Universidad Nacional Autónoma de Nicaragua

UNAN-Managua

Departamento de Computación

Seminario de Graduación para optar al título de
Licenciatura en Ciencias de la Computación

Tema:

Computación Forense

Subtema:

El programa RecoverMyFiles y su aplicación en la informática forense de la Policía Nacional, para la recuperación de archivos en la actualidad.

Tutor:

Lic. Juan de Dios Bonilla.

Presentan:

- Br. Betty Silva Granera.
- Br. Karen Vargas Granera.
- Br. Mayling Marenco Flores.

Managua, Nicaragua Junio 2011.

DEDICATORIA

Dedicamos esta investigación:

A Dios:

Por darnos sabiduría para lograr nuestros objetivos, por su infinita bondad y amor al darnos fuerzas para hacer posible la realización de este trabajo.

A nuestras madres:

Paula Granera, Ileana Granera y Celia Flores por habernos apoyado en todo momento, por sus consejos, por la motivación constante que nos ha permitido ser personas de bien y por lo más importante, su amor.

A nuestros familiares:

Por el apoyo y confianza que nos brindan, ya que siempre podemos contar con ellos en todo momento.
A mi hermana Scarleth Vargas por brindarme su apoyo económico durante mi formación académica.

A nuestros amigos:

Por apoyarnos mutuamente en nuestra formación académica y en la realización de esta tesis.

AGRADECIMIENTO

Queremos agradecer:

Primeramente a Dios por darnos la vida, la fuerza y la sabiduría necesaria para culminar nuestros estudios universitarios y nuestra tesis.

Al personal del Laboratorio de Criminalística de la Policía Nacional, por que tuvieron la cortesía de responder las encuestas para la elaboración de esta investigación.

Al Ing. Juan Alberto Rueda encargado del centro de cómputo del Laboratorio de Criminalística, por responder una de las entrevistas de esta investigación.

Especialmente al Comisionado Aníbal Esteban por habernos brindado la información solicitada, además por su amable trato en las sucesivas visitas a la institución y por regalarnos un poco de su valioso tiempo.

A nuestro tutor, Lic. Juan de Dios Bonilla por sus orientaciones y su paciencia al instruirnos durante el tiempo que ha durado este seminario de graduación. Y a todos los profesores del departamento de computación de la UNAN-Managua, por formarnos académicamente.

También de una forma muy especial al Lic. Alexander Leytón, por brindarnos parte de su tiempo y compartir sus conocimientos con nosotras.

Y a todas aquellas personas que participaron directa o indirectamente en la elaboración de esta tesis.

INDICE

I. INTRODUCCIÓN

En el mundo de hoy los delincuentes se valen de instrumentos que brinda la tecnología, para cometer nuevos delitos que permiten el acceso a toda la información introducida en Internet sin dejar rastros que conduzcan a ellos. La necesidad de prevenir y sancionar estos malos usos en Internet hace necesario determinar las alteraciones que produce esta nueva modalidad delictiva.

Sin embargo, los avances de esta misma tecnología proporcionan las herramientas suficientes para reconstruir un caso y conseguir evidencias. Las modalidades de crimen como el ingenio han crecido a través de los tiempos y en la actualidad el cibercrimen es una de esas modalidades que ha surgido con la globalización del Internet y es la forma preferida de muchos para cometer fraudes, estafas, sabotaje, evasión de impuestos e incluso poner en práctica el espionaje corporativo.

Para capturar a delincuentes que creen que están a salvo de la ley, protegidos por el anonimato que ofrece la tecnología y para evitar la fuga de información principal activo de una empresa, se emplean las técnicas de computación forense.

La investigación forense es la aplicación de métodos y técnicas para obtener, analizar y preservar, evidencia digital que es susceptible a ser eliminada o sufrir alteraciones. Esta permite reunir pruebas para adelantar una acción penal.

Por lo tanto, en este trabajo se abordan algunos aspectos generales de la informática forense y las herramientas que esta emplea para recuperar información.

II. RESUMEN

En este documento se describe un panorama general de la informática forense y algunos temas afines a esta nueva ciencia.

Primeramente se describe que es seguridad y los tipos que existen. Acto seguido se explica el concepto de delitos informáticos, clasificación y sanciones jurídicas de estos en Nicaragua. A continuación se expone las características, beneficios y las técnicas de eliminación y recuperación de archivos informáticos. Luego se revela que es la computación forense, su importancia, sus objetivos y usos. También, se explica brevemente el concepto, categorías y características legales de la evidencia digital. Posteriormente se habla un poco de métodos anti-forenses, una de las nuevas técnicas utilizadas en la actualidad por los delincuentes informáticos para desafiar a los investigadores forenses.

A continuación se presenta las generalidades y funcionamiento de RecoverMyFiles, programa usado por los investigadores forenses en la recuperación de información. Después se muestra la hipótesis, variables y resultados de este estudio. Seguido de la metodología de investigación empleada para este estudio.

Y en la parte final de este trabajo se dan las conclusiones obtenidas durante la realización de esta investigación.

III. ANTECEDENTES

El Laboratorio de Criminalística es un órgano de la Policía Nacional, que tiene como objeto fundamental la realización de peritajes aplicando métodos, técnicas y conocimientos de medicina forense. Su función principal es auxiliar en las investigaciones policiales y penales a los poderes encargados de impartir justicia, mediante el estudio e investigaciones de los elementos de pruebas, recolectados en la escena del crimen.

El Laboratorio de Criminalística tiene como misión apoyar la función policial, a los tribunales de justicia y otros órganos que lo requieran de acuerdo a la ley en la realización de peritajes por medio de métodos, técnicas y conocimientos científicos, que garanticen el desarrollo de una actividad probatoria fiable, útil y veraz.

Y su visión es ser un órgano de apoyo de referencia nacional, con un personal altamente calificado en el conocimiento, técnico y científico de las ciencias criminalísticas en permanente transformación, moderno, eficiente, con vocación de servicio, convirtiéndose en parte integrante de la comunidad científica Nacional e Internacional.

El Laboratorio de Criminalística fue fundado en el año 1980 y en sus inicios el registro de la información se realizaba de forma manual. El desarrollo tecnológico del centro de cómputo se ha dado en paralelo con el avance de la tecnología en Nicaragua a través de donaciones de países extranjeros.

En la actualidad esta en construcción un nuevo laboratorio que dispondrá de los medios tecnológicos más modernos, para luchar contra el delito y la inseguridad ciudadana.

IV. PROBLEMÁTICA

El desarrollo de internet y el avance de las bases de datos han creado un nuevo tipo de sociedad denominada “Sociedad de la Información”, con la que surgen delitos y mal comportamiento, estos comportamientos anómalos son conocidos como delitos informáticos.

Con el fin de identificar a los autores y de preservar la evidencia de un delito informático surge lo que se conoce hoy en día como cómputo forense o informática forense, la cual se basa en la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar y presentar datos que sean válidos dentro de un proceso legal.

Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.

El Laboratorio de Criminalística ha decidido hacer uso de la herramienta de recuperación de datos, con el fin de recuperar la información que se pierde cuando se presenta un delito informático en la institución.

La información eliminada por los operadores del sistema se pierde, debido a que la institución no cuenta con un software para recuperar dicha información. Después que se comete un delito informático en la institución la acción que se toma es crear un escrito manual para registrar el hecho.

Por la situación antes mencionada, usar RecoverMyFiles probablemente es la solución óptima para la recuperar la información importante del Laboratorio de Criminalística.

V. JUSTIFICACIÓN

Con esta investigación se pretende dar a conocer que es la informática forense y las herramientas que esta emplea en la recuperación de archivos. También se desea dar a conocer las generalidades y los beneficios que ofrece una herramienta en específico como es RecoverMyFiles.

Por la razón antes mencionada se muestra de forma práctica el funcionamiento de esta herramienta. Mediante esta práctica se desea dar solución al problema que tiene actualmente el Laboratorio de Criminalística debido a que:

- ✓ Ayudará al personal de la institución a ampliar los conocimientos informáticos, por que tendrán a su alcance información general sobre la informática forense y RecoverMyFiles.

- ✓ Permitirá recuperar la información eliminada en el sistema del Laboratorio de Criminalística.

Con la realización de esta investigación también se espera proporcionar un precedente, debido a que dentro de la universidad no existe ningún trabajo monográfico del tema. Es decir que esta sirva de base para futuras investigaciones o estudios relacionados con el tema.

VI. OBJETIVOS

6.1. Objetivo General

Valorar la efectividad del programa RecoverMyFiles y su aplicación en la informática forense.

6.2. Objetivos Específicos

- ✓ Conocer las generalidades que constituyen el origen y funcionamiento de la informática forense.
- ✓ Describir el proceso desarrollado por el programa en la recuperación de archivos.
- ✓ Analizar la efectividad del programa en la recuperación de archivos.

VII. MARCO TEÓRICO

7.1. Seguridad

Se puede definir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. La seguridad es una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo y que en cierta manera es infalible. Técnicamente es imposible lograr un sistema ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos.[1]

7.1.1. Seguridad informática

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.[2]

La seguridad informática comprende software, bases de datos, metadatos y archivos que signifiquen un riesgo si estos llegan a manos de otras personas.

Hay dos tipos de seguridad, la seguridad lógica y la física. La lógica son aplicaciones y herramientas informáticas diseñadas para la seguridad. Y la física esta relacionada con el mantenimiento eléctrico, anti-incendio, humedad y otros.

[1] www.duiops.net/hacking/seguridad-sistemas
[2] www.alegsa.com.ar/Dic/seguridad informatica

Algunas amenazas que pueden afectar la seguridad de un sistema informático son:

- ✓ Programas malignos como: virus, espías, troyanos, gusanos, phishing, spamming, etc.
- ✓ Siniestros como: robos, incendio, humedad y otros; que pueden provocar pérdida de información.
- ✓ Intrusos informáticos: que pueden acceder remotamente (si está conectado a una red) o físicamente a un sistema para provocar daños.
- ✓ Operadores: los propios operadores de un sistema pueden debilitar y amenazar a la seguridad de un sistema ya sea por boicot o por falta de capacitación.

Las siguientes técnicas se usan para mantener la seguridad informática:

- ✓ Utilización de aplicaciones de protección como: cortafuegos, antivirus y anti espías.
- ✓ Encriptación de la información y uso de contraseñas.
- ✓ Capacitación a los operadores del sistema.
- ✓ Capacitación a la población en general sobre las nuevas tecnologías y las amenazas que pueden traer.

7.1.2. Seguridad de la red

Una red es un conjunto de equipos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos. [1]

[1] www.alegsa.com.ar/Dic/seguridad informatica

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones.

La seguridad de red es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos.[1]

7.1.3. Seguridad en los sistemas

Para mantener un sistema seguro se deben garantizar tres aspectos:

- ✓ Confidencialidad: es decir que un sistema sea accedido únicamente por elementos autorizados y estos no deben convertir la información en disponible para otras entidades.
- ✓ Integridad: que los objetos sólo pueden ser modificados por elementos autorizados y de manera controlada.
- ✓ Confiabilidad: se refiere al nivel de calidad del servicio ofrecido.

La seguridad en los sistemas trata de asegurar la confidencialidad, integridad y disponibilidad de los sistemas en red. En la seguridad en sistemas se habla de seguridad física cuando se quiere tener un equipo seguro, es importante considerar todos los aspectos que están involucrados. Uno de ellos sin duda es la seguridad que se brinda en el entorno donde está ubicado el equipo. [2]

[1] www.wikipedia.org/wiki/Seguridad_de_la_red
[2] Tanenbaum, Andrew S. "*Redes de Computadoras*", 4ª Cuarta edición 2003, Ed. Prentice-Hall.

El punto más débil que tienen la mayoría de los equipos es su consola, ya que siempre se asume que la persona ubicada frente a la consola, es la persona que administra el equipo y tendrá pleno conocimiento del funcionamiento del mismo.

Llegado el caso de que un intruso logre estar personalmente en frente de la consola, este punto se puede controlar tomando las siguientes precauciones:

- ✓ Colocar el equipo en una sala cerrada bajo llave.
- ✓ Eliminar cualquier periférico que no se utilice con frecuencia.
- ✓ Setear el arranque en el BIOS, para permitirlo solamente desde el disco rígido primario.
- ✓ Proteger el BIOS del equipo con clave.
- ✓ Eliminar puertos (seriales o paralelos) que no se utilicen.
- ✓ Desconectar teclado, ratón y video si estos no son utilizados.

Como siempre existen muchas formas de quebrar la seguridad de un sistema, nunca se es lo suficiente precavido, pero es importante complicar al máximo la entrada de un posible intruso. Debe insistirse una vez más que si un potencial intruso tiene acceso al hardware no hay ningún tipo de seguridad lógica inviolable. La seguridad lógica se relaciona con la configuración adecuada del sistema para evitar el acceso a los recursos y configuración del mismo por parte de personas no autorizadas, ya sea a nivel local o vía red.

Entre los puntos más importantes a tomar en cuenta para la seguridad lógica tenemos:

- ✓ Utilizar un sistema operativo relativamente seguro.
- ✓ Elegir buenas claves o passwords.
- ✓ Activar el protector de pantalla con clave cuando el equipo queda desatendido y hacer logoff antes de retirarse del mismo.
- ✓ Utilizar algún firewall, antivirus, troyano, etc. [1]

[1] www.duiops.net/hacking/seguridad-sistemas

- ✓ Utilizar dispositivos de identificación por biométrica (huellas dactilares, escaneo de retina o reconocimiento de voz).[1]

7.1.4. Seguridad y privacidad de la información

Los mecanismos adecuados para que la información de una organización o empresa sea segura, dependen de la protección que el usuario aplique para el uso normal del equipo. Esto se consigue con las garantías de confidencialidad que garantice el acceso a la información, protegiendo la integridad y totalidad de la información y sus métodos de proceso. También asegura la disponibilidad, que garantiza a los usuarios autorizados el acceso a la información y los recursos.

Algunas amenazas que se pueden dar a la información son:

1. Piratas (hackers): son personas aficionadas a las computadoras cuya diversión es aprender todo acerca de un sistema de red y mediante una programación hábil, llevan el sistema al nivel máximo de rendimiento.
2. Virus y troyanos: son programas habitualmente ocultos dentro de otro programa, e-mail, fichero, etc. Se ejecutan automáticamente, haciendo copias de sí mismos dentro de otros programas a los que infectan. Dependiendo del modo en que atacan y se propagan reciben un nombre.
3. Spam: correo basura no solicitado con el que se bombardea a los e-mails, suelen estar relacionados con la publicidad.
4. Spyware: es un software que de forma encubierta utiliza la conexión a Internet para extraer datos e información sobre el contenido del ordenador como páginas visitadas, programas, etc.
5. Dialers: cuelgan la conexión telefónica utilizada y establecen otra de forma maliciosa, utilizando una conexión de tarificación especial, que se reflejará en la factura telefónica. [2]

[1] www.duiops.net/hacking/seguridad-sistemas

[2] www.wikipedia.org/wiki/Seguridad_de_la_red

6. Agujeros (bugs) en la seguridad: son errores de programación que pueden provocar errores y daños a la información. Los agujeros en la seguridad pueden ser utilizados para lanzar ataques por parte de intrusos.

Algunas formas para protegerse de estas amenazas son:

- ✓ Mantenerse informado.
- ✓ Conocer el sistema operativo.
- ✓ Instalar antivirus, anti-spam, spyware, firewalls, etc.
- ✓ Limitar el número de puntos de entrada (puertos).
- ✓ Definir una política de seguridad interna (contraseñas, activación de archivos ejecutables, etc.).
- ✓ Evitar que personas no autorizadas intervengan en el sistema con fines malignos.
- ✓ Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
- ✓ Asegurar los datos mediante la previsión de fallas.
- ✓ Garantizar que no se interrumpan los servicios.
- ✓ Actualizar frecuentemente el software.

Para prevenir ataques se debe aumentar la seguridad de un sistema durante su funcionamiento normal, previniendo que se produzcan violaciones a la seguridad. Las contraseñas y permisos de acceso establecen a que recursos puede acceder un usuario.

Para asegurar las comunicaciones se deben emplear mecanismos basados en la criptografía que consiste en el cifrado de contraseñas y firmas digitales. No existe el ordenador cien porciento seguro, salvo que se encuentre completamente aislado, tanto físicamente como vía red.[1]

[1] www.wikipedia.org/wiki/Seguridad_de_la_red

7.2. Delito Informático

El delito informático implica cualquier actividad ilegal o criminal que encuadra en figuras tradicionales ya conocidas como: robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

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 muchos países aún no ha sido objeto de tipificación.

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

Es común la expresión "la información cuesta", lo que refleja el atractivo que representa en la actualidad manejar datos, ya que se ve a la información como un elemento de conocimiento, poder y fortuna. Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros.

Es importante señalar que las nuevas tecnologías se convierten en instrumentos del delito, cuando sus técnicas y sofisticadas herramientas para el tratamiento automatizado de la información se utilizan como medio de comisión de acciones generadoras de importantes daños y lesiones (patrimoniales o no) a personas y organizaciones.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

Esta emergente categoría criminal ha sido encuadrada usando los términos: delitos computarizados, delitos informáticos y en un sentido más amplio son designados como crimen silencioso o tecnológico.

El delito silencioso se caracteriza principalmente por la participación de la tecnología, como instrumento u objeto, en sucesos relacionados con los delitos. Pero existen otros elementos distintivos de donde se origina tan peculiar denominación de silenciosos. Estos hechos (a diferencia de delitos ordinarios como el secuestro, el homicidio o la violación) son absolutamente discretos, no ocupan grandes titulares en los medios de comunicación y en la mayoría de las ocasiones permanecen ocultos e ignorados.

Esta peculiaridad se debe a la dificultad existente para descubrir su ocurrencia, a la creciente imposibilidad de lograr evidencias que permitan descubrir a los culpables y a la común inacción de los agraviados, que normalmente prefieren evitar la divulgación de estas acciones que demuestran una cuestionable vulnerabilidad de sus sistemas de información.

Son varios los elementos que hacen atractiva la comisión de estos delitos. El primero de estos elementos es la relativa facilidad con que un experto informático puede perpetrar estas acciones, las cuales requieren del manejo de conocimientos y herramientas especiales, que en la mayoría de los casos, son de dominio exclusivo de personal técnico.

Los montos de las operaciones delictivo-informáticas son considerablemente elevados, en comparación con los delitos comunes contra la propiedad. La mayoría de estos delitos no están tipificados, es decir considerados expresamente en la ley, lo que contribuye a incrementar los índices de impunidad que tales conductas tienen en las estadísticas policiales y judiciales.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

Estos delitos pueden perpetrarse a distancia, programar en el tiempo la aparición de sus efectos, borrar los rastros dejados e incluso emplear datos que deliberadamente desvíen las investigaciones hacia otra persona, a quién pudiera incriminarse. Además, resulta casi imposible distinguir de manera objetiva las frágiles fronteras entre la intención, el error técnico o la impericia.

7.2.1. Sujetos del delito informático

Existen dos tipos de actores o personas involucradas en una actividad informática delictiva: el sujeto activo es la persona que comete el delito informático y el sujeto pasivo es la persona víctima del delito informático.

7.2.1.1. Sujeto activo del delito informático

Las personas que pueden cometer delitos informáticos son aquellas que poseen ciertas características que no presentan los delincuentes comunes, esto son los sujetos activos, estos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Estas características nos remiten a:

- ✓ Operadores: que se pueden poner en relación con el sistema para modificar, agregar, eliminar, sustituir información o programas y copiar archivos para venderlos a competidores.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

- ✓ Programadores: que pueden violar o inutilizar controles protectores del sistema; para dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos y acceder a información confidencial.
- ✓ Analistas de sistemas: que pueden unirse con usuarios, programadores u operadores; para revelarles la operación de un sistema completo.
- ✓ Analistas de comunicaciones: que enseñan a otras personas la forma de violar la seguridad del sistema de comunicación de una empresa, con fines de fraude.
- ✓ Supervisores: que pueden en razón de su oficio manipular los archivos de datos, ingresos y las salidas del sistema.
- ✓ Personal técnico y de servicio: que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.
- ✓ Ejecutivos de la computadora: que pueden actuar en alianza con otras personas.
- ✓ Auditores: que pueden actuar como los anteriores.
- ✓ Bibliotecarios de preparación: que pueden vender la documentación.
- ✓ Bibliotecarios de operaciones: que pueden destruir información mediante errores o pueden venderla a competidores.
- ✓ Personal de limpieza, mantenimiento y custodia: que pueden vender el contenido de los costos de papeles, fotocopiar documentos y sabotear el sistema.
- ✓ Usuarios: que pueden modificar, omitir o agregar información con fines fraudulentos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que los diferencia entre sí la naturaleza de los cometidos. Así la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

Los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

7.2.1.2. Sujeto pasivo del delito informático

El sujeto pasivo es la víctima del delito, es el ente sobre quien recae la conducta de acción u omisión que realiza el sujeto activo y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos y otros, que usan sistemas automatizados de información generalmente conectados a otros.

Los bienes jurídicos afectados pueden ser:

- ✓ Las personas.
- ✓ El honor de las personas.
- ✓ La intimidad de las personas.
- ✓ La propiedad (de hardware o software).
- ✓ Los documentos, archivos, registros, bases de datos y toda información concerniente al que hacer propio de la entidad.
- ✓ La fe pública.

7.2.2. Tipos de delitos

Los delitos informáticos incluye los cometidos contra el sistema y los cometidos por medio de sistemas informáticos ligados con telemática o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, dinero, etc.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

7.2.2.1. Delitos comunes

- ✓ Acceso no autorizado: el uso legitimo de contraseñas (passwords) y el ingreso a un sistema informático sin autorización del propietario esta tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

- ✓ Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

- ✓ Infracción de los derechos de autor: la interpretación de los conceptos de copia, distribución y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel de la prudencia jurídica. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line respecto a las copias ilegales introducidas en el sistema.

  El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

- ✓ Distribución de música por Internet: es sabido que con relación a la música existe el conocido MP3 un formato digital de audio que permite comprimir el tamaño de una canción digitalizada en una relación de 10 a 1 es decir que 10 MB de sonido digitalizado ocuparía solo 1 MB, esto es lo que ha permitido un intenso tráfico de música dentro de la red que ha derivado inclusive en la venta ilegal de compactos sin intervención de las discográficas dando lugar a todo un movimiento al respecto que ha sido motivo de numerosas medidas para tratar de evitarlo.

- ✓ Intercepción de E-mail: se refiere a la violación de correspondencia ajena y la intercepción de telecomunicaciones, es decir la lectura de mensajes electrónicos ajenos. Ambos delitos tienen el mismo nivel de gravedad.

- ✓ Estafas electrónicas: las compras electrónicas son un atractivo más para que aumenten los casos de estafa y para que exista un engaño a la persona que compra al distribuidor, al banco y al equipo principal encargado de la operación. La proliferación de las compras telemáticas permite que aumenten también los casos de estafa.

  Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para cometer determinadas tareas. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, entre otras cosas se han abierto nuevas perspectivas de consumo mediante el uso de Internet. Todos los que navegan por Internet, conocen que se venden cientos de productos de diferentes marcas y modelos a través de la red.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

El ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es muy lógico pues se ahorran muchos costos y amplían su potencial de mercado. Lógicamente, todo depende del tipo de empresa y del producto o servicio que venda. Nos podemos encontrar con que la supuesta empresa manda productos incorrectos y no podemos reclamar directamente porque no sabemos dónde se ubica la empresa o simplemente hemos hecho un pago con la tarjeta de crédito.

Todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio, por ejemplo al dar un número de tarjeta de crédito falso que se acepta como válida, esto es conocido en el mundo de Internet como carding. Con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos.

Con todo lo anterior podemos definir la estafa informática como la manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico a un tercero.

- ✓ Transferencias de fondos: este es el típico caso en el que no se produce engaño a una persona determinada; sino a un sistema informático ya sea por el mal uso de passwords, tarjetas electrónicas falsificadas, llaves falsas o adulterando el contenido de la información externamente calificando dicha conducta como robo.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

7.2.2.2. Delitos convencionales

Son todos los delitos que se dan sin el empleo de medios informáticos y que con la aparición de las rutas virtuales se están reproduciendo también en el ciberespacio. También los actos que no son propiamente delitos sino infracciones administrativas o ilícitos civiles.

- ✓ Espionaje: se están presentando casos de acceso no autorizado a sistemas informáticos e intercepción de correo electrónico de entidades gubernamentales, estos actos podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, evidenciándose una vez mas la vulnerabilidad de los sistemas de seguridad gubernamentales por personas especializadas.

  Entre los casos más famosos podemos citar el acceso al sistema informático del pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje.

- ✓ Espionaje industrial: también aparecen casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales y fórmulas que posteriormente las utilizan otras empresas de la competencia o las divulgan sin autorización.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

- ✓ Terrorismo: se refiere a la presencia de equipos que encubren la identidad del remitente, convirtiendo el mensaje en anónimo, los servidores que ofrecen servicio de correos gratis permitiendo ingresar datos personales y direcciones ficticias para crear cuentas de correo que posteriormente aprovecharon personas o grupos terroristas para enviar amenazas, remitir consignas y planes de actuación ilícitos.

- ✓ Narcotráfico: se ha detectado el uso de mensajes encriptados mediante Internet, con el fin de transmitir formulas para la fabricación de estupefacientes, el blanqueo de dinero y la coordinación de entregas y recogidas. Los EE.UU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. El notable avance de las técnicas de encriptación permite el envío de mensajes que a pesar de ser interceptados pueden resultar indescifrables para los investigadores policiales.

7.2.2.3. Otros delitos informáticos

Al igual que los narcotraficantes, se presentan los traficantes de armas, las sectas satánicas y otros, obteniendo las mismas ventajas que encuentran en Internet aprovechadas para la planificación de los respectivos ilícitos.

- ✓ Difusión de pornografía: en la mayoría de países así como en nuestro país es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia. Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas escaneadas a los mailbox de un país en donde estuvieran también prohibidos los actos de difusión o comercialización de las mismas.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

- ✓ Manipulación de datos: este fraude conocido también como sustracción de datos, es el delito informático más representativo ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos. De acuerdo a la información entregada por entidades de seguridad a nivel mundial, el 75% de los casos de sustracción de datos lo realiza personal interno de la organización o que pertenecieron a esta.

- ✓ Manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados por las personas que tienen conocimientos especializados en programación informática es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- ✓ Manipulación informática: es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos falsos, colocar datos en distinto momento y lugar, variar las instrucciones de elaboración, etc.

  Se diferencian las estafas informáticas cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

- ✓ Falsificaciones informáticas: estas pueden darse de dos formas, como objeto o instrumento.

  Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada, cuando por necesidad se comparten directorios y con esto se permite que usuarios remotos tengan acceso abriendo una ventana para que ingrese en forma fraudulenta personal ajeno a esta información. Para contrarrestar este acceso se necesita que los usuarios tengan conocimiento tanto de las ventajas (acceso a recursos siempre con claves) como desventajas (intrusión) de esta herramienta, además la adquisición inmediata de equipos muros para autenticar usuarios y ubicar las partes vulnerables de la red.

  Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial, con la ayuda de escáner y de impresoras de alta calidad para modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original donde solo un experto puede diferenciarlos de los documentos auténticos.

- ✓ Sabotaje informático: estos pueden ser realizados por medio de cualquiera de los siguientes métodos.

  1. Virus: son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho daño y más si se utiliza Internet como vía de infección. Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente EXE y COM, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado y así sucesivamente.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero. Como sabemos los virus son programas y para crearlos los programadores de virus utilizan kits de desarrollo de virus que se distribuyen por Internet, entre las que podemos destacar las siguientes: Virus Creation Laboratories, Virus Factory, Virus Creation 2000, Virus C destruction Est, o The Windows virus Entine. Por ello cualquiera que adquiera alguno de estos kits y sepa programación pueda crear sus propios virus, en este contexto no es raro que la estimación de los virus que existen en la actualidad sea de más de 7,000. Pueden ingresar en un sistema por la copia de un archivo infectado o por Internet que infectan algunos archivos de su sistema y lo pueden transmitir a otros equipos.

2. Gusanos: se fabrican de forma similar al virus con el objetivo de infiltrarlo en programas originales, para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Podría decirse que 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, es decir, un programa gusano que posteriormente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego destruirse.

3. Bomba ilícita o cronológica: exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en el futuro. Lo contrario de los virus y los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso entre todos los dispositivos informáticos criminales, la bombas lógicas son las que poseen el máximo potencial de daño.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

Su activación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. Puede utilizarse como material de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4. Piratas informáticos: el acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son, 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.

   Los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en sistemas donde los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema. En todos estos casos se producen pérdidas de dinero provocadas por las conductas involucradas. Frecuentemente, el objetivo de los hackers es controlar una máquina para poder llevar a cabo acciones deseadas obteniendo información que puede utilizarse en ataques, explotando las vulnerabilidades del sistema o forzando un sistema para irrumpir en él.

Podemos protegernos de los hackers de la siguiente manera:

- ✓ Instalar y mantener actualizado un buen antivirus y firewall.
- ✓ Instalar todos los parches de seguridad para su sistema operativo.
- ✓ Cerrar todos los servicios, excepto los imprescindibles. No dejar ninguno que no se utilice, por que pueden ser la puerta de entrada de un intruso.
- ✓ Acceder a su ordenador remoto en forma segura cuando desee transferir archivos importantes.[1]

[1] Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

7.2.3. Sanciones de los delitos informáticos en Nicaragua

Existe un "anteproyecto de ley especial sobre delitos informáticos" en Nicaragua elaborado por CONICIT en el año 2005. El cual establece en su contenido los delitos informáticos y sus sanciones jurídicas, pero esta no fue aprobada por la Asamblea Nacional de la República de Nicaragua.

7.3. Archivo Informático

Un archivo o fichero es una colección de datos relacionados entre sí, que son almacenados en algún medio y pueden ser usados por las aplicaciones. Estos sirven como soporte material de la información, como entrada y salida a la computadora y son manejados con programas.

Los archivos no requieren de un tamaño predeterminado, es decir que se pueden hacer archivos de datos grandes o pequeños, según se necesiten.

7.3.1. Beneficios de los archivos

- ✓ Independencia de la información respecto de los programas.
- ✓ La información almacenada es permanente.
- ✓ Un archivo puede ser accedido por distintos programas en distintos momentos.
- ✓ Gran capacidad de almacenamiento.

7.3.2. Característica de los archivos

- ✓ Nombre y extensión: cada archivo es individual y es identificable por un nombre y una extensión opcional que suele identificar su formato. El formato suele servir para identificar el contenido del archivo. [1]

[1] www.alegsa.com.ar/Dic/archivo.php

- ✓ Datos sobre el archivo: además para cada fichero, según el sistema de archivos que se utilice, se guarda la fecha de creación, modificación y de último acceso. También poseen propiedades como oculto, de sistema, de solo lectura, etc.
- ✓ Tamaño: los archivos tienen también un tamaño que se mide en bytes, kilobytes, megabytes, gigabytes que depende de la cantidad de caracteres que contienen.
- ✓ Ubicación: Todo archivo pertenece a un directorio o subdirectorio. La ruta de acceso a un archivo suele comenzar con la unidad lógica que lo contiene y los sucesivos subdirectorios hasta llegar al directorio contenedor.

7.3.3. Perdida de archivos

Los datos se pueden perder completamente debido a varias causas, tales como:

1. Disco duro dañado físicamente.
2. Virus que al entrar en acción destruyen los datos.
3. Escritura de otros archivos en el disco.

7.3.4. Eliminación de archivos

La información es un bien invaluable para las instituciones y por ello debe ser protegido. Teniendo en cuenta las posibilidades que existen actualmente, borrar un archivo puede no ser seguro, debido a que puede ser recuperado por una persona con acceso al equipo.

Una de las ideas más comunes acerca de la información, es que una vez borrada de la papelera de reciclaje esta información es irrecuperable, pero esto no es del todo cierto por que una persona con el conocimiento suficiente podría recuperarla. [1]

[1] www.alegsa.com.ar/Dic/archivo.php

Los avances en la informática y la corta vida de los equipos informáticos nos obligan a deshacernos con cierta frecuencia de ellos. El problema es la información que contienen los discos, que en muchos casos puede ser información confidencial.

Normalmente para solucionar este fallo de seguridad se suele formatear el disco duro, pensando así que estos datos ya no se pueden recuperar.

Pero esto no es cierto, en general la mayoría de los sistemas que gestionan los medios de almacenamiento como disquetes, discos duros y demás, no eliminan físicamente los datos contenidos en estos; sino que el cluster hacia el cual apunta el archivo es marcado de forma lógica como libre o eliminado. Pero el archivo aun esta en el disco y se puede acceder a este con la ayuda de algún software especializado en recuperación de datos. Los datos marcados como eliminados se irán perdiendo gradualmente a medida que otros datos comiencen a ocupar sus espacios.

Existen medios que no pueden ser borrados luego de grabarse como los CD, CD-R, DVD, DVD-R, etc. También otros medios de almacenamiento, como las memorias RAM, borran su información al dejar de recibir corriente eléctrica. Y esta información no puede ser recuperada.

Existen varios métodos para eliminar físicamente los archivos de los medios de almacenamiento, entre estos están:

- ✓ Sobrescritura múltiple: esto quiere decir reescribir (varias veces) toda el área física donde estaban los datos eliminados. [1]

[1] www.alegsa.com.ar/Dic/archivo.php

- ✓ Este método consiste en emplear aplicaciones especializadas, las cuales utilizan un algoritmo que permite seleccionar un número de ciclos de barridos entre 1 y 35 a realizar sobre la superficie del disco duro, sobreescribiendo la información utilizando diferentes procedimientos de forma aleatoria. De este modo, la recuperación de datos resulta prácticamente imposible.

- ✓ Destrucción física: consiste en utilizar sierras, mazos, sustancias químicas o la incineración para destruir la unidad en donde están almacenados los datos.

- ✓ Degaussing (desmagnetización): consiste en reducir la fuerza magnética grabada de un disco duro a 0, es decir este vuelve al estado inicial de fabricación. Este es un proceso destructivo rápido, con este la información es borrada por completo y ni un procedimiento de laboratorio con las técnicas conocidas a la fecha o un análisis puede recuperar la información que antes estaba grabada.

7.3.5. Recuperación de archivos

La situación ideal sería darse cuenta inmediatamente que se han eliminado archivos que consideramos importantes. A partir del momento que han sido eliminados, si se sigue utilizando ese disco duro, la información de los archivos borrados puede ir perdiéndose de a poco a medida que es reemplazada por otra información. Por lo tanto es importante dejar de usar el disco duro en cuestión.

Lo más adecuado es poseer un segundo disco duro (configurado como maestro), donde debe estar el sistema operativo y así poder acceder al otro disco duro (configurado como esclavo) sin afectar su información. [1]

[1] www.alegsa.com.ar/Notas/91.php

Muchas veces no es posible acceder a un segundo disco duro con un sistema operativo, así que se puede llevar el disco a otra computadora y conectarlo como esclavo en ella y así usar el sistema operativo de esa computadora para acceder al disco.

Si no se desea trasladar el disco duro a ningún lado, se puede intentar recuperar la información desde el mismo sistema operativo donde se perdieron los archivos. Esto implica un riesgo, el cual puede crecer o disminuir dependiendo de algunos factores como:

- ✓ Espacio libre disponible: a mayor espacio libre en disco, menos posibilidades hay de que otros archivos reemplacen justamente los archivos eliminados.

- ✓ Tiempo transcurrido desde que se eliminaron los archivos: puesto que el sistema operativo en sí mismo lee y graba archivos en el disco duro, a medida que pasa el tiempo el mismo sistema puede reemplazar la información perdida.

- ✓ Instalación de programas: al instalar programas se graba información en el disco, con la consecuente elevación del riesgo de perder los archivos borrados. Incluso el mismo programa que instalaremos y utilizaremos para recuperar la información puede afectar los ficheros eliminados.

Para recuperar los archivos eliminados se necesita de un programa especial que lo haga. En el mercado existen muchos de este tipo de programas tanto gratuitos como pagados. Si se tiene un segundo disco duro con Windows o si se instaló el disco en otra computadora, se debe proceder a instalar el programa de recuperación de archivos. [1]

[1] www.alegsa.com.ar/Notas/91.php

La mayoría de programas son muy parecidos de usar entre sí, así que si se conoce como utilizar uno de ellos se podrá utilizar otros también. Sin embargo es importante mencionar que existen programas unos mejores que otros, para recuperar archivos perdidos o eliminados. [1]

Es imposible garantizar una recuperación 100% efectiva de los archivos que han sido eliminados, por eso la mejor manera de no tener que pasar por una situación de estas características, es mantener un respaldo de nuestra información más importante.

Para aumentar las oportunidades de recuperar datos, se deben considerar algunos puntos:

1. No guardar archivos importantes en el directorio raíz: los archivos que se guardan en el directorio raíz son sensibles a perderse por formateo rápido, porque las entradas de archivo se encuentran en la raíz.
2. No guardar datos importantes en unidades de pequeña capacidad: la probabilidad de recuperación es menor, cuando la capacidad de la unidad de almacenamiento es más pequeña.
3. Guardar datos en diferentes unidades: es aconsejable distribuir copias de los datos importantes en diferentes unidades de almacenamiento.
4. No usar la unidad que se necesita para la recuperación: no instalar software de recuperación de datos, no guardar ningún dato y no usar ningún programa usual en la unidad que contiene los datos a recuperar, para no sobrescribir datos eliminados importantes. Para recuperar datos de un disco duro se debería usar un segundo disco.[2]

[1] www.alegsa.com.ar/Notas/91.php

[2] www.RecoverMyFiles.com

7.4. Computación Forense

El constante reporte de vulnerabilidades en sistemas informáticos y el aprovechamiento de fallas ya sean humanas o tecnológicas sobre infraestructuras de computación, ofrecen un escenario perfecto para los intrusos informáticos.

Por esto es preciso establecer un conjunto de herramientas, estrategias y acciones que permitan descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que se hacen sobre los hechos delictivos.

La computación o informática forense es una disciplina auxiliar de la justicia moderna para enfrentar los desafíos y técnicas de los intrusos informáticos y también sirve como garantía de la intensidad de la evidencia digital que se puede aportar en un proceso legal.

La especialidad de la informática forense asume dentro de su procedimiento tareas asociadas con la evidencia en la escena del crimen, como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas, de la situación que se está investigando.

7.4.1. Definición de computación forense

Existen muchas definiciones en la actualidad para el término informática forense dentro de las cuales se tiene:

- ✓ Computación Forense (computer forensics): esta definición podrá interpretarse de dos maneras: [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos*". Primera edición 2009, Ed. alfaomega.

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

Estas dos definiciones son complementarias, una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica pero ambas procuran el esclarecimiento y la interpretación de la información en los medios informáticos.

- ✓ Forensia en Redes (network forensics): para comprender esta definición es necesario conocer la manera como los protocolos, las configuraciones y las infraestructuras de comunicaciones operan. Para ser capaz de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado, el profesional forense debe entender las operaciones de las redes de computadores, seguir los protocolos y la formación criminalística.

- ✓ Forensia Digital (digital forensics): es una forma de aplicar conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes. O como una disciplina especializada que procura el esclarecimiento de los hechos en eventos que podrían catalogarse como incidentes, fraudes o usos indebidos en el contexto de la justicia especializada. O como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos*". Primera edición 2009, Ed. alfaomega.

7.4.2. Importancia de la computación forense

Los crímenes informáticos, su prevención y procesamiento se vuelven cada vez más importantes en la actualidad. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática. Sin embargo, la importancia real de la informática forense proviene de sus objetivos.

7.4.3. Objetivos de la computación forense

La informática forense tiene tres objetivos:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas la principal es la recolección de evidencia.

7.4.4. Uso de la computación forense

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria y no tienen que estar directamente relacionados con la informática forense:

- ✓ Prosecución criminal: evidencia incriminatoria puede ser usada para procesar una variedad de crímenes incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Litigación civil: casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

- ✓ Investigación de seguros: la evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- ✓ Temas corporativos: puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial y aún de espionaje industrial.

- ✓ Mantenimiento de la ley: la informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

7.4.5. Evidencia digital

La evidencia digital es cualquier información que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. Este es un término utilizado de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal.

7.4.5.1. Categorías de la evidencia digital

1. Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.). [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).

3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

7.4.5.2. Características legales de la evidencia digital

Para que la evidencia contenida en medios electrónicos sea admisible en un proceso judicial, esta debe cumplir con las siguientes características legales:

- ✓ Autenticidad: es aquella característica que muestra que los medios originales no han sido alterados, busca confirmar que los registros aportados correspondan a la realidad identificada en la fase de identificación y recolección de la evidencia.

  En medios no digitales, la autenticidad de las pruebas no se refuta, es decir que todas las pruebas que se aportan en la corte serán validas para la demostración de los hechos. Sin embargo en los medios digitales resulta complicado aplicar lo anterior, dada la volatilidad y alta manipulación que se presenta en los medios de almacenamiento electrónico.

  Para verificar la autenticidad de los registros digitales, se requiere desarrollar y configurar mecanismos que aseguren la integridad de los archivos y el control de cambios en los mismos. Al contar con estos mecanismos, se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Confiabilidad: nos dice, que si efectivamente los elementos probatorios aportados provienen de fuentes que son creíbles, verificables y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue.

  Cuando se logra configurar una infraestructura de computación que asegure la evidencia, se busca demostrar que los registros electrónicos son confiables para ser identificados, recolectados y verificados.

- ✓ Completitud o suficiencia de la evidencia: es la presencia de toda la evidencia necesaria para adelantar el caso. Frecuentemente la falta de pruebas ocasionan la dilatación o la terminación de procesos que podrían haberse resueltos.

- ✓ La conformidad con las leyes y regulaciones de la administración de la justicia: se refiere a los procedimientos aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien aun no existe en algunos Códigos Procesal Penal una ley que contemple las actividades requeridas para aportar evidencia digital a los procesos judiciales, ya existen iniciativas internacionales en donde se establecen lineamientos de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos.

Cuando se tiene acceso a evidencia digital por medios no autorizados y no existen medios para probar su autenticidad, confiabilidad y suficiencia, los elementos aportados carecerán de la validez requerida y podrán ser tachados de falsos. La evidencia obtenida de este modo no ofrece maneras para comprobar las posibles hipótesis que se hayan hecho sobre el caso, dadas las irregularidades que enmarcan su presentación. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

La evidencia digital es la materia prima para los investigadores y la tecnología informática es la parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante de las infraestructuras de computación y comunicaciones es preciso detallar las características propias de la evidencia en este entorno. La evidencia digital en este sentido es la búsqueda de la verdad y posee entre otras características las siguientes: es volátil, anónima, duplicable, alterable, modificable y eliminable.

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos como en técnicas y herramientas tecnológicas; para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito.

7.4.6. Principios de la computación forense

Existe un número de principios básicos en el proceso investigativo de la informática forense, a continuación se consideran algunos de estos principios para mantener la integridad del procedimiento forense:

- ✓ Esterilidad de los medios informáticos de trabajo: es decir que los medios informáticos utilizados por los profesionales en esta área deben estar certificados de tal manera que estos no hayan sido expuestos a variaciones magnéticas, ópticas o similares.

- ✓ Verificación de las copias en medios informáticos: las copias efectuadas en los medios previamente esterilizados deben ser idénticas al original del cual fueron almacenadas. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados: el investigador debe ser el custodio de su propio proceso; es decir cada uno de los procesos realizados, las herramientas utilizadas y los resultados obtenidos del análisis de los datos, deben estar claramente documentados de tal manera que cualquier persona externa pueda revisarlo.

- ✓ Mantenimiento de la cadena de custodia de la evidencia digital: se refiere a documentar la custodia, es decir quien la entregó, cuándo, en qué estado, como se ha traspasado, quien ha tenido acceso a ella, entre otras.

- ✓ Informe y presentación de los resultados obtenidos del análisis de los medios informáticos: la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones.

- ✓ Administración del caso realizado: los investigadores forenses deben prepararse para declarar ante un jurado o juicio, por tanto es probable que en el curso de la investigación o del caso lo puedan llamar a declarar en ese instante o mucho tiempo después. Por tanto el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

- ✓ Auditoría de los procedimientos en la investigación: es recomendable que el investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

7.4.7. Herramientas empleadas por la computación forense

Las herramientas informáticas son la base esencial para el análisis de las evidencias digitales en los medios informáticos. En la actualidad existen cientos de herramientas las cuales se pueden clasificar en cuatro grupos principales.

7.4.7.1. Clasificación de las herramientas

a. Herramientas para la recolección de evidencia: existen una gran cantidad de herramientas para recuperar evidencia, pero el uso de herramientas sofisticadas se hace necesario debido a:

- ✓ La gran cantidad de datos que pueden estar almacenados en un computador.
- ✓ La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- ✓ La necesidad de recopilar la información de una manera exacta y que permita verificar que la copia es exacta.
- ✓ Limitaciones de tiempo para analizar toda la información.
- ✓ Facilidad para borrar archivos de computadores.
- ✓ Mecanismos de encriptación o de contraseñas.

b. Herramientas para el monitoreo y control de computadores: algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

Existen algunos programas simples como recolectores de pulsaciones del teclado (key loggers), que guardan información sobre las teclas que son presionadas, hay otros que guardan imágenes de la pantalla que ve el usuario del computador y hasta casos donde la máquina es controlada remotamente.

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

El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensible, tienen mecanismos para validar el ingreso, pero debido a que no existe nada como un sitio cien por ciento seguro se debe estar preparado para incidentes.

d. Herramientas de hardware: debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información, se han diseñado varias herramientas como “Portable Evidence Recovery Unit”.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses están algunas herramientas aplicadas en todo el proceso de la investigación forense tales como: FORENSIC TOOLKIT, Encase, WinHex, FIRE, Snort, Ossim, Fport, Stunnel, PyFlag, entre otras.

Si bien las herramientas mencionadas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto. [1]

[1] Jeimy Cano. “*Computación Forense. Descubriendo los rastros informáticos”*. Primera edición 2009, Ed. alfaomega.

7.4.8. Metodología de la investigación forense

Como en todo proceso de análisis existe una metodología a seguir que nos marca los pasos a desarrollar de forma que siempre acabaremos con los cabos bien atados y con unos resultados altamente fiables.

7.4.8.1. Etapas de la investigación forense

1. Adquisición: significa copiar de una manera especial el contenido en bruto de la información del sistema en observación. Luego se trabajará sobre esta copia dejando intacta la información original.

   Esta tarea se hará no arrancando la computadora por los medios convencionales sino accediendo a los volúmenes en modo de sólo lectura para que ni un byte sea alterado desde el momento en que empieza la intervención. Hay que tener en cuenta que el simple booteo (arranque) de una computadora altera por lo menos algunos archivos en sus contenidos y fechas, varía la cantidad total de archivos, etc.

   Lo mismo ocurre cuando abrimos un archivo aunque solo sea para leerlo o imprimirlo. Se puede rastrear todo este tipo de actividad en una computadora. La adquisición puede involucrar desde un disquette o un disco duro de una computadora hasta un conjunto de discos de un servidor, un juego de cintas o varias computadoras de una organización.

2. Validación y preservación de los datos adquiridos: por medios matemáticos se debe calcular de manera normalizada un código único correspondiente a esa combinación única de bytes que constituye la totalidad del medio en observación. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

Este código de validación ha de ser lo suficientemente complejo como para impedir que sea generado en forma reversa con fines dolosos y normalizado como para que cualquier auditor independiente pueda por su cuenta verificar la autenticidad de la imagen tomada y así establecer una cadena de custodia consistente. Desde este momento ya se pueden efectuar copias exactamente iguales de la imagen a los efectos para que diferentes actores puedan conservar una copia de seguridad.

3. Análisis y descubrimiento de evidencia: se procede a realizar una batería de pruebas en el laboratorio sobre la copia validada. Es posible analizar y buscar información a diferentes niveles. Partimos de la base de que el usuario sospechoso de una actividad ilícita puede haber borrado la información que lo compromete o pudo haberla ocultado almacenándola por medios no convencionales.

   Estas búsquedas están orientadas por cada caso en particular y aquí contamos con la información que provee quien solicita el servicio. Se pueden buscar:

   - ✓ Archivos borrados, creados, accedidos o modificados dentro de determinado rango de fechas.
   - ✓ Tipos de archivos con un formato particular que hayan sido alterados, por ejemplo archivos de un sistema de contabilidad renombrados como archivos de un procesador de texto.
   - ✓ Imágenes, mensajes de correo electrónico, actividad desarrollada en internet.
   - ✓ Diferentes niveles de palabras claves tales como un número telefónico, el nombre de una ciudad o una empresa, etc. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

En base a este análisis se determina un patrón de comportamiento del usuario en cuanto a la creación, modificación y borrado de mensajes, etc.

4. Informe: se presenta un informe escrito en un lenguaje técnico y claro, y un CD donde se hace accesible al usuario no especializado de una forma ordenada la evidencia recuperada y su interpretación.

7.4.9. La mente de los intrusos

Hablar de la mente de los intrusos se refiere a las motivaciones de sus acciones y su manera de actuar para avanzar donde otros no lo hacen. Revisar la mente de los atacantes es avanzar en un terreno donde la imaginación es más importante que el conocimiento.

No podemos comparar a un intruso cuya motivación está más allá del reto y del reconocimiento por sus capacidades, con un hacker que busca una manera de mostrar que el manual no está completo y requiere completarse con una nueva experiencia y comportamiento inesperado del sistema.

7.4.9.1. Motivaciones de los intrusos

Los atacantes pueden tener muchos motivos para violar la seguridad en una red y entre estos están: [1]

Motivaciones	Ciberterrorista	Phreakes	Script Kiddes	Crackers	Desarrollador de virus	Atacante interno
Reto		X			X	X
Ego		X	X		X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

7.4.9.2. Tipos de intrusos

- ✓ Ciberterrorista: este atacante usa los medios electrónicos para recabar información, efectuar inteligencia estratégica e interconectar a todos sus simpatizantes alrededor de una red de comunicación eficiente, práctica y efectiva.

  Las redes de comunicación le ofrecen al terrorista un escenario de anonimato, imperceptibilidad y adaptación que canaliza en comunicaciones y actividades que aparentemente son normales para los navegantes de Internet, pero que llevan mensajes que solo pueden ser identificados y analizados por sus compañeros ideológicos.

  El ciberterrorista enterado de las interconexiones genera inestabilidad en los sistemas, incertidumbre sobre la operación y fallas de las comunicaciones, creando un ambiente propicio para iniciar una guerra de desinformación y actuar para generar la sensación de pérdida de control que llevará a las autoridades a una experiencia semejante al terror y vulnerabilidad.

- ✓ Phreakers (amantes del teléfono): cree en la telefonía sin costo, en un mundo abierto para construir y crear lazos más allá del mundo real, el reto de estos es lograr expandir y evadir el cerco de los controles establecidos, bien sea por convicción propia o por alguna recompensa económica. En algunos momentos estos se sienten como los reivindicadores de los derechos de los usuarios, al decirles a los operadores que su tarifa no compensa el servicio que prestan. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Script Kiddies: son todos aquellos que mirando los logros de los hackers, utilizan las herramientas y técnicas utilizadas por estos para lograr penetrar sistemas o inutilizar sistemas de comunicaciones o tecnología de información, estos son motivados por su curiosidad para experimentar y ver que tan reales son los efectos de las armas de los hackers.

  Los Script Kiddies son una amenaza latente ya que las herramientas diseñadas por los hackers o curiosos informáticos estarán disponibles en la red esperando que algún curioso experimente con ellas, exponiendo a las organizaciones a situaciones inesperadas que están fuera de los reportes normales de operaciones.

- ✓ Crackers: tienen como objetivo vulnerar un sistema con una motivación de venganza o económica. Es catalogado como un mercenario que vende sus conocimientos al mejor postor para tener una ventaja competitiva en un mundo dominado por la tecnología. Este mercenario tecnológico sabe que la tecnología siempre tendrá fallas y por tanto las estudia y analiza para concebir nuevas formas de vender su servicio, no para proteger a las organizaciones sobre nuevas amenazas, sino para crearlas y esperar el tiempo requerido para lucrarse.

- ✓ Desarrollador de virus: los mueve la necesidad de ir más allá de lo que muestra la realidad esto los lleva a generar una estrategia de espionaje silencioso, que le permiten recabar información necesaria para mantener una posición de ventaja sobre otra persona u organización.[1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Atacantes Internos: puede ser cualquier persona, son empleados insatisfechos o que han terminado en malos términos con la organización y solo se requiere un disparador o detonante para que se transforme en un potencial delincuente que encuentre en la organización la manera para demostrar que existe y requiere atención a su situación

Como se puede observar la mente de los atacantes es compleja y sus motivaciones son varias.

7.4.10. Retos tecnológicos para la computación forense

En la actualidad los atacantes han descubierto en las tecnologías de información no solo un incentivo y motivación para materializar sus acciones; sino también maniobras para evadir las investigaciones.

Debido a esto se analizarán algunas estrategias tecnológicas que pueden ser aprovechados por los criminales informáticos para entorpecer la investigación en curso.

- ✓ Archivos cifrados: es una de las técnicas más usadas por los atacantes, una de sus actividades delictivas es cifrar la información residente en el dispositivo de almacén con algoritmos, utilizando llaves generalmente largas, que limite un ataque de fuerza bruta de quien intente descifrar lo que se encuentre allí.

- ✓ Esteganografía en video: es una técnica a través de la cual, manipulando la estructura interna de un archivo inicial logramos esconder (no cifrar) otro en este. Si bien este engaño ha sido ampliamente usado, en la actualidad ya existen herramientas que buscan detectar el uso del mismo. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Rastros en ambientes virtuales: los entornos virtuales buscan aislar el sistema operativo de otro, es probable que comparta segmentos de memoria en conjunto con instancias de otros sistemas operativos en ejecución, lo cual puede hacerlo vulnerable a una falla generalizada de la máquina original que lo contiene.

- ✓ Información almacenada electrónicamente en memoria volátil: en la actualidad es posible capturar lo que hay en la memoria de un computador encendido y es viable exportar los resultados del mismo a un archivo para su análisis posterior. Por lo antes mencionado se recomienda a los investigadores que se encuentran en el lugar del crimen, no apagar la máquina si la encuentran encendida dado que la información volátil residente en la memoria es una clave para conocer lo que ha ocurrido.

- ✓ Análisis de sistemas en vivo: cuando un investigador se enfrenta al análisis de sistemas en vivo sabe que la modificación de archivos en el sistema revisado siempre será un riesgo a mitigar. Es por esto que las técnicas que se utilicen para este trabajo deben ser procedimientos formales y probados que limiten la modificación involuntaria de la escena del crimen.

  Este es un reto tecnológico crítico para los investigadores forenses, pues saben que un atacante informado y conocedor como él puede poner en duda sus procedimientos y el uso de sus herramientas para causar incertidumbre en los resultados de la información almacenada electrónicamente. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

7.5. Métodos Anti-forenses

Los atacantes evolucionan tan rápido como la inseguridad de la informática, que cuando un nuevo desarrollo tecnológico hace su aparición, surge un nuevo producto para evidenciar las vulnerabilidades del diseño de la aplicación o herramienta. En este entorno las herramientas utilizadas para adelantar procedimientos de informática forense, han generado la aparición de las llamadas técnicas anti-forenses. Es decir las técnicas anti-forenses retan a los investigadores, al hacer fallar las herramientas forenses disponibles.

7.5.1. Definición de método anti-forense

Las técnicas o herramientas anti–forenses se pueden definir como:

- ✓ Limitar la identificación, recolección y validación de datos electrónicos.
- ✓ Cualquier intento de comprometer la disponibilidad de la evidencia para un proceso forense.
- ✓ Cualquier intento para limitar la cantidad y calidad de la evidencia forense.

Estas técnicas proporcionan a los atacantes una ventaja inusual sobre los investigadores en computación forense, ya que al hacerse efectivas sobre la evidencia digital, pueden comprometer fácilmente la confianza y claridad de la misma en un proceso. Así mismo sugiere a los investigadores observar con un mayor detalle las evidencias digitales encontradas en una escena del crimen lo que exige replantear los protocolos para investigaciones pasadas y futuras. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

7.5.2. Clasificación de los métodos anti-forenses

A medida que se investiga más sobre las técnicas anti-forenses se han generado varias clasificaciones, entre las más conocidas esta: destruir, ocultar, eliminar y falsificar la evidencia.

A continuación se explica brevemente cada método de la clasificación antes mencionada:

- ✓ Destrucción de la evidencia: el principal objetivo de esta técnica es evitar que la evidencia sea encontrada por los investigadores y en caso de que estos la encuentren, disminuir sustancialmente el uso que se le puede dar a dicha evidencia en la investigación formal. Este método no busca que la evidencia sea inaccesible si no que sea irrecuperable. Esto implica que se deben destruir, desmantelar o en su defecto modificar todas las pruebas útiles para una investigación. Así como en la vida real cuando ocurre un crimen y el criminal quiere destruir todo rastro o evidencia se vale de una serie de herramientas que le facilitan este objetivo. Existen dos niveles de destrucción de la evidencia:

  1. Nivel Físico: A través de campos magnéticos.

  2. Nivel Lógico: Busca reinicializar el medio, cambiar la composición de los datos, sobrescribir los datos o eliminar la referencia a los datos.

  Existe una variedad de herramientas para la destrucción de evidencia de las cuales se pueden valer los intrusos para realizar este método anti-forense. Un ejemplo de herramientas son: Wipe, Shred, PGP Secure Delete, Evidence Eliminator y Sswap. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Ocultar la evidencia: este método tiene como principal objetivo hacer inaccesible la evidencia para el investigador. No busca manipular, destruir o modificar la evidencia sino hacerla lo menos visible para el investigador.

  Esta técnica puede llegar a ser muy eficiente de ser bien ejecutada pero conlleva muchos riesgos para el atacante o intruso, puesto que al no modificar la evidencia de ser encontrada puede ser válida en una investigación formal y por lo tanto servir para la incriminación e identificación del autor de dicho ataque. Este método puede valerse de las limitaciones del software forense y del investigador, atacando sus puntos ciegos o no usuales de búsqueda de alguna anomalía. Una de las herramientas utilizadas por los atacantes es la esteganografía la cual versa sobre técnicas que permiten la ocultación de mensajes u objetos, dentro de otros llamados portadores, de modo que no se perciba su existencia. En el mercado se pueden encontrar muchos instrumentos fáciles de usar de bajo costo que pueden ayudar a realizar esta técnica anti-forense.

- ✓ Eliminación de las fuentes de la evidencia: este método tiene como principal objetivo neutralizar la fuente de la evidencia, por lo que no es necesario destruir las pruebas puesto que no han llegado a ser creadas. Por ejemplo, en el mundo real cuando un criminal utiliza guantes de goma para utilizar un arma lo que está haciendo es neutralizando y evitando dejar huellas dactilares en el arma. Así mismo en el mundo digital esta neutralización de las fuentes de la evidencia aplica.

  Una de las acciones que los atacantes pueden llevar a cabo para realizar este método anti-forense es la desactivación de los log de auditoría del sistema que esté atacando. [1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

- ✓ Falsificación de la evidencia: este método busca engañar y crear falsas pruebas para los investigadores forenses logrando así cubrir al verdadero autor, incriminando a terceros y por consiguiente desviar la investigación con lo cual sería imposible resolverla de manera correcta.

  El ejercicio de este método se vale en una edición selectiva de las pruebas creando evidencias incorrectas y falsas que corrompen y dañan la validez de dichas pruebas en una investigación forense formal, por lo cual no podrán ser tomadas en cuenta como evidencias.[1]

[1] Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.

VIII. DESARROLLO DEL SUBTEMA

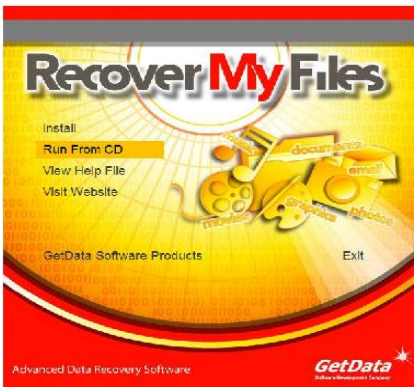
8.1. ¿Qué es RecoverMyFiles?

Es una herramienta que ha sido diseñada para recuperar información borrada físicamente del disco duro de una manera sencilla. Con esta aplicación se pueden recuperar los archivos perdidos por obra de virus, por una equivocación o por cualquier otro problema que haya hecho que los datos se perdieran. Este puede recuperar los datos incluso si el disco duro fue formateado por completo.

Figura1. Presentación del programa

Las versiones de RecoverMyFiles con licencia, pueden ser instaladas desde Internet, un CD, una Memoria USB o corrido directamente desde un CD. Las licencias tienen costos que van desde los U$ 50 hasta U$80, según la versión. También se pueden conseguir versiones gratis de este programa, las cuales restringen la recuperación de archivos desde el disco duro.

Figura2. Corriendo el programa desde un CD



RecoverMyFiles recupera archivos borrados o perdidos, discos formateados, discos RAW, controladores perdidos y otros. Recupera datos de tipo documentos, gráficos, multimedia, juegos, archivos, entre otros.

8.2. Ventajas del programa

- ✓ Recupera archivos borrados que han sido eliminados de la papelera de reciclaje.
- ✓ Recupera documentos, fotos, vídeo, música y otros.
- ✓ Recupera datos de disco duro, tarjeta de cámara, memoria USB, disco flexible o cualquier otro medio de almacenamiento, aun si este fue formateado por completo.

8.3. Desventajas del programa

- ✓ Los archivos recuperados solo pueden ser guardados en una unidad física alterna.
- ✓ Tarda mucho tiempo en recuperar los archivos, cuando se elige la opción “búsqueda completa”.
- ✓ Mientras más grande es el volumen de la unidad de almacenamiento, mayor será el tiempo de búsqueda.

8.4. Requerimientos mínimos para instalar RecoverMyFiles:

- ✓ Windows 95, 98, ME, NT, 2000, XP, 2003.
- ✓ 3 megabytes de espacio de disco.
- ✓ 64 megabytes de RAM (recomendado 128 o más megabytes).

8.5. Funcionamiento de RecoverMyFiles

RecoverMyFiles encuentra los archivos eliminados haciendo una búsqueda en todo el disco duro para localizar los datos por su estructura de archivo interno (el contenido de encabezado y pie de página).

Debido a que el nombre original del archivo se destruye, esta aplicación llama a todos los archivos recuperados de la siguiente manera: “nombre.tipo de archivo".

La pantalla de bienvenida que presenta RecoverMyFiles permite seleccionar entre los siguientes tipos de búsqueda:

- ✓ Fast File Search (búsqueda rápida de archivo).
- ✓ Complete File Search (búsqueda completa de archivo).
- ✓ Fast Format Recover (recuperar formato rápido).
- ✓ Complete Format Recover (recuperar formato completo).

Tabla1. Descripción de los tipos de búsqueda.

Tipo de búsqueda	**Encontrará**	**Duración de la búsqueda.**
Búsqueda rápida de archivo.	Archivos eliminados.	Aproximadamente 20 minutos.
Búsqueda completa de archivo (incluye una búsqueda rápida).	Archivos eliminados y archivos perdidos (se recupera archivos de Microsoft Windows con referencia destruida).	1 a 10 horas (en función de los tipos de archivos seleccionados).
Recuperar Formato rápido	Se utiliza cuando una unidad o partición ya no es visible, pero la unidad no ha sido formateada (se recuperan las estructuras completas de las carpetas).	20 o más minutos.
Recuperar formato completo	Se utiliza cuando una partición se ha eliminado cuando una nueva partición ha sido creada y formateada (reconstruye particiones después de un formato y encuentra todos los archivos en la partición perdida).	1 a 10 horas, dependiendo del tamaño del disco duro.

Es recomendable que en primera instancia se pruebe una "búsqueda rápida de archivos ", ya que se podría encontrar los archivos en 20 minutos. Si no se localizan los archivos con este tipo de búsqueda, se puede intentar una "búsqueda completa de archivos" y si se ha formateado el disco duro, se puede seleccionar la opción "recuperar formato completo".

La siguiente pantalla que presenta RecoverMyFiles, permite seleccionar la unidad en donde se realizará la búsqueda. Esta muestra automáticamente todas las unidades externas conectadas al equipo como: discos duros, cámara digital, USB, etc.

La siguiente pantalla permite ver todos los tipos de archivos que se pueden recuperar, se pueden realizar múltiples selecciones de formatos. Algunos archivos no los clasifica en ningún tipo, pero aún así se pueden recuperar igual que el resto.

Para comenzar la búsqueda se selecciona “start” y en seguida aparece una ventana que muestra el progreso de la búsqueda. Una vez que se ha escaneado la unidad completamente aparece en pantalla los resultados de la búsqueda.

La pantalla de resultados, suele mostrar tamaño, tipo, estado y fecha de creación de los archivos encontrados. Esta misma pantalla cuenta con un área preview, que se activa al dar click sobre uno de los archivos encontrados, esta permite conocer el contenido de los archivos.

Según su estado los archivos pueden ser:

- ✓ Overwritten (Sobrescrito): el archivo original fue completamente sobre-escrito y no puede ser recuperado.
- ✓ Poor (Pobre): la búsqueda indica que entre el 1% y 50% del archivo puede ser recuperado.

- ✓ Médium (Medio): la búsqueda indica que entre el 51% y 90% del archivo puede ser recuperado.
- ✓ Good (Bueno): la búsqueda indica que entre el 91% y 99% del archivo puede ser recuperado.
- ✓ Very Good (Muy bueno): el archivo puede ser completamente recuperado.

Para salvar los archivos que se muestran en la pantalla es necesario seleccionarlos, existe la posibilidad de seleccionar los archivos de forma individual o por grupo según el tipo. Una vez seleccionados los archivos, se elige la opción salvar del menú SAVE y se indica la unidad en que estos serán guardados.

Cabe mencionar que los archivos recuperados solo pueden ser guardados en una unidad física alterna, es decir no pueden ser guardados en la misma unidad de donde fueron eliminados, esto puede ser en otro disco duro, memoria flash, disquete, CD, DVD u otros.

Algunos puntos importantes que hay que conocer del proceso de búsqueda son:

1. Seleccionar entre 1 y 10 tipos archivos.
2. En archivos MP3, el tiempo de búsqueda se reduce considerablemente y se debe buscar por separado.
3. Este programa también funciona si una nueva versión de Windows se ha instalado, sin embargo cualquier archivo eliminado que haya sido sobrescrito por la nueva instalación está permanentemente destruido.
4. Si solamente una letra de unidad de almacenamiento es visible (por ejemplo, "D: \") la búsqueda se realizará en la letra de la unidad.
5. Para recuperar una mayor cantidad de datos, es mejor no utilizar el disco duro del ordenador para guardar información o instalar programas, porque se puede sobrescribir los datos que se quieren recuperar.

8.6. Prueba de RecoverMyFiles versión 3.9.2

El proceso llevado a cabo para conocer y valorar el funcionamiento del programa consistió en: eliminar algunos archivos con el método estándar de Windows, instalar y ejecutar el programa RecoverMyFiles versión 3.9.2 para hacer la recuperación de los datos.

Una vez instalado el programa el proceso que se realizó, se puede resumir en los siguientes pasos (ver pantallas en anexos):

1) Seleccionar el tipo de búsqueda
2) Seleccionar la unidad para buscar.
3) Seleccionar tipos de archivos a buscar.
4) Ejecutar la búsqueda.
5) Seleccionar archivos de la pantalla de resultados que desea recuperar.
6) Salvar archivos recuperados.

Es importante mencionar que los archivos eliminados tenían formatos diferentes y estaban almacenados en diferentes dispositivos de almacenamiento como: disco duro, memorias USB y memorias SD.

También se debe comentar que cuando término la búsqueda, se observó que algunos archivos estaban en buen estado y otros no. También se observó que ninguno de los archivos tenían sus nombres originales, por lo cual no se sabia que archivos recuperar, pero esto se resolvió usando el preview de la pantalla de resultados.

Después de realizar una serie de pruebas con RecoverMyFiles, se encontró que es un programa bueno debido a que, puede recuperar bastante información y encuentra archivos ocultos o con extensión desconocida, pero presenta inconvenientes tales como: no recupera información cuando el disco duro está dañado y no recupera los archivos con el nombre de origen.

A continuación se presenta una tabla que refleja el número de pruebas realizadas y la relación que existe entre el tiempo que tienen los archivos de estar eliminados y el estado de los mismos al ser recuperados.

Tabla2. Resultados de las pruebas

No. Prueba	**Tiempo de eliminación (días)**			**Calidad del archivo**				
	1	3	5 o más	S	P	M	B	MB
1	x			x				
2		x			x			
3		x					x	
4			x	x				
5	x							x
6		x						x
7			x	x				
8	x							x
9			x					x
10	x				x			
11		x						x
12			x					x
13		x						x
14		x					x	
15		x						x
16			x					x
17		x						x
18		x						x
19		x		x				
20			x					x
Total	4	10	6	4	2	0	2	12

Simbología: S: Sobrescrito, P: Pobre, M: Medio, B: Bueno y MB: Muy Bueno.

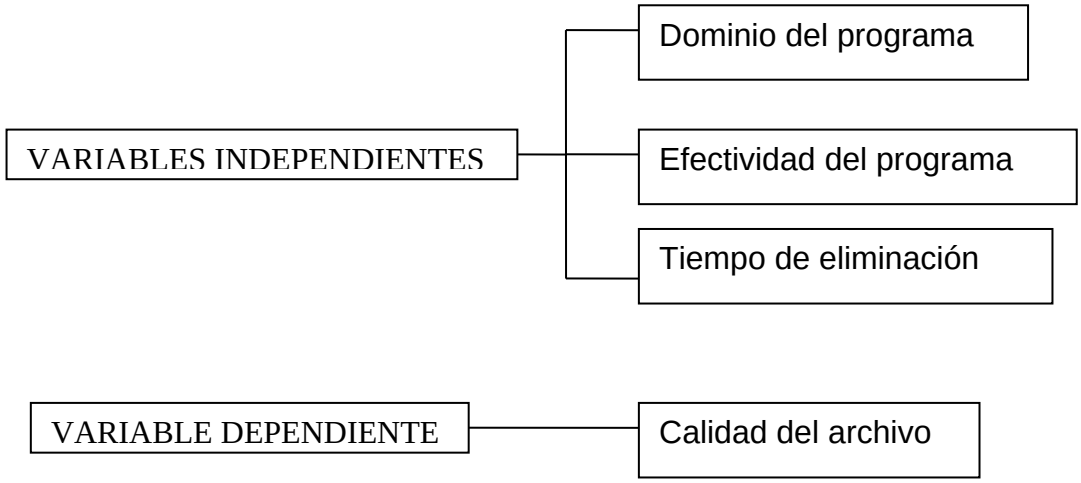
De la tabla anterior se puede concluir que entre menor tiempo tengan los archivos de estar eliminados, mejor será su estado.

IX. HIPÓTESIS Y VARIABLES

9.1. Hipótesis

La recuperación de archivos en el Laboratorio de Criminalística de la Policía Nacional será más efectiva con la aplicación de las herramientas proporcionadas por el programa RecoverMyFiles.

9.2. Esquema de las variables



9.3. Operacionalización de las variables

Variables	Indicador	Escala	Fuentes	Instrumentos
Dominio del programa	% de dominio	- Mucho - Poco - Nada	Usuario	Encuesta
Efectividad del programa	% de efectividad	- Excelente - Buena - Regular - Mala	Usuario	Encuesta
Tiempo de eliminación	Cantidad de días	1 día 3 días 5 o mas días	Usuario	Observación
Calidad del archivo recuperado	Cantidad de archivos recuperados	- Sobrescrito - Pobre - Medio - Bueno - Muy Bueno	Usuario	Observación

9.4. Resultados

En esta investigación se quiso dar respuesta a los objetivos de la misma, por tanto se aplicaron diferentes instrumentos como: entrevista, encuesta y observación. Los datos analizados a continuación fueron obtenidos de la encuesta, que proporciono junto con la observación los resultados de este estudio.

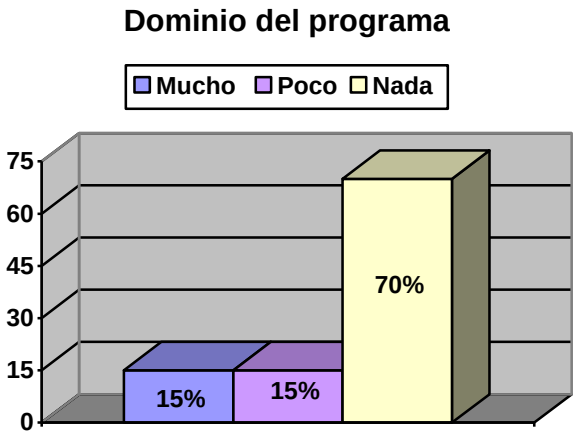
9.4.1. Variable Dominio del programa

Tabla de frecuencia

Dominio del programa	Frecuencia
Mucho	4
Poco	4
Nada	18
Total	26

Tabla de porcentaje

Dominio del programa	Porcentaje (%)
Mucho	15
Poco	15
Nada	70
Total	100



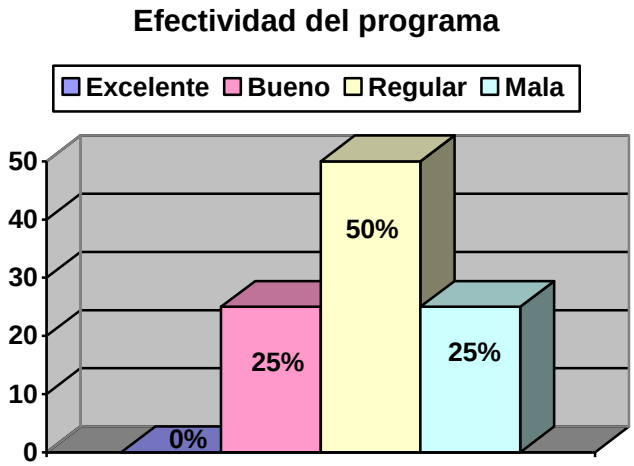
9.4.2. Variable Efectividad del programa

Tabla de frecuencia

Efectividad del programa	Frecuencia
Excelente	0
Buena	2
Regular	4
Mala	2
Total	8

Tabla de porcentaje

Efectividad del programa	Porcentaje (%)
Excelente	0
Buena	25
Regular	50
Mala	25
Total	100



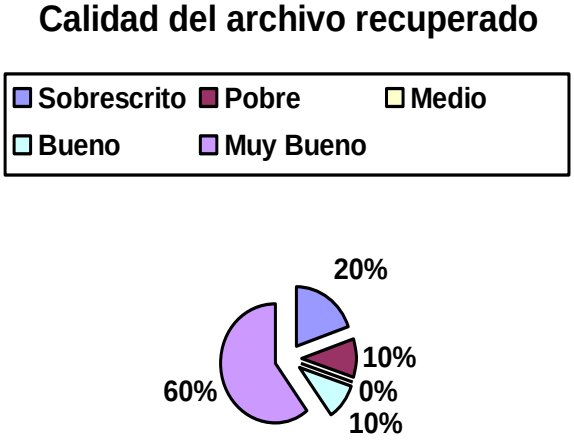
9.4.3. Variable Calidad del archivo recuperado

Tabla de frecuencia

Calidad del archivo recuperado	Frecuencia
Sobrescrito	4
Pobre	2
Medio	0
Bueno	2
Muy Bueno	12
Total	20

Tabla de porcentaje

Calidad del archivo recuperado	Porcentaje (%)
Sobrescrito	20
Pobre	10
Medio	0
Bueno	10
Muy Bueno	60
Total	100



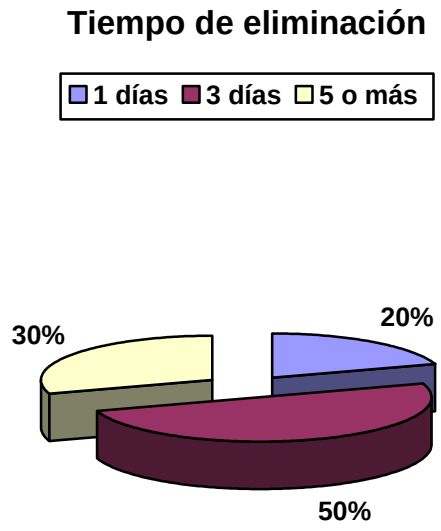
9.4.4. Variable Tiempo de eliminación

Tabla de frecuencia

Tiempo de eliminación	Frecuencia
1 día	4
3 días	10
5 días o mas	6
Total	20

Tabla de porcentaje

Tiempo de eliminación	Porcentaje (%)
1 día	20
3 días	50
5 días o mas	30
Total	100



X. DISEÑO METODOLÓGICO

Para las siguientes clasificaciones se usará el criterio del libro “Investigar es Fácil” del autor Valinda Sequeira Valero y Astralia Cruz Picón.

10.1. Tipo de estudio

Según su aplicabilidad esta investigación es de tipo teórica; porque se tomó como base de esta, un conjunto de conocimientos generales sobre la informática forense.

Según el tipo de profundidad del conocimiento es descriptiva; por que estudiamos los factores que influyen en la pérdida de archivos pero no damos una medida preventiva que evite estos daños.

Y según la amplitud con respecto al proceso de desarrollo del fenómeno esta investigación es de tipo transversal; por que se valora la importancia de la aplicación en un periodo de corta duración lo que corresponde al año 2011.

10.2. Objeto de estudio

Vamos a estudiar la funcionalidad y los beneficios de la aplicación.

10.3. Universo o población

Se refiere al conjunto de individuos que se desea representar en la investigación. En esta investigación el universo está conformado por 98 policías que laboran en el Laboratorio de Criminalística de la Policía Nacional.

10.4. Selección de la muestra

Es un grupo de unidades que representan al universo y que contiene las mismas características y atributos del mismo. Para esta investigación se seleccionó una muestra de 2 operadores por cada departamento que conforma el Laboratorio de Criminalística.

10.5. Técnicas aplicadas en la recolección de la información

Para realizar esta investigación se aplicaron una secuencia de técnicas que contribuyeron a la recolección de los datos:

Consultas bibliográficas: este fue el método inicial para la obtención de información sobre los términos, definiciones y análisis que se relacionan con el tema. Se recopilaron archivos vía Internet proporcionados por diferentes personas expertas en el tema.

Entrevista: se hicieron entrevistas con el fin de conocer la problemática, los antecedentes y la historia del Laboratorio de Criminalística de la Policía Nacional. Esta información se obtuvo del personal que labora actualmente en el Laboratorio de Criminalística de la Policía Nacional.

Encuesta: se hicieron encuestas con el fin de conocer el dominio que se tenía respecto a informática forense y RecoverMyFiles. Se recopiló información de los operadores del sistema con que cuenta el Laboratorio de Criminalística.

Observación: se utilizó este método con el fin de analizar el funcionamiento del programa y así conocer las ventajas y desventajas que este tiene. Esta información se obtuvo haciendo pruebas prácticas, que consistían en borrar información intencionalmente y luego emplear el programa para recuperarla.

XI. CONCLUSIÓN

Este estudio nos permitido conocer el mundo de la informática forense y las herramientas que esta emplea para lograr sus objetivos, esto nos ayudó a seleccionar una de estas herramientas para realizar un análisis de su funcionamiento.

El análisis de RecoverMyFiles versión 3.9.2 como una herramienta usada por la informática forense para la recuperación de archivos, nos permitió observar las características, ventajas y beneficios que este brinda.

Conocer la informática forense y el mundo que la rodea nos ayudó a comprender la importancia que tiene esta nueva ciencia en la actualidad. Y también conociendo el funcionamiento de RecoverMyFiles versión 3.9.2 se dio solución a uno de los problemas más comunes en la actualidad a como es la perdida de información, la cual es el bien mas valioso para las instituciones.

XII. BIBLIOGRAFÍA

Libros:

- Canales, Alvarado y Pineda. "*Metodología de la Investigación*".
- Valinda Sequeira Valero y Astralia Cruz Picón. "*Investigar es Fácil*".
- Jeimy Cano. "*Computación Forense. Descubriendo los rastros informáticos"*. Primera edición 2009, Ed. alfaomega.
- Tanenbaum, Andrew S. "*Redes de Computadoras*", Cuarta edición 2003, Ed. Prentice-Hall.

Webgrafia:

- www.monografias.com
- www.duiops.net/hacking/seguridad-sistemas
- www.alegsa.com.ar/Dic/seguridad

  informaticawww.wikipedia.org/wiki/Seguridad_de_la_red
- www.duiops.net/hacking/seguridad-sistemas
- www.alegsa.com.ar/Dic/archivo.php
- www.alegsa.com.ar/Notas/91.php
- www.RecoverMyFiles.com
- es.wikipedia.org
- *www.es.masterbase.com/recursos/glosario.asp*
- *es.wikipedia.org/wiki/Spamming*
- www.linguee.es/ingles-espanol/traduccion/degaussing.html

- es.wikipedia.org/wiki/BIOS
- www.alegsa.com.ar/Dic/encriptacion.php
- es.wikipedia.org/wiki/Metadato
- es.wikipedia.org/wiki/Criptografia

Documentos:

- Ana Rosa Chavarría, José Antonio Pereira & Lenin Dávila, *(2008).* "*Delitos Informáticos",* preparado por Corte Suprema de Justicia de Nicaragua.

GLOSARIO

BBS (Bulletin Board System): Sistema de Tablón de Anuncios, es un software para redes de computadoras que permite a los usuarios conectarse al sistema a través de internet o línea telefónica, utilizando un programa terminal (o telnet si es a través de internet). Es un sistema computarizado de intercambio de datos entre un grupo de personas que comparten una misma zona geográfica, donde archivos, mensajes y otra información útil pueden ser intercambiados entre los usuarios.

Sysop: es un acrónimo por system operator. Es el término comúnmente usado para designar a los administradores de los BBS. Individuo que se encarga del mantenimiento de un sistema informático y tiene el control total sobre el mismo. También se encarga de la seguridad.

Phishing: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

El término phishing proviene de la palabra pez en inglés "fishing" (pesca) haciendo alusión al acto de pescar usuarios mediante señuelos cada vez más sofisticados y de este modo obtener información financiera y contraseñas. Quien lo practica es conocido con el nombre de phisher.

Práctica delictiva en la que se utilizan correos electrónicos que parecen provenir de instituciones legítimas, como por ejemplo un banco conocido, con el fin de conseguir información personal que puede utilizarse para suplantar la identidad de un usuario.

Spam: correo basura o mensajes no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Degauss: Desmagnetizar, reducir o eliminar el cambio de calor en monitores.

BIOS (*basic input/output system*): en español sistema básico de entrada y salida, es un código de software que localiza y reconoce todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM. Es en sistema básico de entrada/salida que normalmente pasa inadvertido para el usuario final de computadoras.

Encriptación: es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas. El texto plano que está encriptado o cifrado se llama criptograma.

Metadatos: literalmente «sobre datos», son datos que describen otros datos.

En general, un grupo de metadatos se refiere a un grupo de datos, llamado *recurso*. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos.

Criptografía: literalmente «escritura oculta», es la técnica bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje. La criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la Criptología.

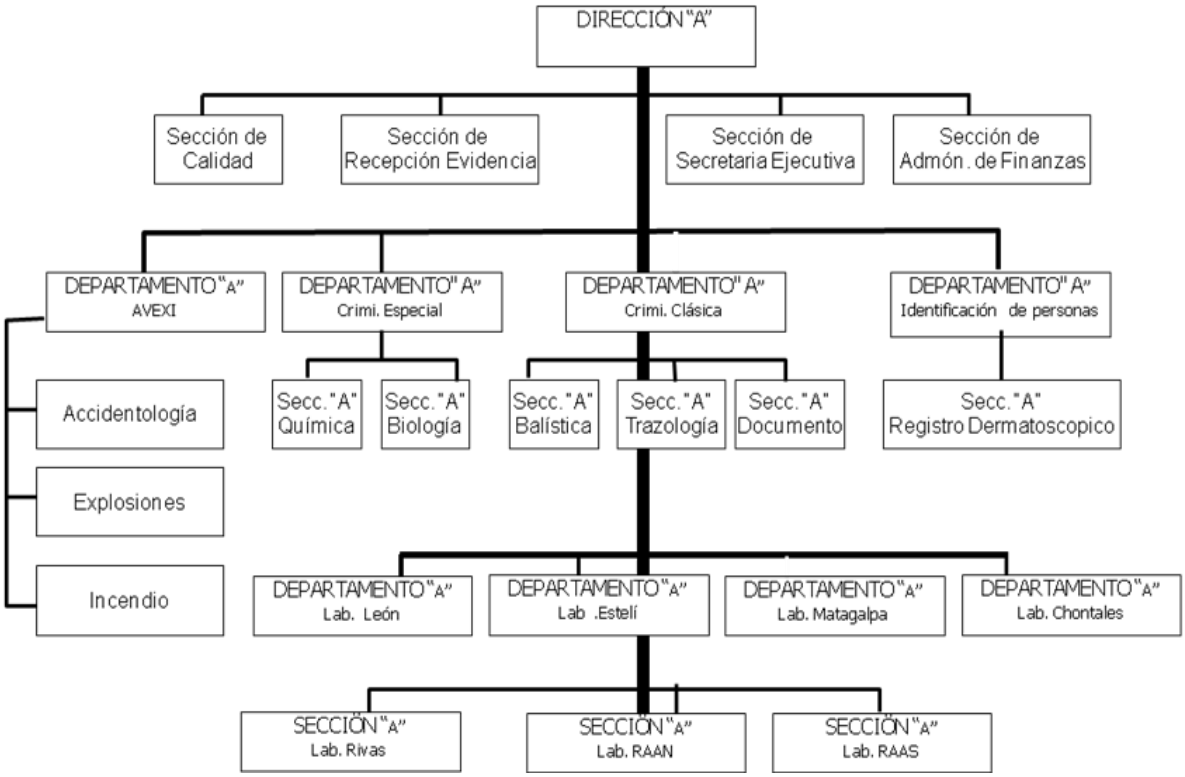
Pederastia: abuso sexual infantil, es toda conducta en la que un menor es utilizado como objeto sexual por parte de otra persona con la que mantiene una relación de desigualdad, ya sea en cuanto a la edad, la madurez o el poder.

Conexo(a): que está conectado, enlazado o guarda una relación con el resto de partes: ideas conexas; problemas conexos.

Carding: uso ilegítimo de tarjetas de créditos ajenas.

ANEXOS

ORGANIGRAMA DEL LABORATORIO DE CRIMINALISTICA DE LA POLICIA NACIONAL



ENTREVISTA #1

Universidad Nacional Autónoma de Nicaragua
Recinto Universitario Rubén Darío
Departamento de Computación

En el seminario de graduación estamos realizando un estudio sobre la informática forense y las herramientas que esta emplea, para la recuperación de archivos. El objetivo de esta encuesta es valorar el dominio que se tiene sobre este tema. Es importante mencionar que la información que se nos brinde será determinante para el logro de los objetivos de este estudio. De antemano le agradecemos por el tiempo brindado.

Guía de entrevista dirigida al Comisionado Aníbal Esteban jefe del departamento de criminalística clásica del Laboratorio de Criminalística de la Policía Nacional.

1. ¿Tiene conocimiento de algún caso donde hubo manipulación de archivo con información importante para la institución?

2. ¿Existen registros escritos del caso?

3. ¿El o los casos fueron solucionados o siguen abiertos?

4. ¿Cuántos casos se han dado de delitos informáticos?

5. ¿Tiene conocimiento de algún artículo que penalice este tipo de crímenes?, ¿mencione cuál es?

6. ¿Cuál es el método de acceso que se utiliza para entrar a los equipos?

ENTREVISTA #2

Universidad Nacional Autónoma de Nicaragua
Recinto Universitario Rubén Darío
Departamento de Computación

En el seminario de graduación estamos realizando un estudio sobre la informática forense y las herramientas que esta emplea, para la recuperación de archivos. El objetivo de esta encuesta es valorar el dominio que se tiene sobre este tema. Es importante mencionar que la información que se nos brinde será determinante para el logro de los objetivos de este estudio. De antemano le agradecemos por el tiempo brindado.

Guía de entrevista dirigida al Ing. Rueda encargado del centro de computo del Laboratorio de Criminalística de la Policía Nacional.

1. ¿Cuenta con algún software para proteger el servidor de la institución?

2. ¿Cuál es la plataforma que utiliza en el servidor?

3. ¿Tiene servidores separados o es el mismo para todos?

4. ¿El servidor es externo o interno?

5. ¿Qué topología de red tiene aplicada?

6. ¿La red es cerrada o tiene comunicación con otras redes?

7. ¿Hacen actualizaciones de software y cada cuanto tiempo lo hacen?

8. ¿Quiénes tienen acceso a la información que hay en el o los servidores?

9. ¿Ha ocurrido alguna vez algún tipo de ataque informático interno o externo contra la información de la institución?, ¿Tienen registro del acto?

ENCUESTA

Universidad Nacional Autónoma de Nicaragua
Recinto Universitario Rubén Darío
Departamento de Computación

En el seminario de graduación estamos realizando un estudio sobre la informática forense y las herramientas que esta emplea, para la recuperación de archivos. El objetivo de esta encuesta es valorar el dominio que se tiene sobre este tema. Es importante mencionar que la información que se nos brinde será determinante para el logro de los objetivos de este estudio. De antemano le agradecemos por el tiempo brindado.

Guía de encuesta dirigida al personal del Laboratorio de Criminalística de la Policía Nacional.

I. Datos generales

Departamento en que labora: _____
Cargo que desempeña: _____
Nivel académico: _____
Antigüedad: _____

II. Desarrollo de la encuesta

En las preguntas seleccione la alternativa que usted considere conveniente, marcando con una X en el espacio correspondiente.

1. ¿Conoce el término delito informático?

   Si_____ No_____

2. ¿Qué entiende por delito informático?

_____

_____

_____

3. Mencione un delito informático que usted conozca.

_____

4. ¿Conoce algún artículo del código procesal penal que sancione este tipo de delitos?

Si_____ No_____

Si su respuesta es sí mencione:

Ley: _____ articulo: _____

5. ¿Tiene conocimiento de algún caso ocurrido dentro de la institución relacionado con delito informático?

Si_____ No_____

6. ¿Ha escuchado hablar de la informática forense?

Si_____ No_____

Si su respuesta es afirmativa defina el término:

_____

_____

_____

7. ¿Conoce algún software que aplique la informática forense para recolectar evidencia de un delito informático?

   Si_____ No_____

   Haga mención de este: _____

8. ¿Conoce el programa RecoverMyFiles?

   Si_____ No_____

   Si su respuesta es sí conteste:

   ¿Cuánto dominio tiene del programa?

   Mucho_____ Poco_____ Nada_____

   ¿Qué tan efectivo le parece el programa?

   Excelente ____ Bueno _____ Regular ____ Malo _____

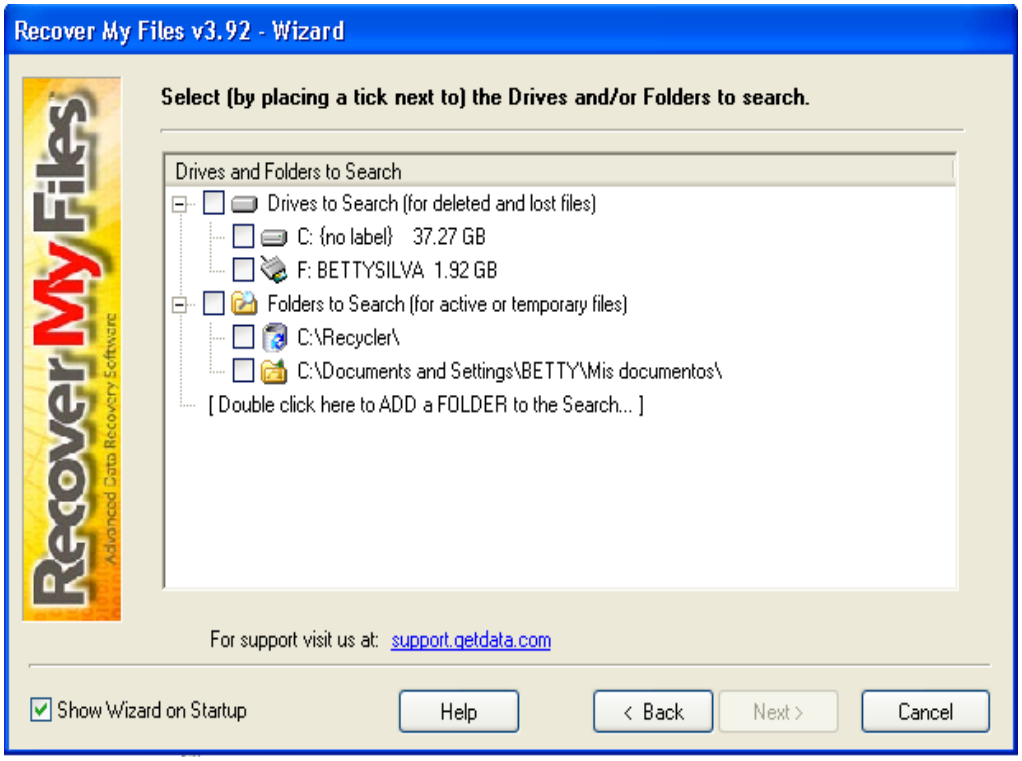
   Justifique su respuesta:

   _____
   _____
   _____

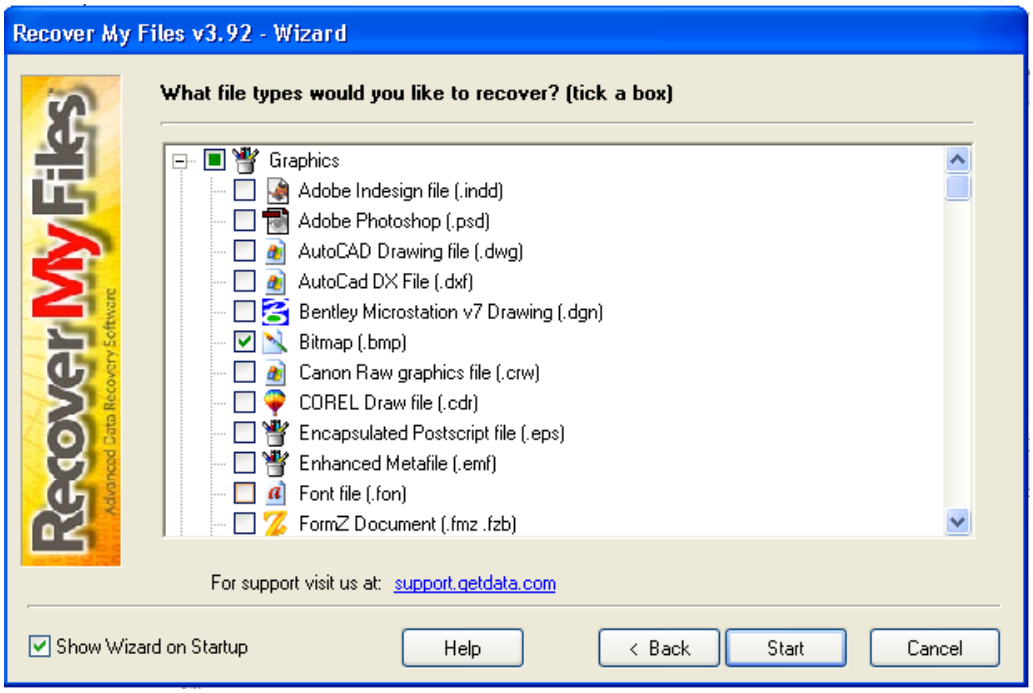
PANTALLAS DEL PROCESO DE RECUPERACIÓN DE ARCHIVOS

Paso1. Seleccionar el tipo de búsqueda

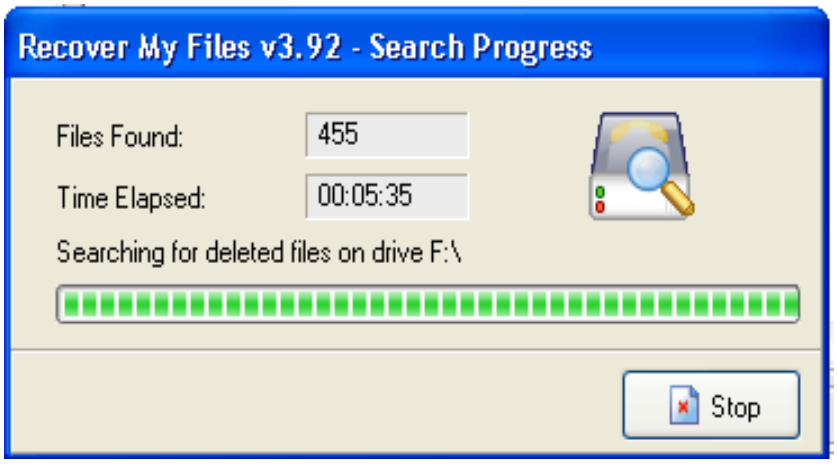
Paso2. Seleccionar la unidad para buscar



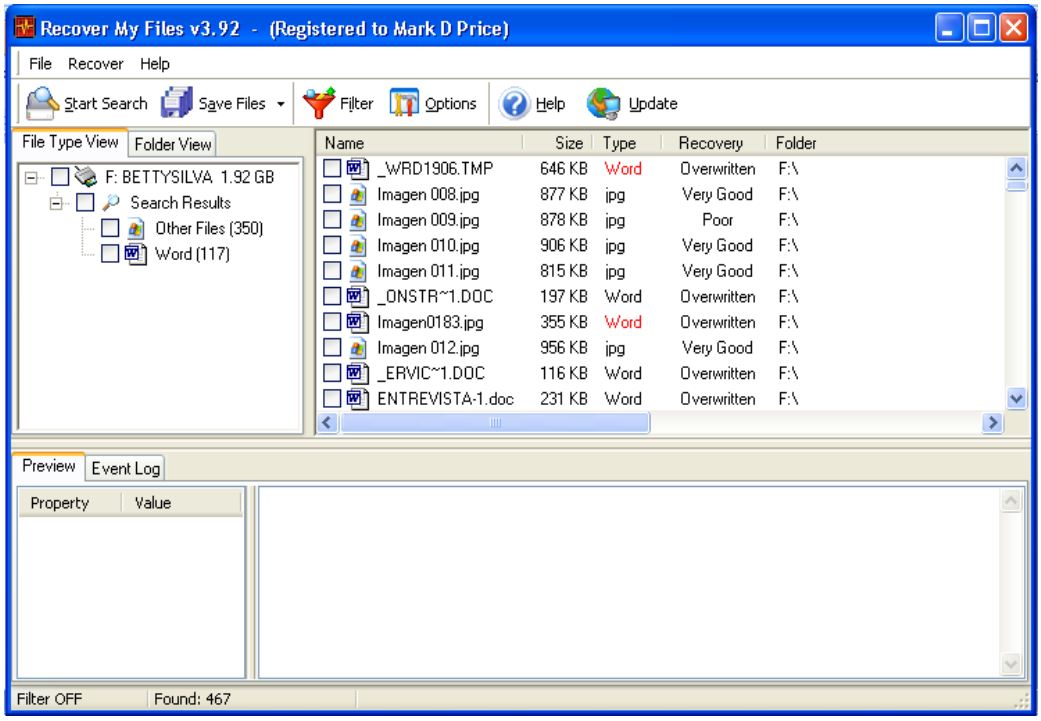
Paso3. Seleccionar el tipo de archivo a recuperar



Paso4. Ejecutar la búsqueda



Paso5. Pantalla de resultados



Paso6. Guardar archivos