.

Cuando se le proporciona una dirección el programa traza la ruta que lo lleva a la dirección solicitada. Esta tarea muestra cada uno de los siguientes puntos:

- Los saltos que tuvo que hacer para llegar a la dirección pedida.
- Informa si es que se perdió algún porcentaje de los paquetes enviados durante la transmisión.
- Las direcciones IP por las que fue pasando.
- Nombre de los nodos.

64 *http://www.virusprot.com/Nt030804.html (23/09/04)*
cabe señalar que la herramienta TCT es de uso libre y se puede descargar desde el sitio de la siguiente liga http://www.porcupine.org/forensics/tct.html

- Ubicación física de cada unos de los nodos.
- Horario que hay en la zona donde está ubicado el host.
- Tiempo de respuesta en cada host.
- Gráfica del tiempo de respuesta en cada salto.
- Nombre de la red donde se encuentra el host.

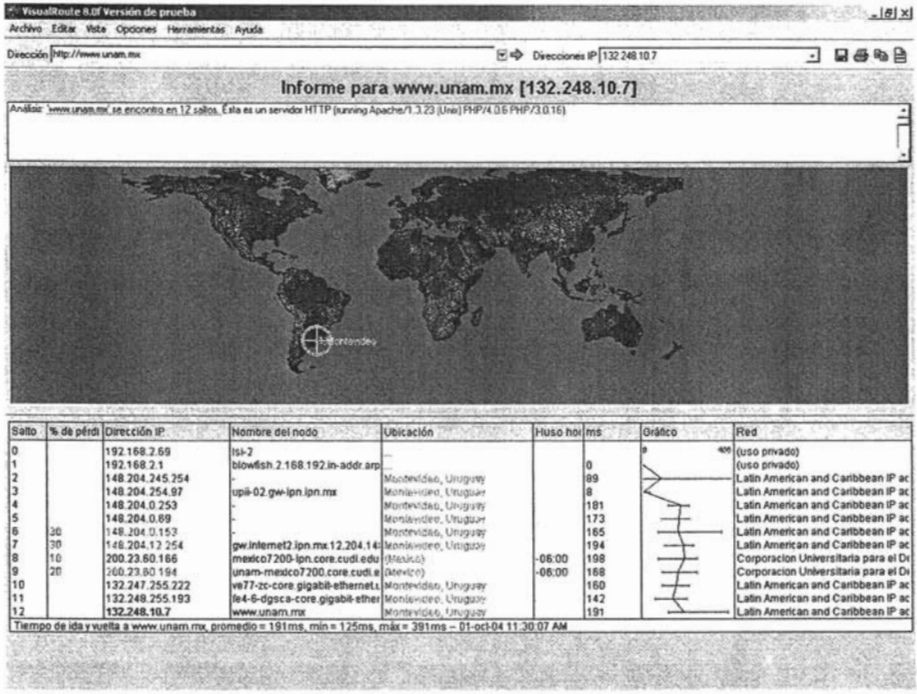

Figura 18.

VisualRoute es una muy buena herramienta para el análisis pues una vez que se han examinado los datos del equipo dañado es posible obtener algunas direcciones IP que podrían ser el origen de los ataques causados al equipo, y con sólo introducir la IP en el programa éste rastreará la dirección en todo el mundo y arrojaría como resultado la ubicación fisica, así como toda la información del administrador de la red en donde se

encuentre el equipo en el que se produjeron los ataques, como se muestra en la siguiente imagen.

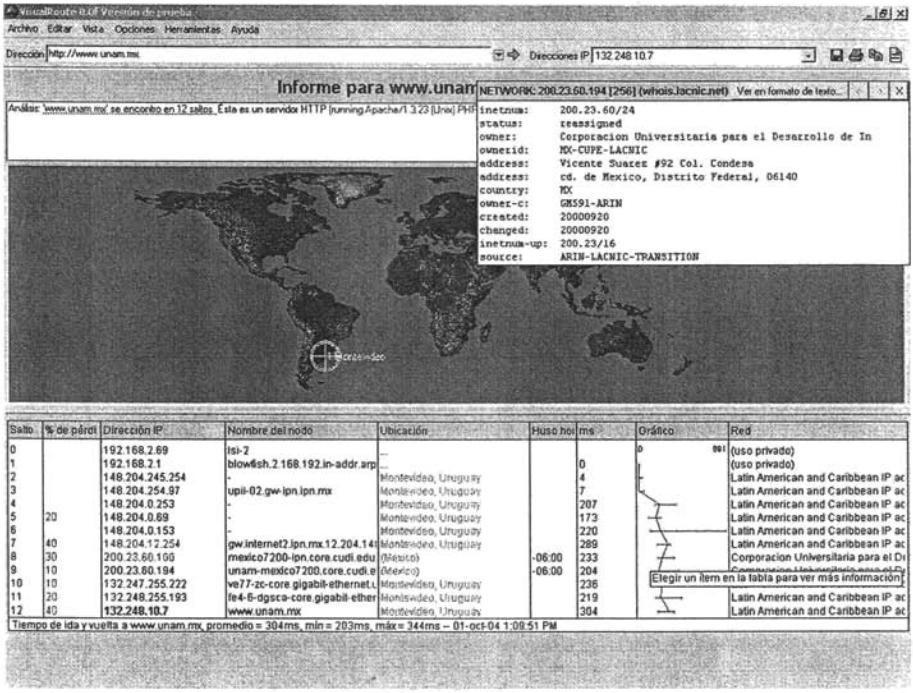

Figura 19.

En realidad, VisualRoute tiene varias herramientas y funciones que nos pueden ayudar en el proceso de investigación para determinar desde el lugar donde se produjo el ataque y, al mismo tiempo, poder llegar a los culpables.

Las herramientas anteriormente revisadas son sólo algunas que se pueden usar durante un proceso de análisis forense de computadoras, aunque se deben de tomar en cuenta los demás aspectos tratados en este capítulo, desde la llegada a la escena del delito, la ubicación y el levantamiento de datos, así como establecer un orden para llevar un buen control en el proceso del análisis de evidencia. Se tiene que garantizar que la evidencia recolectada en el análisis que se hizo a los diferentes equipos y dispositivos

implicados es fiable y verídica, por ello, el proceso de análisis debe estar basado en normas que garanticen el proceso, así como su integridad. Ahora se sabe como es el proceso desde sus partes más elementales hasta algunas opciones relacionadas con el software forense que generalmente se encuentra en la red.

Capítulo III. Derecho Informático

III. DERECHO INFORMÁTICO

En este capítulo definiremos lo que es un delito informático, revisaremos las reformas que se han hecho en las leyes buscando de esta forma evitar el incremento de los delitos informático. Estudiaremos las leyes que más interés tienen para el informático forense.

3.1 ¿QUÉ ES EL DERECHO INFORMÁTICO?

Las Tecnologías de la información han tenido una evolución muy significativa en los últimos tiempos (como ya se ha visto en capítulos anteriores) y su relación con prácticamente todas las ciencias y disciplinas del hombre se ha hecho sentir en una forma notable, el Derecho es una de ellas, la informática se ha hecho su objeto de estudio y se le ha dado el nombre de Informática Jurídica.

Los orígenes de la informática jurídica datan a mediados del siglo pasado en Estados Unidos en 1959, cuando el Health Law Center de la Universidad de Pittsburg comienza a utilizar las computadoras para almacenar información de carácter legal. El sistema fue demostrado posteriormente en 1960, ante la American Association Boreau of Lawyer en la reunión anual en Washington, D.C. esta fue la primera demostración de un sistema legal automatizado de búsqueda de información.[65]

En la década de los sesenta se desarrollaron diversos sistemas similares al ya mencionado. En 1964 la American Corporation of Data Recovery comenzó a vender sistemas de procesamiento de datos legislativos, luego fue la Ohio Bar of Automatized Research (OBAR) y estaba enfocado hacia los abogados litigantes, este sistema tuvo sus inicios en 1967 cuando la barra de abogados del estado de Ohio firmó un contrato con la Data Corporation de Datos en Dayton, Ohio. Los trabajos de este sistema continuaron hacia el año de 1970 por la Mead Data Central, que fue constituida con la fusión de Data

[65] Téllez Valdes, J. "Derecho Informático", Mc graw hill, tercera edición, 2004, pp 18.

Corporation con Mead Corporation. En 1973 la Mead Data Central comenzó a vender el sistema LEXIS como sucesor del OBAR.[66]

En México el estado de Tabasco es el estado con más avances tecnológicos en materia legal, ya que en esta entidad la automatización de sus procesos judiciales esta muy avanzado, cuentan con bases de datos referentes a sus procesos judiciales y muchos servicios gubernamentales en línea, se considera un modelo para llegar a implementarlo a nivel nacional.[67]

En la actualidad las tecnologías de la información son en su conjunto una rama de estudio del derecho, pues como ya hemos visto todo este gran avance en las tecnologías de la información a traído consigo nuevas formas de cometer crímenes y es el Derecho quien se tiene que encargar de regular y dar herramientas a todos aquellos que han sido victimas de algún tipo de delito informático para poder llevar a los responsables ante una corte y proceder legalmente en contra de él o los delincuentes informáticos.

3.2 DEFINICIONES IMPORTANTES DE UN DELITO INFORMÁTICO

A continuación presento las definiciones que dan algunos de los más destacados estudiosos del derecho informático:

Julio Téllez Valdés (México), señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún. Conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas,

[66] http://cibersociedad.rediris.es/congreso/comms/c13penaranda2.htm(09/12/04)
[67] http://www.tabasco.gob.mx/(10/10/04)

antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".[68]

Para Carlos Sarzana (Italia), en su obra Criminalista e Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción criminal, como mero símbolo".[69]

Nidia Callegari (México), define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".[70]

Rafael Fernández Calvo (España), define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española".[71]

María de la Luz Lima (México) dice que el "delito Electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[72]

Tomando la idea de las definiciones anteriores, 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.

[68] Téllez Valdes Julio, Derecho Informatico, p. 48
[69] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm(11/02/05)
[70] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm(11/02/05)
[71] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm(11/02/05)
[72] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm(11/02/05)

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

Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de los datos de entrada:

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 computadora 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.

- Fraude efectuado por manipulación electrónica

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.

- Falsificaciones informáticas

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.

- 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 que se

mencionan a continuación. 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, consideramos, 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.[73]

Según el Dr. Julio Téllez Valdes, asesor de la organización Mundial de Derecho Informático, profesor de derecho en el Instituto Tecnológico y de Estudios Superiores de Monterrey campus Estado de México, y quien es considerado uno de los más destacados peritos en delitos Informáticos en Latinoamérica, este tipo de acciones como lo son los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime)[74], 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.

[73] http://lac.derechos.apc.org/cdocs.shtml?x=8325(29/03/2005)
[74] white collar crime son los delitos cometidos por gente con altos estatus socioeconómico y con preparación técnica o profesional en 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. [75]

Para cometer este tipo de delitos es necesario poseer un perfil que no presenta un delincuente común, es necesario tener un profundo conocimiento en el manejo de los sistemas informáticos, en muchas ocasiones esta clase de delincuentes se encuentra en lugares estratégicos en su trabajo manejando información sensible y valiosa lo cual les facilita llevar acabo el delito.

[75] Julio Téllez Valdéz, *DERECHO INFORMÁTICO, Mc Graw Hill,* 2004, P. 163.

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 a 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.). [76]

[76] Téllez Valdes, Julio. Derecho Informático, Mc Graw Hill pp. 103-104.

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 passwords 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.
- 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.

3.3 SITUACIÓN INTERNACIONAL Y NACIONAL

Los problemas que han traído consigo 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 han desarrollando leyes que castigan a los responsables de los delitos informáticos pretenden que disminuyan los mismos.

Estado Unidos:

Este país implantó en 1994 el Acta Federal de Abuso Computacional, modificando el Acta de Fraude y Abuso Computacional de 1986. Esta ley esta en contra de los actos de transmisión de virus.

Esta nueva ley hace la diferencia entre aquellos que lanzan un ataque en forma temeraria de aquellos que lo hacen con la intención de causar el mayor daño posible. Hace la diferenciación de aquellos que crean virus en dos líneas, la primera

dice: para los que intencionalmente causan un daño por la transmisión de un virus, el castigo es de hasta 10 años en prisión federal más una multa, y la segunda dice: para aquellos que lo transmiten de forma imprudencial, la sanción fluctúa entre una multa y un año de prisión.

También, con respecto a estafas electrónicas, fraudes y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa a la persona que defraude a otro mediante el uso de computadora o red informática.

Alemania:

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

Austria:

Ley de Reforma del Código Penal, promulgada el 22 de diciembre de 1987, en su artículo 148 sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de la elaboración automática de datos, a través de la manipulación del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes llevan acabo este acto utilizando su profesión de especialistas de sistemas.

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.

Francia:

En enero de 1988, dicto la Ley relativa al fraude informático, se contemplan penas de 2 meses a 2 años de prisión y multas elevadas, por la intromisión fraudulenta en sistemas, a quien suprima o modifique datos.

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.

México:

En México, los delitos informáticos se encuentran regulados por el Código Penal Federal, libro segundo, titulo noveno, que se refiere a la revelación de secretos y acceso ilícito a sistemas y equipos de informática, en su capítulo segundo dice:

> Articulo 211 bis 1. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
>
> Articulo 211 bis 2. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código.

Artículo 211 bis 7. Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

3.4 REFORMAS A LAS LEYES Y CÓDIGOS EN MÉXICO

En nuestro país se han creado y modificado algunas leyes que están vinculadas con las tecnologías de la información, están diseñadas para proteger legalmente a cualquier persona o empresa que sea objeto de los delitos informáticos, las siguientes son algunas de las más importantes:

Reformas a la Ley Federal de Protección al Consumidor

El 29 de abril de 2000 se hacen reformas a la Ley Federal de Protección al Consumidor, buscando proteger a los consumidores de productos y servicios en línea, para quedar como sigue:

En el artículo primero fracción VIII hace referencia a la protección de los usuarios en cuanto a compras en línea y transacciones de información, dice:

VIII.- La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

El artículo 24 fracción IX dice:

IX bis.- Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por

esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

El capítulo 76 trata acerca de las obligaciones que tiene el proveedor de servicios o productos en línea, los derechos que tiene el consumidor y delimita las multas a aplicar a los proveedores en caso de no cumplir con lo estipulado en este capítulo.

Artículo 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales.

VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

Artículo 128.- Las infracciones a lo dispuesto por los artículos 8, 10, 12, 60, 63, 65, 74, 76 bis, 80 y 121 serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal.

Reformas al Código Federal de Procedimientos Civiles

En las reformas aplicadas al Código Federal de Procedimientos Civiles el 29 de abril de 2000, se ve una fuerte intención de usar evidencia digital que ayude a la resolución de procesos judiciales, en el mismo se determinan los requerimientos por parte de las autoridades para hacer valida la evidencia digital.

Se adiciona el artículo 210-A al Código Federal de Procedimientos Civiles, en los términos siguientes:

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas

obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta."

Reformas al Código de Comercio

Reformas hechas el 29 de abril de 2000.

Para el comercio en general

Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

Para el comercio electrónico

Artículo 89.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.

Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

I.- Usando medios de identificación, tales como claves o contraseñas de él, o

II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Artículo 91.- El momento de recepción de la información a que se refiere el artículo anterior se determinará como sigue:

I.- Si el destinatario ha designado un sistema de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o

II.- De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información.

Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.

Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo.

Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.

Artículo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes

a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 94.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.

Para los intereses de esta tesis los dos siguientes artículos que siguen son muy importantes pues le da valor probatorio en procesos de comercio, a la evidencia adquirida de las tecnologías de la información inmiscuidas en el asunto.

Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

Artículo 1298-A.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada."

3.5 CÓDIGO PENAL FEDERAL

En estas leyes se pueden enmarcar muy bien muchos de los delitos informáticos más cometidos, como es el caso del fraude que se vera en el Siguiente Capítulo, robustecen los esquemas de seguridad informática a nivel legal con los que se contaba en nuestro país, con estos artículos incluidos en el Código Penal Federal, se puede fincar fácilmente responsabilidad jurídica a los responsables de delitos informáticos.

Acceso Ilícito a sistemas y equipos de informática

Art.211 bis 1 al 211 bis 7 del Código Penal

LIBRO SEGUNDO

TITULO NOVENO REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPITULO II ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Articulo 211 bis 1. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Articulo 211 bis 2. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de

información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código.

Artículo 211 bis 7. Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

3.6 LEY DE INSTITUCIONES DE CRÉDITO

En el siguiente artículo se aprecia el interés que muestran las instituciones de crédito, quienes tratan de poner reglas y medidas legales para las transacciones bancarias, buscando evitar los fraudes por medios electrónicos, sentenciando que la firma electrónica puede tener el mismo valor legal que una firma en papel, como se hace en los contratos tradicionales.

Valor probatorio de documentos electrónicos en legislación diversa

Titulo tercero de las operaciones

Capitulo I de las reglas generales

Artículo 52. Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases para dèterminar lo siguiente:

I. Las operaciones y servicios cuya prestación se pacte;

II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y

III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

3.7 LEY FEDERAL DEL DERECHO DE AUTOR

A continuación se transcriben algunos artículos aplicables a la informática, omitiéndose artículos y capítulos que en forma expresa se refieren a obras de naturaleza distinta a los programas de cómputo y bases de datos.

Capítulo IV

De los programas de computación y las bases de datos

Artículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios

empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104. Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105. El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, concluido el alquiler, y

IV. La descompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107. Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108. Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109. El acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110. El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111. Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114. La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

3. 8 TRATADOS Y ACUERDOS CONTRAÍDOS POR MÉXICO CON OTROS PAÍSES

Es pertinente recurrir y estudiar aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

Tratado de Libre Comercio de América del Norte (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo dos habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos consten en medios electrónicos o magnéticos.

Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, incluso el comercio de mercancías falsificadas.

El Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta nuestros días.

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección u, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o

de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías piratas que lesionan el derecho de autor.

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

Probablemente en nuestro país hoy día se cuente con algunas herramientas legales que nos pueden servir para defenderse legalmente en contra de quien haya cometido un delito informático en contra de algún sistema o equipo de computo, hay algunas leyes que muestran claramente que es un delito perpetrar en sistemas sin autorización y más aun copiar o modificar información, también hemos visto que la evidencia digital esta contemplada dentro del las diferentes leyes y códigos que se han revisado.

Para los fines de este trabajo al artículo 210-A; del Código Federal de Procedimientos Civiles, es muy importante ya que reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología y enmarca los requisitos necesarios para hacer valida esta evidencia. En este artículo podemos encuadrar muy bien las necesidades legales que tienen los informáticos forenses cuando se quiere presentar evidencia digital. Sólo hay un pequeño problema, el cual fue tema de discusión en el Congreso Internacional Derecho y las Tecnologías de la información que se llevó a cabo en el mes de Octubre del 2004, en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, se expuso un caso en el cual, una empresa fue objeto de delito informático y cuando los abogados de

dicha empresa presentaron la evidencia digital recolectada de la investigación que llevaron acabo, el juez al cual se habían dirigido y, quien sería el encargado de llevar acabo el juicio, se declaró incompetente, pues no tenía idea alguna de lo que los abogados le mostraban en ese momento, como evidencia, así pues el juicio no prosperó.

Creo que se tiene que dar solución a este problema, ya que aun cuando en el Código Civil este contemplado la evidencia digital, y la cual es valida, como quedó asentado en párrafos anteriores, los jueces no son capaces de darle pleno valor probatorio, a la misma, por falta de conocimientos técnicos.

Una opción viable que puede funcionar bien es que las mismas instancias legales cuenten con un cuerpo de peritos informáticos certificados, los cuales deberán auxiliar al juez en la toma de algunas decisiones.

Hay otro problema, ¿Qué pasa cuando el delito es cometido en forma remota desde otro país?, pues simplemente no pasa nada, ya que si México no tiene ningún tratado con el país de origen donde se encontraba el delincuente, pues las instancias legales de nuestro país no podrán extraditar ni llevar acabo un juicio.

Capítulo IV. Aplicación de la Informática Forense a un caso de estudio

IV. APLICACIÓN DE LA INFORMÁTICA FORENSE A UN CASO DE ESTUDIO

A continuación se estudia el caso de un fraude bancario y la labor de la informática forense en este tipo de delitos. Se comprenderá cual es la función e importancia de la informática forense estudiando un caso práctico.

4.1 DESCRIPCIÓN DEL CASO DE INFORMÁTICA FORENSE

Todo comenzó cuando los trabajadores del banco sospecharon de un error humano que probablemente había equivocado alguna cifra. Pero el rastro de la evidencia llevó a otra conclusión, un fraude.

Lo que originó la investigación de este caso fue el reporte de una agencia de inversiones filial del banco para confirmar la transmisión al cierre del día, la cual no coincidía con el reporte del banco, los saldos tenían una diferencia de $ 1, 000,000 de pesos. Después de volver a cotejar todos los pagos y movimientos que se realizaron ese día, seguían sin poder encontrar en donde estaba el dinero faltante, solo sabían que ese dinero faltaba del sistema hipotecario del banco, los auditores internos de la agencia de inversión y el banco decidieron contratar los servicios de informática forense.

Con base en el procedimiento y técnicas de investigación en informática forense propuesto en el capítulo dos de la presente tesis, plantearemos el esquema de trabajo y sobre el mismo llevaremos acabo nuestra investigación, aunque hay que hacer un énfasis en que cada caso de estudio tiene sus particularidades y no siempre es posible aplicar ni las mismas técnicas ni el mismo método de investigación en todos los casos. Para nuestro caso de estudio en particular nos veremos sujetos a algunas circunstancias específicas que requerirán moldear nuestra metodología de investigación para obtener los mejores

resultados posibles. A continuación se presenta la metodología propuesta en el capítulo dos del presente trabajo, del cual tomaremos los puntos que más convengan en el proceso de esta investigación.

- Limitar el acceso al área donde se encuentra el equipo que evidentemente fue dañado
- Hacer un estudio preliminar del caso que se va a investigar
- Hacer un enfoque preliminar sobre el caso a estudiar
- Crear un diseño detallado
- Identificar la evidencia digital
- Obtener y copiar los discos donde se encuentra la posible evidencia
- Preservación de la evidencia digital
- Identificar los riesgos
- Eliminar o minimizar los riesgos
- Verificando el esquema de la investigación
- Analizar y recuperar la evidencia digital
- Investigar los datos recuperados
- Hacer un reporte del caso
- Criticar la investigación
- Presentación de la evidencia digital

Lo primero por hacer al llegar al lugar donde se cometió el delito es entrevistarse con la gente que contrato los servicios, ellos nos ubicarán en el lugar donde se encuentra el equipo directamente dañado, verificamos los procesos que esta llevando a acabo el equipo en ese momento, esto lo hacemos directamente desde la pantalla conectada al equipo, tomar fotos, desconectar el equipo de la red y cerrar el acceso al sitio en donde se encuentra este es lo primero por hacer, después nos entrevistaremos con la gente que contrato los servicios, se definirán algunas cosas como privilegios de autoridad que ellos mismos proporcionarán para dar mayor fluidez a la investigación y se tratarán asuntos relacionados con la actividad de su negocio, también sabremos en que horario se puede trabajar procurando no interrumpir los procesos de producción de quien contrata los servicios; lo siguiente es entrevistar a los administradores de el o los sistemas

involucrados quienes proporcionaran información muy valiosa en cuanto a los esquemas de trabajo e infraestructura de la red, así como todo el personal que tiene acceso a los mismos, es bueno llevar notas puntuales de todo lo que se va investigando para no perder ningún detalle. Hasta aquí se han cubierto el punto uno y dos de la metodología.

Es necesario tener una idea clara del tipo de datos que se están buscando, cada caso de estudio tiene sus particularidades, no es igual una investigación, en este caso el robo de dinero a un banco, que buscar datos de pornografía infantil o algún otro delito informático. En el caso que estudiamos de fraude al banco, tenemos que enfocarnos en buscar de donde desapareció ese dinero faltante, por donde pudo haber salido el dinero, ubicar el equipo que se uso para el delito y quien ó quienes pueden haber sido los responsables. Hasta aquí estamos en el punto tres de la metodología que dice, hacer un enfoque preliminar sobre el caso a estudiar.

El siguiente diagrama muestra el proceso a tomar en cuenta para llevar acabo una investigación de informática forense, es un esquema general del seguimiento y tratamiento que se le debe de dar a los datos obtenidos durante la investigación.

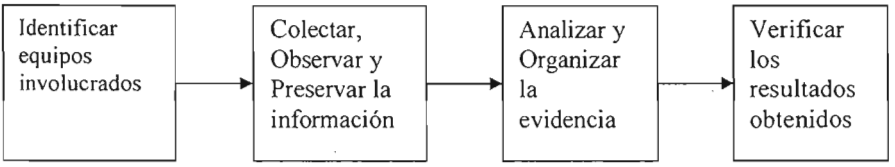

Figura 20.

4.2 IDENTIFICAR EQUIPOS INVOLUCRADOS

Una vez identificado el tipo de delito que se va a investigar, hay que analizar la infraestructura de la red, con el fin de tener un panorama claro de las transacciones de información y los flujos que se llevan acabo dentro de la misma, buscando ubicar los equipos involucrados. Dentro de los datos aportados por los administradores de la red de

sus equipos de seguridad perimetral se recopilo la siguiente información: cuentan con un servidor de DNS[77] (Sistema de Nombres de Dominio) externo el cual esta soportado por un equipo Intel® Pentium IV®, como sistema operativo tiene instalado Microsoft Windows 2003 Enterprise Server®, una solución de antivirus Virus Scan Enterprise 7.1 de Mcafee®. Éste equipo ofrece los servicios de resolución de nombres de dominios de Internet

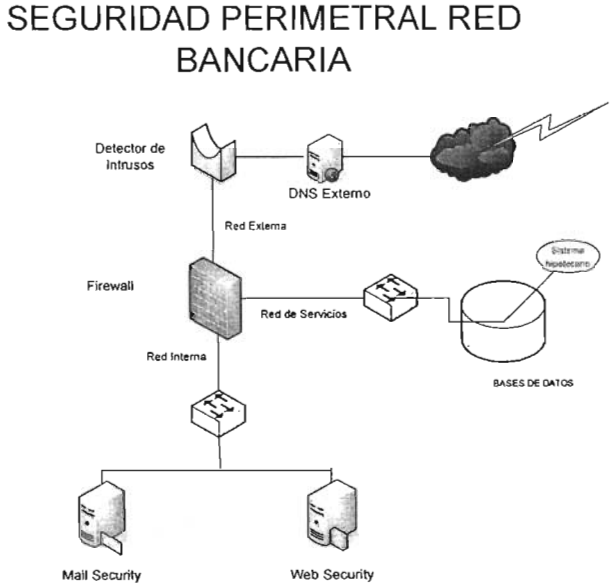

Figura 21.

Detector de Intrusos, un equipo el cual está soportado por tecnología Intel® y con un sistema operativo propietario de Symantec®. La función de este equipo está orientada a detectar los posibles ataques desde Internet hacia la red de datos interna.

[77] DNS, resuelve las direcciones de otros equipos que se encuentran en la red.

Firewall,[78] este equipo está integrado por tecnología Intel® y con un sistema operativo propietario de Symantec®. La función del equipo es, permitir o negar la utilización de puertos de comunicaciones desde y hacia Internet, esto se hace a través de reglas aplicadas a los servidores que se encuentran en los diferentes segmentos de red, y que están controlados por este medio.

Mail Security®, es un equipo con tecnología Intel®, con sistema operativo Microsoft Windows 2003 Server Enterprise®. La misión del equipo está enfocada a controlar todos los correos con protocolo SMTP (Simple Mail Transfer Protocol), hacia y desde Internet, permiten detectar y eliminar correos con virus

Web Security®, es un equipo con tecnología Intel®, con sistema operativo Microsoft Windows 2003 Server Enterprise®. El objetivo del equipo es controlar los requerimientos para navegación de Internet, es a través de este equipo que se establecen las reglas para bloquear con base a categorías los sitos que se consideren prohibidos, cuenta con reglas para negar descargas de archivos desde Internet, se pueden establecer horarios para navegación, revisa si las páginas tienen contenido malicioso, etc.

Después de estudiar el sistema de seguridad perimetral es tiempo de investigar el esquema de seguridad interno, no se debe olvidar que en muchas ocasiones los delitos informáticos se llevan acabo desde el interior de la misma red.

[78] Firewall, es un software integrado a un hardware especializado, el objetivo del mismo es brindar seguridad entre dos redes, controla el uso de los puertos, bloquea aplicaciones desde la red externa hacia la interna y viceversa, monitorear y administrar el intercambio de información.

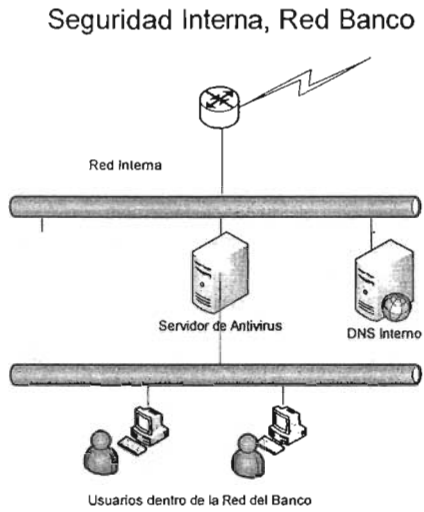

Figura 22.

El servidor de DNS Interno esta soportado por un equipo Intel® el cual tiene instalado como sistema operativo Microsoft Windows 2003 Enterprise Server®, una solución de antivirus Virus Scan Enterprise 7.1 de Mcafee®. Éste equipo ofrece los servicios de resolución de nombres de dominios de Internet y la red interna.

Antivirus, es un equipo con tecnología Intel®, sistema operativo Microsoft Windows 2003 Server Enterprise® y la solución de Mcafee® la cual integra una consola de administración para la configuración de todos los productos de antivirus con los que cuenta la red. Este servidor permite a través de la consola de administración integrar todos los productos "Antivirus" de la suite de Mcafee, establecer las políticas de seguridad para los equipos de cómputo como Computadoras de escritorio, servidores de archivos, servidores de correo, servidores de aplicaciones, servidores de publicación.

Hasta aquí llegamos al punto cinco de la metodología propuesta, que dice, identificar la evidencia digital.

4.3 COLECTAR, OBSERVAR Y PRESERVAR LA INFORMACIÓN

Ahora que se tiene el panorama de la infraestructura de la red y teniendo en cuenta los procesos por los que pasa la información dentro de la red donde se produjo el delito, sabemos por donde comenzar una investigación. En nuestro caso lo primero que se hizo durante la investigación fue examinar el detector de intrusos en su registro de detección de anomalías y el reporte de ingresos al firewall, esto nos permite saber si el delito se cometió desde adentro de la misma red o fuera de ella. Con el firewall todo había trabajado bien sin ninguna intrusión, no se encontraron anomalías ni desviaciones del tráfico normal de la red y los registros del firewall no mostraron bloqueos repetitivos que hicieran pensar el intento ó la intromisión de alguien extraño. Estos datos hacen pensar que todos los eventos de acceso que involucran al sistema aplicativo hipotecario el cual había sido el blanco de ataque, fueron llevados a cabo por alguien desde dentro de la misma red o algún usuario con autorización dentro del identificador de intrusos y el firewall.

Se sabe que el sistema hipotecario se procesa en una unidad central la cual se encuentra en un área separada lo que se conoce como DMZ (zona desmilitarizada) debido a sus datos y aplicaciones sensibles. También se sabe que ningún software de servicios Web esta localizado en la misma unidad que el sistema Hipotecario y que todos los sistemas de servicio Web, como el portal de Internet y el servidor de correo externo están en servidores separados, así el sistema hipotecario no tiene ninguna conexión directa con la red externar. Por lo tanto, la conclusión es que no es probable que estuviese implicado alguien del exterior. Si había algún delito, involucraba a un empleado o alguien que se encontraba dentro de la red bancaria.

El siguiente paso es revisar los registros de seguridad de acceso para conexiones con el sistema aplicativo hipotecario. Los registros de reporte del sistema de seguridad proporcionaron información sobre los empleados que tienen autorización para modificar y hacer transacciones. En la investigación se cotejaron los nombres de estos empleados con su inicio y fin de la conexión, solo durante el período en que se llevo acabo el delito. Una conexión en particular llamo la atención, en la cual una empleada registró la cancelación de una hipoteca residencial por un monto de $1, 000,000 de pesos, la cual coincidió con el monto faltante y la fecha en que tuvo lugar la perdida del dinero.

Ahora que hay una sospechosa es hora de buscar evidencia contundente para inculparla por los daños causados al banco, aquí hay un punto muy importante para tener en cuenta, ya que la intención de la investigación es identificar al delincuente y fincarle responsabilidades legales hay que apegarse a la legislación que rige en nuestra localidad, en nuestro caso México Distrito Federal, para poder formar una demanda con evidencia digital sustentable, el Código Federal de Procedimientos Civiles dice en su Artículo 210-A.

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedara satisfecho si se acredita que la información generada, comunicada, recibida o archivada, por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido integra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta puede ser accesible para su ulterior consulta".

Una de las políticas del banco sobre informática al nivel de toda la organización es que todos los aparatos y recursos informáticos son activos de la compañía que pertenecen al banco. Por consiguiente, el banco puede tener acceso e inspeccionar en cualquier momento todo artefacto, sistema de cómputo o dispositivo de comunicaciones.

Con base en lo anterior se llega con la sospechosa para incautar su equipo de cómputo, diciéndole que se esta llevando acabo una actualización de sistemas y le tocaba a su computadora aplicarle dicho proceso, entregándole la autorización correspondiente emitida por el área de Informática y firmada por el gerente de la misma, con el fin de no molestarle ya que aún es sospechosa y no hemos encontrado evidencia clara de que ella sea la culpable. Una vez con la computadora de la sospechosa en nuestro poder tomamos nuestro Kit forence que nos ayuda a generar copias de los discos duros que se van a investigar y nos dirigimos al MP (ministerio público), para levantar el acta correspondiente y frente a él generar la copia del disco y dejar la computadora de la sospechosa resguardada por el mismo MP, con el fin de cubrir el requisito del artículo 210-A del Código Federal de Procedimientos Civiles, antes mencionado. Al llegar al MP levantamos una demanda en contra de quien o quienes resulten responsables por el cargo de ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA, también hacemos la solicitud de que el MP de fe en el proceso de copiado que llevaremos acabo del disco duro que se encuentra dentro del equipo de la sospechosa, para hacer la copia utilizamos el software EnCase® el cual ya explicamos su funcionamiento en el capítulo II Investigación Forense, una vez efectuada la copia del disco duro solicitamos al MP que tanto el disco duro original como el equipo de computo, se queden en resguardo de la Procuraduría General de la Republica en su almacén de pruebas, y ahora es tiempo de comenzar el análisis del disco en nuestro laboratorio o lugar de trabajo.

4.4 ANALIZAR Y ORGANIZAR LA EVIDENCIA

Haciendo una revisión profunda del disco duro que usaba la sospechosa, se examinaron los registros del sistema operativo buscando información que vinculara a la usuaria con el fraude, en los cuales se encontraron indicios que efectivamente mostraban a la usuaria del equipo como la culpable de haber llevado acabo tal delito.

Una vez en el lugar de trabajo y con la copia del disco duro que se va a examinar lo primero que hay que hacer es generar una nueva copia de la copia del disco duro que se tiene, pues muy probablemente en la búsqueda de evidencia se dañe el disco sobre el que se trabaja y siempre es bueno tener otro de respaldo, también se necesita una hoja de registro para saber quien hace uso de la evidencia que se tiene o simplemente para llevar un buen control de la investigación, algo como lo que sigue.

Investigación en Informática Forense			
Caso No.:		Empresa a investigar:	
Investigador:			
Tipo de caso:			
Lugar de donde se obtuvo la evidencia:		Software para hacer imagen:	

Descripción de la evidencia		Marca	Modelo y No de serie
Producto1			
Producto2			
Producto3			
Producto4			

Evidencia recuperada por:		Fecha y Hora	
Evidencia asegurada por:		Fecha y Hora	

Producto #	Revisión de evidencia #	Investigador:	Fecha y Hora

Ya que se ha instalado el disco duro en una máquina hay que a analizar la información contenida en él, tiene instalado como sistema operativo Windows XP Home Edition con service pack 1, Office 2003, el sistema aplicativo hipotecario y Antivirus.

Revisar el visor de eventos del sistema operativo en busca de algunas pistas que sirvan para ir reconstruyendo la escena del delito, específicamente los registros del día en que ocurrieron los hechos, se encontró que la usuaria se conecto con el servidor donde se encuentra hospedado el sistema hipotecario, la conexión duró aproximadamente diez minutos, comenzó a las 11:12:35 a.m. del día 4 de octubre del año 2004 y termino a las 11:21:56 a.m. del mismo día y año. Revisando el sistema aplicativo hipotecario que se encuentra instalado en el disco duro que se esta analizando (este sistema aplicativo hace la conexión directa con el servidor en donde se encuentra el sistema hipotecario), y a simple vista no se encontró nada la bitácora, esta vacía, lo más probable es que la hubiese borrado, así que se recupera toda la información que ha sido borrada y se descubren los registros del sistema aplicativo borrados el mismo día 4 de octubre del 2004 a las 11:25:33 a.m., en los registros se ve la última transacción que hizo la usuaria fue del día 4 de octubre del 2004 a las 11:19 a.m. el registro se ve como lo siguiente:

BANCO XXXXX	
SISTEMA HIPOTECARIO	
USUARIO: MARÍA XXXXXXXXXXXX	CLAVE USUARIO XXXXXXX
NUMERO DE CLIENTE: 1234567890 TIPO DE OPERACIÓN: Cancelación de hipoteca	
04/10/2004	hora 11:19

Esta pantalla se guarda como bitácora para los empleados del banco después de hacer alguna operación, para confirmar la transacción realizada e imprimirla como comprobante para los clientes.

Mientras se buscaban la los registros del sistema hipotecario se encontraron algunos correos electrónicos que habían sido borrados recientemente y uno de ellos llamo la atención, pues sirve como evidencia:

Figura 25.

Era evidente que el delito se cometió desde esta máquina y con los permisos de esta usuaria, solo se necesita ubicarla en el momento en que se realizo el delito trabajando en su computadora para poder garantizar que fue ella quien lo llevo acabo, así que es necesario revizar los videos de las cámaras de seguridad internas del día 4 de octubre del 2004 entre las 11:00 y 11:30 a.m., fue dentro de este horario que se realizo la transacción

con el sistema hipotecario, y efectivamente el video mostró a la sospechosa trabajando frente a su computadora en el horario en que se llevo acabo el delito

Reporte de la investigación.

Contabilizando la evidencia recolectada hasta el momento y evaluando si es que lo que se tiene es suficiente para llevar el asunto ante las autoridades:

1.- Se tienen los registros del firewall que nos indican que no hubo ningún acceso no autorizado hacia nuestra red el día del delito. Esto nos garantiza que no pudo haber sido nadie sin autorización que se haya colado del exterior a nuestra red.

2.- Los registros del detector de intrusos no detectaron ningún intento repetitivo por entrar a nuestra red ese día, con lo cual podemos decir que el delito se llevo acabo desde dentro de nuestra red.

3.- Los registro del sistema hipotecario de donde desapareció el dinero, muestran a la sospechosa haciendo una transacción por el monto del dinero faltante el mismo día del delito.

4.- Se tiene la información almacenada en el disco duro de la computadora de la sospechosa, en la que encontramos un correo del cliente beneficiado con la cancelación de la hipoteca, también verificamos el visor de eventos de la máquina en la fecha y hora aproximada del delito, se encontró que la empleada estuvo conectada y haciendo transacciones con el sistema hipotecario durante aproximadamente 10 minutos, además se descubrió un archivo borrado aproximadamente 5 minutos depuse de que se llevo acabo la transacción, este es el comprobante de la transacción realizada pues siempre que se lleva acabo una transacción el sistema hipotecario envía un comprobante para que se le imprima al cliente como comprobante de la operación que se realizó.

5.- Como prueba de que en realidad fue la sospechosa y no otra persona que se hizo de sus permisos quien cometió el delito, están los videos de las cámaras de seguridad que la muestran en su lugar de trabajo en la hora que se cometió el delito.

6.-Mientras tanto, el deudor hipotecario en cuestión no pudo proporcionar una copia de un cheque depositado al banco o un recibo por la transferencia del dinero, y la cancelación de $ 1000,000 fue anulada.

Aunque realmente no se perdieron fondos, el banco presentó una demanda penal.

Basado en el Código Penal Federal en su Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

La recopilación de los registros y reportes de rastros verificables y la reconstrucción de la transacción fueron datos que se convirtieron en evidencia para determinar qué sucedió y quien fue la culpable de tal acto. Un examen del disco duro de una PC o de otros medios no habría proporcionado la evidencia necesaria para resolver este asunto. Cualquier investigación de un delito que involucre a los sistemas informáticos debe extenderse mucho más allá de la computadora personal. La evidencia electrónica debe ser

descubierta por toda la red. El secreto para exponer los argumentos del caso es pensar más allá del disco duro.

Es evidente que aun cuando se cuenta con equipo de seguridad perimetral para la red privada eso no garantiza que nuestros sistemas estarán totalmente seguros pues como se muestra en el escenario anterior muchos de los ataques y delitos cometidos hacia nuestros sistemas se perpetran desde adentro.

Lo que refleja el caso anterior es la necesidad de supervisar la actividad de los empleados, en Estados Unidos existe una asociación llamada Asociación Americana de Administración (AMA) quien realizo una encuesta y que arrojo los siguientes resultados, la tercera parte de los empleados en Estados Unidos fueron sujetos a supervisión y monitoreo en su lugar de trabajo, el 63% fue monitoreado en el acceso a la Internet, 47% fue monitoreado en correo electrónico, 36% en los archivos de su computadora y 8% en su correo de voz.[79]

Es muy probable que los empleados hagan un mal uso de los recursos tecnológico de la empresa, realizando actividades que nada tiene que ver con los intereses del lugar donde laboran, como por ejemplo el chat, sitios de pornografía, juegos, o bien actividades de hackeo, divulgación de información confidencial y que pertenece a la empresa donde trabajan.

Es necesario instrumentar algunas herramientas de control fundamentadas en las políticas de seguridad e integridad de la información de la empresa para que la aplicación de las mismas sea efectiva, se tiene que generar toda una cultura en las organizaciones haciéndoles ver que el equipo en el que laboran, así como la red y todos los equipos son propiedad del lugar donde trabajan y el objetivo del mismo debe estar enfocado a cubrir las necesidades o intereses de la empresa.

[79] Francisco Javier Villegas Landín, "Supervisión de la actividad de los empleados", *TECNOLOGIA EMPRESARIAL,* marzo 2004, pg40.

Así que para fortalecer la seguridad e integridad de la información que se encuentra en nuestros sistemas se recomienda la implementación de software especializado en el análisis de las actividades que se están llevando a cabo en nuestra red tales como:

- Filtrado de contenido
- Monitoreo y supervisión de actividades a nivel de la computadora
- Monitoreo y supervisión de actividades en la red

CONSTITUCIÓN DE UN DISCO DURO Y SU FUNCIONAMIENTO

En este punto estudiaremos la estructura física y como funcionan los dispositivos de almacenamiento magnético como el disco duro. No es un secreto que los archivos eliminados pueden ser recuperados desde el disco duro y otros dispositivos de almacenamiento magnético. Pero ¿cómo podemos estar seguros de que hemos capturado estos datos?

En general los medios de almacenamiento magnético como discos duros se basan en fenómenos físicos:

- Una corriente eléctrica produce un campo magnético.
- Hay materiales que se magnetizan fácilmente al ser expuestos a un campo magnético débil, entonces, al apagarse el campo, el material se desmagnetiza rápidamente. Éstos se conocen como materiales magnéticos suaves.
- En algunos de los materiales magnéticos suaves, la resistencia eléctrica cambia cuando el material es magnetizado. La resistencia regresa a su valor original cuando el campo magnetizante se apaga. Esto se llama magneto resistencia o MR. La Magneto-Resistencia Gigante, o efecto GMR, es mucho mayor que el efecto MR y se encuentra en sistemas específicamente de materiales de películas delgadas.
- Hay materiales que difícilmente se magnetizan ya que requieren de un campo magnético fuerte, pero una vez magnetizados se mantienen así aún cuando el campo se apaga. Son conocidos como Materiales Magnéticos Duros o Magnetos Permanentes y es de este tipo de material con el que están hechos los discos duros.

Estos fenómenos físicos son explotados por los fabricantes de las cabezas grabadoras magnéticas, cuya función es leer y escribir datos, para almacenar y recuperar datos en unidades de disco, de cinta y otros dispositivos de almacenamiento magnético.

Ya que los medios de almacenamiento magnético serán los que el informático forense más analizará en busca de evidencia, a continuación revisaremos como está compuesto un disco duro y como es su funcionamiento, para tener una idea de los procesos que lleva a cabo.

Figura 26.

Unidad de disco duro

La memoria principal RAM (Random Access Memory) es volátil, está construida sólo por componentes electrónicos, por tal motivo, al apagar la computadora se pierden los datos almacenados en ella. Su ventaja es que es sumamente rápida.

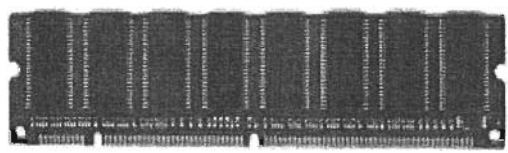

Figura 27.

Memoria RAM

La memoria secundaria (Disco Duro) no es volátil, esto quiere decir que conserva permanentemente los datos almacenados en ella, es más lenta y cuenta con componentes mecánicos.

En la memoria principal se concentran los datos que el usuario está manejando en tiempo real, pero tiene que recurrir a la memoria secundaria cuando tenga la necesidad de consultar nuevos datos o de guardar información permanentemente.

La estructura física de un disco duro es parecida a la de un disquete, porque en ambos casos la información digital se almacena en discos recubiertos de material ferromagnético. Asimismo los datos se graban y se leen por medio de cabezas magnéticas que se encuentran en ambas caras del disco siguiendo el mismo patrón de pistas y sectores, como se ve en la figura (c).

Cada superficie magnética tiene asignado uno de los cabezales de lectura/escritura de la unidad. Por lo tanto, habrá tantos cabezales como caras tenga el disco duro, y como cada plato tiene dos caras, este número equivale al doble de platos de la pila. Los cabezales se pueden desplazar linealmente del exterior al interior de la pila de platos por medio de un brazo mecánico que los mueve. Por último, para que los cabezales puedan acceder a la totalidad de los datos, es necesario que la pila de discos gire. Este giro se lleva a cabo a velocidad constante y no se detiene mientras está encendida la computadora. En cambio, en los discos flexibles sólo se produce el giro mientras se está efectuando alguna operación de lectura o escritura. El resto del tiempo, la disquetera permanece en reposo. Con las unidades de CD-ROM ocurre algo parecido, sin embargo en este caso la velocidad de giro es variable y depende de la distancia al centro del dato que se esté leyendo.

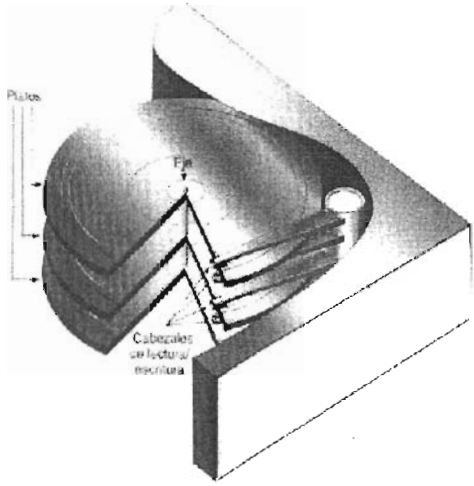

Figura 28.

Disco duro visto por dentro

Los disquetes están fabricados en base a un sustrato de plástico (un material denominado "Invar"), sobre el que se adhieren las partículas ferromagnéticas donde se almacenará la información; mientras tanto que en los discos duros, el sustrato de los platos giratorios está formado por aluminio, vidrio o cerámica.

En cuanto a la densidad de almacenamiento; por ejemplo, un disquete de 3.5 pulgadas y alta densidad, tiene 80 pistas o anillos concéntricos para almacenar información, mientras que un disco duro moderno puede tener más de mil cilindros en un área equivalente.

En lo que se refiere al motor del disco, una unidad de disquete gira a 300RPM, mientras que la velocidad de giro de los discos duros oscila entre 3600 y7200 RPM, dependiendo la marca y tipo del disco duro, llegando a alcanzar las 10.000RPM en

unidades de alto desempeño.[80] El disco duro es un conjunto de componentes electrónicos y mecánicos que hacen posible el almacenamiento y recuperación de los datos en el disco. El disco es, en realidad, una pila de discos, llamados platos, que almacenan información magnéticamente. Cada uno de los platos tiene dos superficies magnéticas, la superior y la inferior. Estas superficies magnéticas están formadas por millones de pequeños elementos capaces de ser magnetizados positiva o negativamente. De esta manera, se representan los dos posibles valores que forman un BIT de información (un cero o un uno). Ocho bits contiguos constituyen un byte (un carácter).

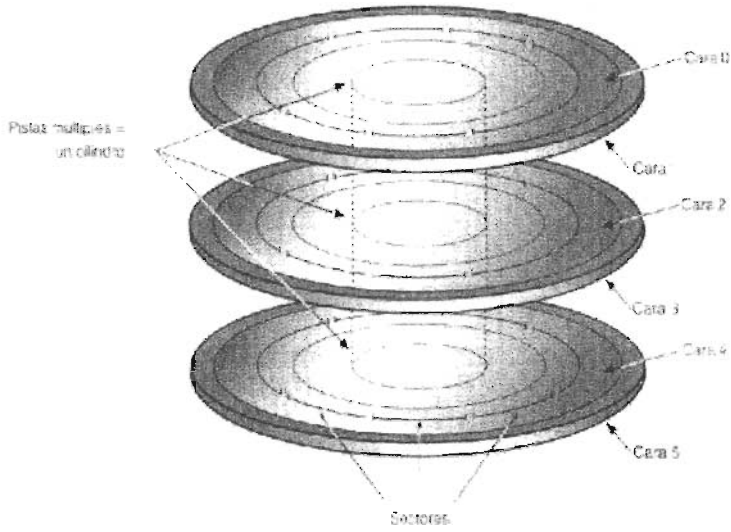

Figura 29.
Platos del disco duro

Las cabezas de escritura/lectura de un disco duro vuelan a una velocidad de hasta 340 km/h sobre la superficie del disco. En la figura cinco puede verse una cabeza de

[80] http://html.rincondelvago.com/disco-duro_1.html (06/09/2004)

escritura/lectura de un disco duro, tal y como se observa bajo un microscopio electrónico.[81]

Figura 30.
Cabeza del disco duro.

[81] http://www.recuperadores.convar.com/ursachen/koepfe.htm (07/09/2004)

CONCLUSIONES

Es evidente que las nuevas tecnologías cada vez son más potentes y económicas, lo cual permite su fácil acceso para la mayoría de la gente, pero esta apertura a traído consigo individuos que buscan la forma de cometer delitos con el uso de las tecnologías. La necesidad de empresas y bancos por brindar servicio en línea a sus clientes, los hace vulnerables a ser blanco de ataques mediante la red Internet y aunque cuenten con una fuerte infraestructura de seguridad siempre hay la posibilidad de ser vulnerados, es por eso que ha nacido una nueva ciencia llamada Informática forense.

Cuando comencé a investigar para la elaboración de la presente tesis me tope con un gran problema. No existe en México literatura relacionada con el tema, en un principio toda la información la obtuve de Internet más adelante de libros estadounidenses adquiridos por el postgrado de la Escuela Superior de Ingeniería Mecánica Eléctrica unidad Culhuacan, de los cuales obtuve muchos datos técnicos, pero cuando llegue a la parte legal se me presento otro problema y es que los delitos informáticos es un área que el derecho en nuestro país no ha trabajado mucho, o al menos no hay mucha información, mi investigación en esta parte fue más de campo asistiendo a congresos, como el de "El Derecho y las Nuevas Tecnologías", que tuvo lugar en el Instituto de Investigaciones Jurídicas de la UNAM en Noviembre del 2004 en el cual tuve acercamiento con especialistas en la materia y de quienes obtuve información sustancial para mi trabajo, también tuve acercamiento con un juez quien me guío acerca de los requisitos que debe de presentar mi evidencia para ser valida en un proceso legal y la forma de apegarme a la legislación. Ahora en este trabajo he reflejado el procesamiento de toda esa información adquirida en una metodología para llevar acabo una investigación en informática forense, esta metodología pretende ser una herramienta que ayude a llevar paso a paso una investigación, tratando de atacar las necesidades que presenta la presencia de un delito por medio de tecnologías de la información, aportando herramientas y técnicas para el análisis, así como presentando un panorama general que ayude a entender los alcances de la informática forense.

La característica de la metodología que he propuesto en esta tesis es que es un modelo general el cual puede ser aplicado en diferentes casos, solo basta con adaptarla a los requerimientos del caso a estudiar, pero más que nada la característica de esta metodología es que le ayudará al informático forense a saber como iniciar una investigación, como prever algunos problemas, saber en que momentos de la investigación se encuentra, en donde buscar pistas, como tratar la información obtenida, como analizarla y como ir armando el caso para que quede bien estructurado y al final de la investigación sea claro.

Ahora que he terminado este trabajo e investigado a fondo la informática forense, me doy cuenta que hacen falta muchos puntos por cubrir, pero la intención de esta tesis es introducir a todos los interesados en esta área mostrando un panorama general de los alcances de esta ciencia y crear conciencia acerca de las necesidades que se van presentando en una sociedad como la nuestra, en donde debemos estar preparados para atacar problemas como los delitos informáticos que día a día se incrementan, pues estamos entrando a la denominada sociedad de la información.

BIBLIOGRAFÍA

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

ANONYMOUS, Maximum Security, A Hacker's Guide to Protecting Your Computer Systems and Networks, SAMS PUBLISHING, United States of America, 2003.

BILL NELSON, AMELIA PHILLIPS, FRANK ENFINGER, CHRIS STEUART. Computer Forensics and Investigations. THOMSON COURSE TECHNOLOGY, United States of America, 2004.

DEBRA LITTLEJOHN, Scene of the Cybercrime Computer Forensics Handbook, SYNGRESS SHINDER BOOKS, United States of America, 2002.

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

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

FRED CHRIS SMITH, REBECCA GURLEY BACE, A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as and Expert technical Witness.ADDISON-WESLEY, United States of America, 2003.

HARLAN CARVEY, "Windows Forensics and Incident Recovery", ADDISON WESLEY, United States of America, 2005.

JOHN R. VACCA. Computer Forensics. Computer Crime Scene Investigation, CHARLES RIVER MEDIA, INC., United States of America, 2002.

JULIO TÉLLEZ VALDÉS. Derecho Informático. Mc.GRAW-HILL Interamericana, México, 2004.

LAUDON C., KENNETH y LAUDON P., JANE. Sistemas de información gerencial. Organización y tecnología de la empresa conectada en red. PEARSON EDUCACIÓN, México, 2002.

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