# UNIVERSIDAD AUTONÓMA DEL ESTADO DE MÉXICO
# CENTRO UNIVERSITARIO UAEM TEXCOCO

## MÉTODO QUE MEDIANTE HERRAMIENTAS DE INFORMÁTICA FORENSE PERMITA CONOCER LAS AFECTACIONES EN LA INFORMACIÓN DE LOS USUARIOS DE LAS ORGANIZACIONES

**T E S I N A**

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO EN COMPUTACIÓN**


**PRESENTA:**

**MARCO ANTONIO ARIAS HERNANDEZ**

**DIRECTOR:**

**M EN C. JOSÉ SERGIO RUIZ CASTILLA**



**TEXCOCO, ESTADO DE MÉXICO, MÉXICO.** **AGOSTO 2013**

# Contenido

## Introducción

Hoy en día la seguridad de nuestra información es algo vital, especialmente cuando esta contiene datos sensibles o de alto riesgo para las organizaciones, si llegan a caer en manos malintencionadas o bien si por algún error es borrada de nuestros sistemas de respaldo de información.

Un archivo de información puede ser borrado, alterado, dañarse o ser robado y las organizaciones necesitan saber que sucedió, definir planes de prevención y pérdidas económicas.

Por medio de la informática forense se puede obtener:

- Quién realizó la intrusión
- Cómo entró en el sistema
- Fecha exacta en la que se ha realizado la intrusión o cambio
- Qué daños ha producido en el sistema

En este trabajo se pretende proponer un método que mediante herramientas de informática forense permita conocer las afectaciones en la información de los usuarios de las organizaciones, para recuperar información y conocer los detalles del problema.

Mediante el método que se propondrá en este documento se podrá obtener un análisis completo de las causas que implican en el ataque a la información.

Se podría obtener como resultado la detención de la afectación y establecer nuevos controles informáticos que eviten nuevas amenazas dentro de la empresa y aseguren una mayor confidencialidad de la información.

**Planteamiento del problema**

La seguridad de la información es algo vital en los últimos tiempos, especialmente cuando los archivos contienen datos sensibles y de alto riesgo para las organizaciones, si llegan a caer en manos de personas que la puedan usar para satisfacer sus necesidades sin nuestra autorización o bien si por algún error es borrada de nuestros sistemas de respaldo de información.

Es ahí donde entra la informática forense que se basa en hechos premeditados para recabar pruebas para luego analizarlas en una actividad post-mortem. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y pruebas necesarias. La escena del crimen es la computadora y la red a la cual éste conectada.

*¿Cómo proceder cuando accidental o intencionalmente ha sido afectada la información de la computadora de un usuario?*

**Justificación**

Hoy en día en una sociedad en la que existe gente malintencionada, la seguridad de la información es vital ya que es muy probable que esta información pertenezca a la identidad o economía personal o institucional.

Si se toma en cuenta que en los últimos años se ha incrementado la cantidad de intrusiones a las bases de datos informáticas de empresas y usuarios reflejando grandes pérdidas económicas parar los afectados.

Por medio de la informática forense podemos obtener:

- Fecha exacta en la que se ha realizado la intrusión o cambio de información
- Quién realizó la intrusión
- Cómo entró en el sistema
- Qué daños ha producido en el sistema

Este trabajo tiene como una de sus metas principales, apoyar a informáticos forenses sobre qué hacer ante un hecho de la afectación de archivos. La alternativa de usar la informática forense y así mismo como documento de apoyo para trabajos futuros sobre el tema.

## Objetivos

### Objetivo principal

Proponer un método de la aplicación de la informática forense en las organizaciones que han sufrido afectaciones en sus archivos de información de los usuarios de la organización, para recuperar información y conocer los detalles de la afectación.

### Objetivos específicos

*O.E.1*: Tipificar afectaciones  a la información de los usuarios.

*O.E.2*: Definir un método para proceder de acuerdo a la afectación.

*O.E.3*: Probar el método para llegar a la integración del dictamen correspondiente

# Capítulo 1. Seguridad de la Información

## 1.1Objetivos de la seguridad informática

Entre los principales objetivos de la seguridad informática podríamos destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para cumplir con estos objetivos una organización debe contemplar cuatro lados de actuación:

- *Técnico:* tanto a nivel físico como a nivel lógico
- *Legal*: algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad (sector de servicios financieros y sector sanitario en Estados Unidos, protección de datos personales en todos los Estados miembros de la Unión Europea, etcétera).
- *Humano*: sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal…
- *Organizativo*: definición e implementación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

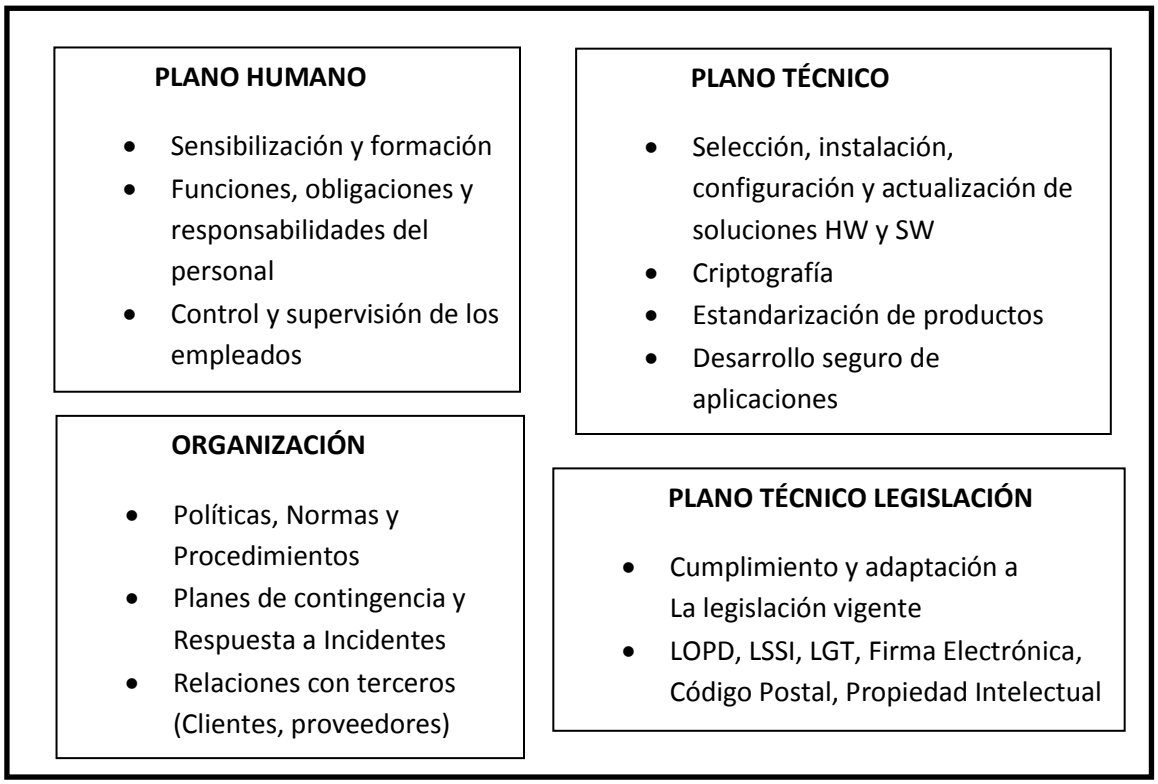



Ilustración 1.1 - Planos de actuación de la Seguridad Informática (Vieites, 2007)

Una organización debe entender la Seguridad Informática como un proceso y no como un producto que se pueda "comprar" o "instalar". Se trata, por lo tanto, de un ciclo iterativo, en el que se incluyen actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad.

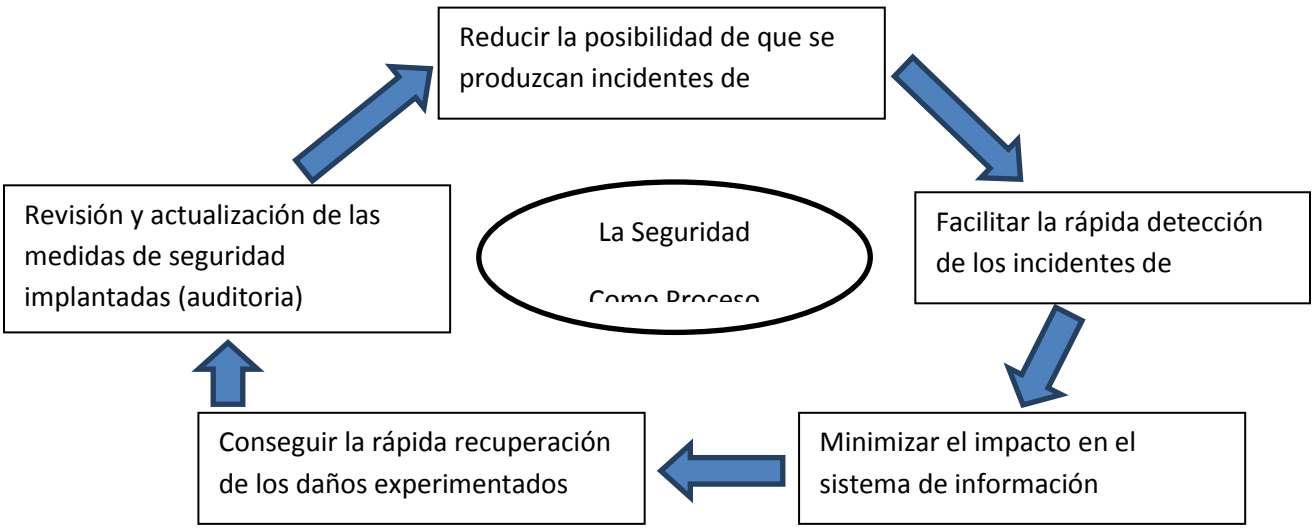



Ilustración 1.2 - La seguridad informática como proceso y no como producto (Vieites, 2007)

Por otra parte, la problemática asociada a la adecuada gestión de la seguridad en una organización del siglo XXI se ve condicionada por distintos factores y características del propio sistema informático y de su entorno. Así, sería necesario contemplar cuestiones como el nivel de centralización/descentralización del sistema, la necesidad de garantizar el funcionamiento continuado del sistema, el nivel de sensibilidad de los datos y de los recursos, la existencia de un entorno potencialmente hostil (conexiones a redes abiertas como internet) o el cumplimiento del marco legal vigente(LOPD, LSSI-CE, Propiedad Intelectual, Delitos Informáticos…) y de la certificación basada en una serie de estándares internacionales (BS 7799-2, ISO 17799…) o nacionales(UNE 71501 y 71502). (Vieites, 2007)

### 1.2 Inseguridad centralizada

Durante los años 60 y 70 la computación centralizada era la realidad evidente en los centros de procesamiento de datos. Los grandes computadores centrales o mainframes eran los que estaban en el primer nivel del uso informático de las organizaciones. Este tipo de computación era la norma que apoyaba los diferentes procesos de la organización, los cuales eran operados por personal especializado para esas labores. Es importante anotar que no todo el mundo tenía acceso a esas máquinas. En este sentido, la seguridad informática alrededor de este escenario, más que concentrarse en el descubrimiento de la inseguridad de los programas, estaba orientada a la inseguridad física de los equipos y el buen procesamiento de la información. Una falla en el programa de control de la información, o en la integridad de la misma, generaba una alta desconfianza en los informes y sus cifras.

En cuanto a la seguridad y el control, los años 60 y 70 se caracterizaron por un énfasis marcado en el control de acceso, la segregación de funciones y el debido registro de las operaciones y transacciones. Los mecanismos de seguridad propios de la época eran los registros de auditoria que, si bien existían y eran frecuentemente consultados, no tenían mayores protecciones, dado que el personal que tenía acceso a ellos eran profesionales con alto nivel de confianza y

con perfiles especiales, claramente registrados e identificados. Esta es la época de aplicación de modelos de seguridad, como Bell-Lapadula y Biba-Model, modelos que hacían hincapié en la confidencialidad y el acceso a la información. (Martínez, 2009)

### 1.3 Inseguridad descentralizada

Durante los años 80 se pasaba de una realidad centralizada y cerrada, a una descentralizada y abierta. Se concluye la época de los mainframes y se abre la puerta al concepto de las infraestructuras cliente/servidor-c/s. En este modelo de interacción existen máquinas que solicitan servicios y otras que los ofrecen. El énfasis se concentra en el tráfico de información a través de la red, y en el uso de puertos de conexión, los cuales están asociados con los servicios que se prestan.

Este cambio abre la puerta a un nuevo tipo de inseguridad, a unas nuevas relaciones que van más allá del servidor centralizado y, por tanto, requiere repensar nuevamente la gestión de la seguridad de la información. Con la llegada de una computación más abierta y con más oportunidades, se inicia la carrera para desarrollar mecanismos de la seguridad de la información, particularmente orientadas a las redes firewalls, sistemas de detección de intrusos, criptografía asimétrica, SSL (secure cocket layer), proxies, entre otros, los cuales establecen una nueva responsabilidad para el área de tecnologías de información.

Los nuevos mecanismos de seguridad que se presentan recogen las prácticas de los años 70 y desarrollan nuevas funcionalidades para disminuir los impactos de la inseguridad propia de los protocolos asociados con TCP/IP. A continuación, se hace una breve descripción de los principales mecanismos de seguridad en los ambientes cliente c/s.

*Firewall(fw) o cortafuegos*, una tecnología de los años 80 que busca desarrollar un control de acceso en el tráfico de red, con el fin de identificar que paquetes pueden o no ingresar o salir del perímetro de la red de una organización. Para ellos, se plantea un esquema de construcción de reglas, ya previamente vigente en los sistemas de enrutamiento para controlar los recorridos que seguían

los paquetes en una red, con el propósito de hacer más granular el control tanto como la organización quisiera. Este portal de control de acceso del tráfico se convierte en la fortaleza de la organización para evitar que personas no autorizadas trataran de invadir desde el exterior la red interna. Luego, con el tiempo, se hace evidente que no solamente el control desde el exterior era necesario, pues en el interior se podían presentar empleados desmotivados que podrían atentar contra la organización misma.

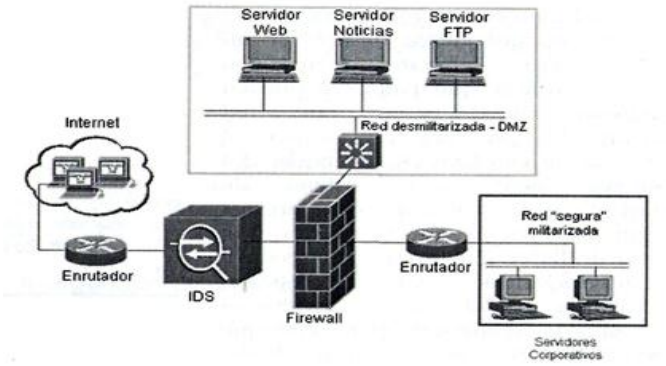



Ilustración 1.3 - Configuración de un firewall (Martínez, 2009)

*Los sistemas de detección de intrusos* (en inglés IDS, Intrusion Detection System) son otros de los adelantos tecnológicos de seguridad propios del mundo c/s, pues actúan como un monitor del tráfico de red, descubriendo y analizando ahora el contenido de los paquetes que ingresan a la organización. Si bien el fw hace parte del trabajo de control de acceso, no tiene capacidad para observar "la intencionalidad del mensaje" que lleva el paquete. Los sistemas de detección de intruso se asemejan a las alarmas que se instalan en casas, carros y oficinas a fin de advertir la presencia de una persona no deseada. En la primera parte de la evolución de esos sistemas su función era exclusivamente reactiva de la presencia de un posible ataque al sistema protegido, pero su grado de confiabilidad dependía del afinamiento de las reglas propias de detección y el tráfico de red frente a la dinámica de la organización.

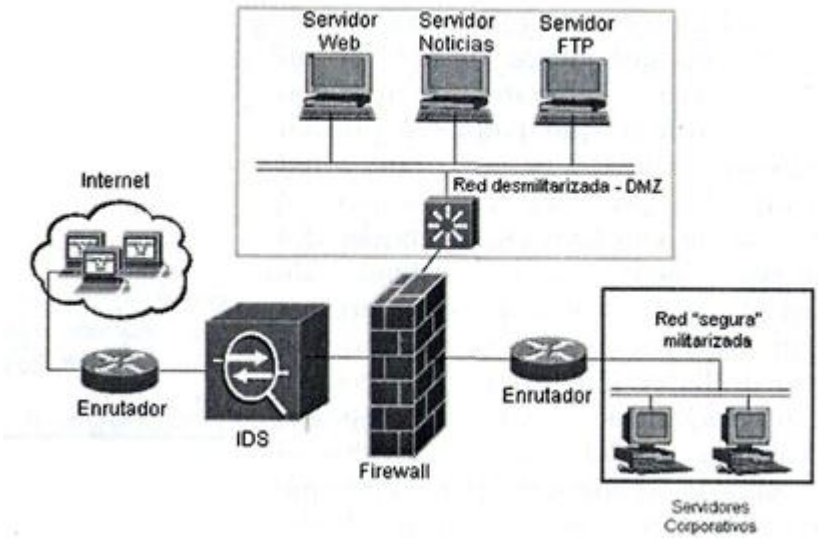



Ilustración 1.4 - Configuración de un firewall (Martínez, 2009)

Los sistemas de detección de intrusos continuaron su desarrollo, haciéndose cada vez más versátiles en la detección y en la reacción contra posibles escenarios de ataques, siempre con el margen de error asociado con los falsos-positivos; es decir, aquellos eventos o paquetes de tráfico de red que, sin ser una amenaza real, fueron reportados como tales. Con el paso del tiempo, en las infraestructuras de seguridad fue necesario combinar la presencia de un firewall y luego en un ids, con el fin de aumentar la capacidad de detección y de alerta de los intrusos en una infraestructura de red. Se hicieron parte fundamental de una estrategia de seguridad en el perímetro de las organizaciones y una herramienta clave para monitorear a los usuarios internos.

Por otra parte, tenemos los proxies, o estrategias de reducción o ampliación de acceso a conexiones desde o hacia una red, la cual puede ser normal o inversa. Un proxy es un intermediario que recibe, registra, valida y autoriza la salida o la entrada de un tráfico de red. Está asociado con permitir el acceso de muchas personas a recursos en Internet, donde únicamente se publica una dirección en Internet, protegiéndola de cada uno de los usuarios internos de la red.

La otra modalidad es que un usuario del exterior envíe una petición a un recurso que se encuentre detrás del proxy y este remita el paquete, luego de su verificación, al servidor correspondiente. Mientras el primer funcionamiento es el normal de esta estrategia, el segundo se denomina proxy reverso.

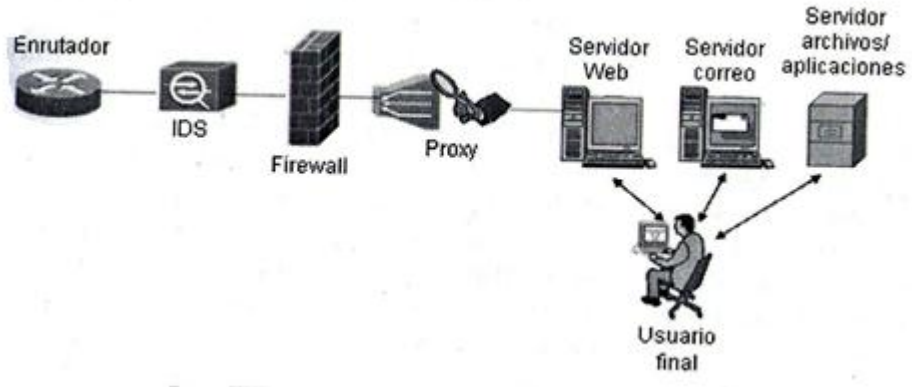



Ilustración 1.5 - Inseguridad descentralizada (Martínez, 2009)

Basado en el modelo OSI de ISO, promulgado en la década de los 70 y de uso diario en nuestros días, se establece una manera de pensar en la protección de las redes; es decir, recorriendo cada uno de los niveles conocidos(físico, enlace, red, transporte, sesión, presentación y aplicación) se pueden establecer los mecanismos de seguridad requeridos para disminuir el nivel de inseguridad propio de las aplicaciones c/s, y así dimensionar la inversión que habría que hacer para aumentar la confianza de la organización en el uso de las redes, y el transporte confiable de la información.

| Niveles OSI | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Autenticación de origen | | | * | * | | | * |
| Autenticación de origen de los datos | | | * | * | | | * |
| Servicio de control de acceso | | | * | * | | | * |
| Confidencialidad de la conexión | | | * | | | | * |
| Confidencialidad del flujo de información | * | | * | * | | | * |
| Confidencialidad de campos selectivos | | | | | | * | * |
| Integridad de la conexión con recuperación | | | | * | | | * |
| No repudiación de origen | | | | | | | * |
| No repudiación de destino | | | | | | | * |
| Control de acceso al servicio y aplicaciones | | | | | * | | * |

Ilustración 1.6 - Algunos servicios de seguridad en el OSI/ISO (Martínez, 2009)

Ahora, en el mundo c/s, el director de tecnología no solamente es responsable porque la infraestructura funcione de acuerdo con lo requerido, sino que debe hacerlo con mayor confiabilidad, disponibilidad, trazabilidad e integridad. Este requerimiento se hace en medio de una nueva tendencia de ataques y de incidentes que se llevan a las organizaciones a fallas importantes de los sistemas y a pérdidas de continuidad ya no ocasionadas por una caída del servidor central, sino por acceso no autorizado, una negación de servicio, una suplantación de dirección IP, envenenamiento del cache del DNS (Domain Name Service), monitoreo no autorizado de conexiones, suplantación de direcciones MAC, asalto de sesiones TCP, entre otros.

Esta nueva realidad desarrolla y propulsa una nueva dinámica de la seguridad de la información, no solamente motivada por los ataques, sino por las posibilidades que se abren al explorar los protocolos que soporta la suite de protocolos TCP-IP. Las aplicaciones cliente/servidor ofrecen una gama de nuevas posibilidades para utilizar la capacidad de cómputo de las máquinas, y abrir la interacción de las mismas a los usuarios de toda la organización. (Martínez, 2009)

## 1.4 Políticas de seguridad

En la siguiente figura se representa la jerarquía de conceptos manejados al hablar de las Políticas, Planes y Procedimientos de seguridad.


Ilustración 1.7 - Políticas, Planes y Procedimientos de seguridad (Vieites, 2007)

Así, en la cúspide de la pirámide se situarían los objetivos fundamentales de la Gestión de la Seguridad de la Información, resumidos mediante el acrónimo CIA (confidencialidad, integridad y disponibilidad de la información). Una vez fijados los objetivos fundamentales, es necesario definir las Políticas de Seguridad, así como los Planes y Procedimientos de actuación para conseguir su implantación en la organización.

Los procedimientos de la seguridad se descomponen en tareas y operaciones concretas, las cuales, a su vez, pueden generar una serie de registros y evidencias que facilitan el seguimiento, control y supervisión del funcionamiento del Sistema de Gestión de la Seguridad de la Información.

Los Procedimientos de Seguridad permiten implementar las Políticas de Seguridad definidas, describiendo cuales son las actividades que se tienen que realizar en el sistema, en qué momento o lugar, quiénes serían los responsables

de su ejecución y cuáles serían los controles aplicables para supervisar su correcta ejecución.

En este sentido, las Políticas definen *qué* se debe proteger en el sistema, mientras que los procedimientos de Seguridad describen *cómo* se debe conseguir dicha protección. En definitiva, si comparamos las Políticas de Seguridad con las leyes de un Estado de Derecho, los Procedimientos serian el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes.

| Política | Procedimiento | Tareas a realizar |
|---|---|---|
| Protección del servidor Web de la organización contra accesos no autorizados | Actualización del software del servidor Web | ✓ Revisión diaria de los parches publicados por el fabricante<br>✓ Seguimiento de las noticias sobre posibles fallas de seguridad |
| | Revisión de los registros de actividad en el servidor | ✓ Revisión semanal de los "*logs*" del servidor para detectar situaciones anómalas<br>✓ Configuración de las alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión |

Ilustración 1.8 –Ejemplo de Política y procedimientos de seguridad (Vieites, 2007)

Así, a modo de ejemplo, podríamos citar como procedimientos la planificación de las tareas administrativas y de sus responsables: administración de las cuentas de usuario y de los controles de acceso a los recursos lógicos; realización y supervisión de las copias de seguridad; seguimiento de los eventos de seguridad; etcétera. Otro grupo de procedimientos de seguridad estaría relacionado con la instalación, configuración y mantenimiento de distintos elementos de seguridad: cortafuegos (*firewalls*), servidores *proxy*, antivirus,

Sistemas de Detección de Intrusiones (IDS)…

### 1.4.1 Características deseables de las Políticas de Seguridad

En este apartado se presentan de forma esquemática las principales características y requisitos que debería cumplir las Políticas de Seguridad:

- Las Políticas de Seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable de sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas hardware y software que implementen servicios de seguridad.
- Deben definir claramente las responsabilidades exigidas al personal con acceso a sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización…
- Deben cumplir con las exigencias del entorno legal (Protección de Datos Personales –LOPD-, Protección de la Propiedad intelectual, Código Penal…).
- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. En este sentido, se debería contemplar un procedimiento para garantizar la revisión y la actualización periódica de las Políticas de Seguridad.
- Aplicación del principio de “Defensa en Profundidad”; definición e implantación de varios niveles o capas de seguridad. Así, si un nivel falla, los restantes todavía podrían preservar la seguridad de los recursos del sistema. De acuerdo con este principio, es necesario considerar una adecuada selección de medidas de prevención, de detección y de corrección.

- Asignación de los mínimos privilegios: los servicios, aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberán ser eliminados de los sistemas informáticos.
- Configuración robusta ante fallos: los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.
- Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros (clientes, Administración Publica…), sino que deberían estar adaptadas a las necesidades reales de cada organización.

Por otra parte, es necesario tener en consideración una serie de dificultades a la hora de definir las Políticas de Seguridad.

Así en primer lugar conviene destacar que la información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad, situación que no se produce con los equipos informáticos, la documentación o las aplicaciones informáticas.

Además, con la proliferación de las redes de ordenadores, la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo. Por este motivo, en la actualidad muchas organizaciones no conocen con precisión toda la información que hay en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riegos que tienen de sufrir ataques u otro tipo de desastres, ni cómo la propia organización utiliza esta información.

Debemos tener en cuenta dos aspectos contradictorios en las redes y sistemas informáticos: por un lado, su principal razón de ser es facilitar la comunicación y el acceso a la información y, por otro, asegurar que solo acceden a ella los usuarios debidamente autorizados. Esta contradicción está presente continuamente, ya que las medidas adoptadas para mejorar la seguridad (autenticación, control de accesos, monitorización del uso, encriptación, herramientas de detección de ataques, antivirus…) dificultan el uso de las redes y sistemas, al ralentizar los accesos e imponer ciertas restricciones, por lo que es necesario mantener un compromiso entre la usabilidad y un rendimiento de los sistemas informáticos, por una parte, y su seguridad, por otra.

Otro factor que muchas veces se olvida, es que, según numerosos estudios publicados, más del 75 % de los problemas inherentes a la seguridad se producen por fallos de los equipos o por un mal uso por parte del personal de la propia organización. Por este motivo, las Políticas de Seguridad deben contemplar no solo los ataques provenientes del mundo exterior ajeno a la organización, sino también los procedimientos de uso interno, prestando especial atención a la formación y sensibilización de los empleados y directivos.

La adopción de determinadas medidas burocráticas (registros de entradas y salidas, inventario de soportes informáticos…) o de determinados controles y procedimientos de seguridad se traduce generalmente en una mayor incomodidad para los usuarios, por lo que resultara fundamental explicar la importancia de la correcta aplicación de estas medidas para mejorar la seguridad en el trabajo cotidiano con los recursos de la organización.

Los problemas con las aplicaciones y los programas informáticos (productos incompletos o defectuosos que requieren de la aplicación de continuos parches y actualizaciones de seguridad), los continuos cambios en el entorno tecnológico y normativo, la creciente complejidad de los sistemas informáticos, así como la cada vez, mayor dependencia de las conexiones a Internet y de los accesos y servicios remotos son factores que han venido a complicar aún más, si cabe, el escenario en el que tienen que definirse e implementarse las medidas de seguridad.

Además, las medidas de seguridad no contribuyen a mejorar la productividad de los sistemas y redes informáticas, sino, más bien, todo lo contrario, ya que pueden reducir el rendimiento de los equipos y las aplicaciones (los sistemas criptográficos, por ejemplo, consumen mayores recursos computacionales y ancho de banda en las conexiones a Internet), por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Sin embargo, es necesario contar con los adecuados recursos técnicos, humanos y organizativos, así como de una dotación presupuestaria suficiente para conseguir una adecuada implantación de las Políticas de Seguridad definidas por la organización. No invertir en seguridad informática en una organización del siglo XXI sería como circular en un automóvil sin seguro frente a terceros: en caso de accidente las consecuencias pueden ser muy graves para el propietario y los acompañantes.

No se debe olvidar que la finalidad última del Departamento de Informática es proporcionar las herramientas y la información que van a necesitar los usuarios para poder llevar a cabo su trabajo de forma sencilla y eficiente (y, por supuesto, de forma segura). Sin embargo, en muchas organizaciones se sacrifica la seguridad por la usabilidad y rendimiento del sistema, primando de este modo la productividad. (Vieites, 2007)

### 1.5 Principio de “Defensa en Profundidad”

El principio de “Defensa en Profundidad” consiste en el diseño e implantación de varios niveles de seguridad dentro del sistema informático de la organización. De este modo, si una de las “barreras” es franqueada por los atacantes, conviene disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial o el control por su parte de recursos críticos del sistema: seguridad perimetral (cortafuegos, *proxies* y otros dispositivos que constituyen la primera “línea de defensa”); seguridad en los servidores; auditorias y monitorización de eventos de seguridad; etcétera.

Aplicando este principio también se reduce de forma notable el número de potenciales atacantes, ya que los aficionados y "script kiddies" solo se atreven con los sistemas informáticos más vulnerables y, por tanto, más fáciles de atacar.

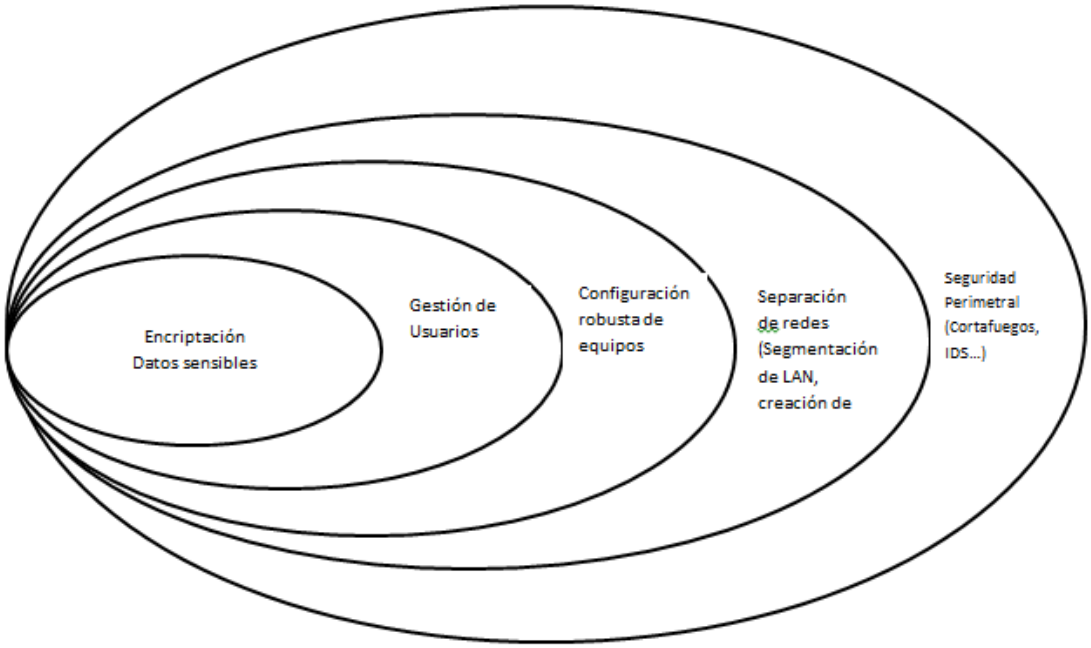



Ilustración 1.9- Principio de Defensa en Profundidad (Vieites, 2007)

Por este motivo, no conviene descuidar la seguridad interna en los sistemas informáticos, de modo que no dependa todo el sistema de la seguridad perimetral (cortafuegos en la conexión de la organización a redes externas como Internet). Así, por ejemplo, se puede reforzar la seguridad interna mediante una configuración robusta de los servidores, con medidas como la actualización de *parches* para eliminar vulnerabilidades conocidas, la desactivación de servicios innecesarios o el cambio de las contraseñas y cuentas por defecto en cada equipo.

## 1.6 Firewall

Una de las definiciones más básicas de firewalls es que estos son sistemas de defensa que forman parte de una red de trabajo y están diseñados para denegar o permitir el acceso a ella en base a reglas configurables y otros criterios predefinidos. Dentro de sus funcionalidades se destacan las siguientes:

- Bloqueo de paquetes que se originan desde un determinado rango de IP, puertos, dominios, direcciones de correo, etc.
- Bloqueo de paquetes generados por determinados protocolos o aplicaciones no autorizados.
- Bloqueo de paquetes que son reconocidos por el *firewall* como ataques informáticos.
- En algunos casos, el *firewall* genera informes que son útiles como una herramienta de análisis del comportamiento de la red interna y externa.
- Generación de registros que puedan ser utilizados en el análisis forense.
- Integración de sistemas de defensa en contra de virus, *spam*, y *malware* en general.
- Segmentación segura entre distintas redes internas además de Internet.

### 1.7 Clasificación de firewalls

Mientras que la definición de un cortafuego define su funcionalidad básica, los *firewalls* se pueden clasificar en virtud de diferentes características o modos de empleo:

- *Modelo de arquitectura*. Dependiendo del lugar donde se coloquen en la red pueden tener distintas funciones. Así cuando hay dos o más *firewalls* implementados en una red, aquel que es más externo y se comunica con otras redes o Internet se denomina *firewall de contención*, en cuanto el que se encuentra situado internamente y protege redes internas se denomina *firewall bastión*. Cuando sólo hay un *firewall* protegiendo la red será el bastión.
- *Instaladores de software vs. appliance*. Algunos *firewalls* son implementados mediante instaladores, como es el caso de VPN-1/Firewall-1 de Checkpoint, Iptables de Linux o ISA server de Microsoft. Existe hoy en día el formato appliance, donde en vez de instalar y configurar la solución, este último se conecta, se enciende y solo requiere configuraciones mínimas para funcionar. Este tipo de *firewall* proviene usualmente de fabricantes que acostumbran a crear

soluciones *hardware* embebidas con su propio sistema operativo, como es el caso de PIX Firewall de Cisco, Netscreen de Juniper o los dispositivos de SonicWALL. Muchos fabricantes hoy en día, sin embargo, empiezan a ofrecer sus soluciones de cortafuego en formato *appliance*, para que otros fabricantes de *hardware* lo puedan embeber, como es el caso de IP-Nokia/Firewall-1 o Crossbean/Firewall-1. A los fabricantes de *hardware* les gusta trabajar, además, con otros fabricantes terceros de *software* para integrar sus soluciones de antivirus o *antispam* y ofrecer un dispositivo "todo en uno".

*Características de Cortafuegos en software*

- Soportados por varios sistemas operativos
- Pueden ser instalados en varias plataformas de *hardware*
- Altamente configurables

*Características de cortafuegos en Appliance*

- *Hardware* + *Software* embebido.
- *Software* se ejecuta en un sistema operativo propietario del propio fabricante.
- Se acompañan con soluciones de otros fabricantes para realizar seguridad.
- Utilización de memoria ROM (Memoria de Solo Lectura) para ejecución rápida de procesos.
- Hardware específico para *firewall* que ayuda a procesar mejor ciertos algoritmos de cifrado de datos.

- *Firewalls de host vs. Firewalls de red.* Aquí la diferencia es el entorno que se desea proteger. Mientras uno lo hace solo en los sistemas donde están instalados, otros protegen la red o redes donde se han implementado.

*Características de cortafuegos de red*

- Protege redes enteras.
- Sistema dedicado a la función de *Firewall.*
- Módulos adicionales como IDS/IPS, antivirus o *antispam*.
- Requieren recursos dedicados de CPU y memoria RAM.

*Características de cortafuegos en el ordenador personal*

- *Firewalls* personales.
- En algunos casos ya están embebidos en el sistema operativo.
- Fabricantes de antivirus proveen soluciones “todo en uno” para los usuarios, donde incluyen módulos de cortafuego.

## 1.8 Tipos de filtrado en firewalls

Hay varios tipos de filtrado que pueden ejecutar los *firewalls*; dependiendo de estos filtrados, el *firewall* puede ser más o menos eficiente a la hora de proteger una red o un *host*. Hay tres tipos principales de filtrados basados en la capa del modelo OSI en la que los cortafuegos realizan el filtrado.

- *Filtrado a nivel de paquete*: se realiza a nivel de la capa de red, examinando la cabecera del paquete.
- *Filtrado a nivel de circuito*: se realiza a nivel de la capa de transporte, examinando el flujo de datos TCP y los datagramas UDP.
- *Filtrado a nivel de aplicación (proxies)*: se opera a nivel de las capas de aplicación verificando el contenido de los datos.

# Capítulo 2. Informática Forense

## 2.1 Inicio y definiciones de la informática forense

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas, bien sean humanas, procedimentales o tecnológicas, sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos (Kshetri 2006, Sundt 2006).Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio que nos permite provocar una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones que permitan descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

Así es como la Informática Forense hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, lo mismo que como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso. (Martínez, 2009)

A la fecha, existen múltiples definiciones sobre el tema forense en informática (McKemish 1999). Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, *digital forensics* (forensia digital), *network forensics* (forensia

en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

Conviene anota que, al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asume dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen, como son: identificación, preservación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

Iniciemos con *computer forensics,* cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras: (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; o (2) como la disciplina científica y especializada que, entendiendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses, y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento y la interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de *network forensics*(forensia en redes), estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, las configuraciones y las infraestructuras de comunicaciones se conjugan para dar como resultado un momento especifico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que, entendiendo las operaciones de las redes de computadores, siguiendo los protocolos y la formación criminalística, es capaz de establecer los rastros,

movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, poco frecuentes en equipos particulares.

Finalmente *digital forensics* (forensia digital) trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia e su lucha contra los posibles delincuentes, o como una disciplina especializada que procura el esclarecimiento de los hechos de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea 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.

Como hemos revisado, las definiciones abordan aspectos generales y específicos que en todos los casos convergen hacia la identificación, la preservación, la extracción, el análisis, la interpretación, la documentación y la preservación de evidencia digital, para detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado. No obstante lo anterior, es pertinente tener en cuenta que aquellos dedicados a esta disciplina emergente, como la informática forense, deben ser profesionales no con altos niveles de ética y respeto por las instituciones, sino con los más altos niveles, pues en ellos está el soporte de las decisiones que sobre los hechos analizados se tomen. (Martínez, 2009)

## 2.2 Principios de la Informática Forense

*La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación de los delitos criminales, mediante la identificación, captura, reconstrucción y análisis de las evidencias.*

La ciencia forense recurre a la aplicación de un método científico para analizar las evidencias disponibles y formular hipótesis sobre lo ocurrido. El trabajo de la ciencia forense se basa en el “Principio de Transferencia de Locard”*, según el cual cualquier persona u objeto que entra en la escena del crimen deja un rastro en la escena o en la propia víctima, y viceversa, es decir, también se lleva consigo algún rastro de la escena del crimen.

*Por su parte, la Informática Forense se encarga de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional (definición propuesta por el FBI)*

Un equipo de análisis forense estará constituido por expertos con los conocimientos y la experiencia necesarios en el desarrollo de estas actividades. Además sus miembros deberían contar con el entrenamiento adecuado, prestando especial atención a la puesta al día de sus conocimientos y habilidades.

Para poder realizar este trabajo resultará fundamental contar con los medios y el material especializado para las distintas técnicas del análisis forense, así como disponer de un manual detallado de los procedimientos de actuación, definiendo de forma clara y precisa todas las actividades que se realizaran en cada una de las etapas del análisis forense en sistemas informáticos. (Vieites, 2007)

## 2.3 Etapas de un análisis informático forense

Podemos distinguir las siguientes etapas en el análisis forense de un incidente informático:

1. Identificación y captura de las evidencias
2. Preservación de las evidencias
3. Análisis de la información obtenida
4. Elaboración de un informe con las conclusiones del análisis forense

Seguidamente se estudiaran las actividades y aspectos a tener en cuenta en cada una de estas actividades.

*Captura de las evidencias*

> Una *evidencia* es toda aquella información que podrá ser capturada y analizada posteriormente para interpretar de la información más exacta posible el incidente de seguridad; en que ha consistido, que daños ha provocado, cuáles son sus consecuencias y quien pudo ser el responsable. También se pueden considerar como evidencias los campos magnéticos y los pulsos electrónicos emitidos por los equipos informáticos

A pesar de ser intangibles, las videncias digitales o electrónicas pueden ser admitidas como prueba en un juicio, si se ofrecen unas determinadas garantías en las distintas etapas del análisis forense, mediante el aislamiento de la escena del crimen para evitar la corrupción de esta y de las posibles evidencias que en ella puedan hallarse.

Así, mismo es posible generar distintas copias de las evidencias digitales para facilitar su conservación y posterior análisis. La tecnología informática permitirá averiguar si alguna de estas copias ha sido modificada o falsificada, comparándola con la original.

Debemos tomar en cuenta que el proceso de captura de evidencias digitales no debe alterar el escenario objeto de análisis. En la práctica esto es muy difícil de conseguir, ya que las herramientas utilizadas van a modificar la memoria del sistema informático en el que se ejecutan. De hecho, la ejecución de determinados comandos en el sistema podrá alterar la información registrada en el disco: así, por ejemplo, un simple listado del contenido de un directorio va a modificar la fecha de último acceso a cada fichero.

Además conviene utilizar herramientas grabadas en disquete, en un CD-ROM o en otro soporte de almacenamiento, que se puedan ejecutar directamente sin requerir instalación ni utilizar un entorno gráfico, para que resulten lo menos intrusivas y no afecten  a la imagen en los discos duros del sistema.

No es recomendable emplear las propias herramientas del sistema, ya que estas podrían haber sido manipuladas por terceros, mediante “rootkits” o troyanos. Asimismo es necesario emplear medios forénsicamente estériles para guardar una copia de las evidencias digitales, es decir, medios que o hayan tenido daos previos a ellos.

También es conveniente obtener la imagen fotográfica de todas las pantallas que muestra el sistema informático durante el proceso de captura de las evidencias digitales.

La captura de las evidencias digitales se complica aún más con las *evidencias volátiles*, entendiendo como aquella información que se perderá al apagar un equipo informático objeto de análisis. Podemos considerar la siguiente relación de evidencias digitales volátiles:

- Volcado de la memoria global del sistema y de cada proceso: ante la dificultad de realizar un análisis en profundidad, se podrá utilizar el volcado de memoria para buscar determinadas cadenas de caracteres que puedan dar pistas sobre el incidente que ha afectado al equipo.
- Procesos y servicios en ejecución dentro del sistema: de cada proceso o servicio sería conveniente identificar el fichero ejecutable y los parámetros de ejecución, así como la cuenta de usuario bajo la que se ejecuta, los ficheros que está usando y que otro fichero o servicio lo ha llamado (árbol de ejecución), para posteriormente comparar esta información con la situación estable del sistema objeto de estudio.
- Controladores (drivers) instalados para gestionar distintos recursos hardware del sistema.
- Información de la situación y configuración de los servicios y las tarjetas de red: configuración del protocolo TCP/IP, puertos abiertos, caché del protocolo ARP, caché del DNS, enlaces entre los protocolos y las distintas interfaces de red…

- Usuarios y grupos de usuarios activos dentro del sistema: qué sesiones se encuentran abiertas en el momento de llevar acabo el análisis del equipo. (Vieites, 2007)

*Preservación de las evidencias*

A la hora de preservar las evidencias digitales será necesario contemplar una serie de tareas de tipo técnico y de medidas de carácter organizativo, teniendo en cuenta las recomendaciones de la IOCE (International Organization on Computer Evidence, Organización Internacional sobre Evidencias Informáticas).

Así, en primer lugar, se deberá utilizar un adecuado método de identificación, precinto, etiquetado y almacenamiento de las evidencias, considerando la posible incorporación de una firma temporal ("digital timestamp") en cada evidencia para que quede registrado el momento en que fue capturada.

Estas evidencias digitales deberán ser preservadas de factores ambientales adversos: campos magnéticos, fuentes de radiación, etcétera. Por este motivo, se recomienda conservar los soportes informáticos donde se han registrado las evidencias digitales en bolsas de plástico antiestáticas.

Asimismo, es necesario garantizar que los datos digitales adquiridos de copias no puedan ser alterados, por lo que para su obtención se deberían emplear herramientas de generación de imágenes bit a bit, que incorporen códigos de comprobación (checksums o algoritmos de huella digital como SHA-1 o MD5) para facilitar la comprobación de la integridad de estos datos. (Vieites, 2007)

*Análisis de las evidencias obtenidas*

El análisis de las evidencias digitales capturadas en las etapas anteriores podría ser realizado mediante herramientas especializadas (como EnCase) que permiten analizar la imagen obtenida de los discos duros sin tener que volcarla a otro disco o unidad de almacenamiento.

La labor de análisis puede comenzar con la búsqueda de información(cadenas de caracteres alfanuméricos) en el volcado de la memoria del sistema o en las imágenes de los discos duros para localizar ficheros sospechosos, como podrían ser programas ejecutables, “scripts” o posibles troyanos.

A continuación se podrán ejecutar estos ficheros sospechosos en un entorno de pruebas totalmente controlado. (Vieites, 2007)

## 2.4 Las evidencias tradicionales

Estas son recabadas en las escenas del crimen como “el arma ensangrentada”, “las huellas digitales del vaso”, “el lápiz labial de la colilla de cigarrillo”, “las manchas de fluidos corporales”, entre otras, hoy están acompañadas de discos duros, CD Roms, dispositivos USB de almacenamiento, IPod, access points inalámbricos, direcciones IP, teléfonos celulares, entre otros elementos. En este nuevo orden de rastros, la combinación de la escena física con los análisis de los objetos tecnológicos establecen una nueva forma de pericia que extiende las habilidades de los criminalistas, no solamente para conocer lo que ocurrió en el sitio, sino la información y los detalles de los eventos con la información residente en las tecnologías de información presentes en el sitio. (Martínez, 2009)

## 2.5 Los roles del intruso

Si bien el rol del intruso es interesante y atractivo, no es posible conocer los detalles de los rastros, si no nos adentramos en la mente del administrador, el profesional de tecnologías de información a cargo de la administración y control de la maquinas que posiblemente están involucradas. En este rol, el IF debe comprender los conceptos de protección y control de tecnologías de información, no solo para detallar las medidas tecnológicas de seguridad y control configuradas, sino para identificar y analizar las diferentes formas de alerta, detección, registro y monitoreo que la infraestructura tiene definidas para prevenir algún tipo de incursión no autorizada. Es este papel el IF se enfrentara al reto de

la inseguridad informática y sus diferentes fuerzas, reconocerá las relaciones entre las tecnologías de protección y las fallas de seguridad informática, para afianzar su visión de intruso presentada previamente (figura 2.1)


Ilustración 2.1- Características del administrador de sistema (Martínez, 2009)

El intruso y el administrador son dos roles complementarios y requeridos dentro de la gestión de la inseguridad de la información, pero se requiere un rol adicional que, con mirada emergente y superior, descubra las relaciones y los móviles de lo ocurrido; siga los procedimientos exigidos y establezca las evidencias requeridas para reconstruir la escena de lo anormal identificado. El investigador, ese rol natural de mirada aguda y persistente, es el elemento complementario que el IF debe conocer y desarrollar en sus acciones (figura 2.2)

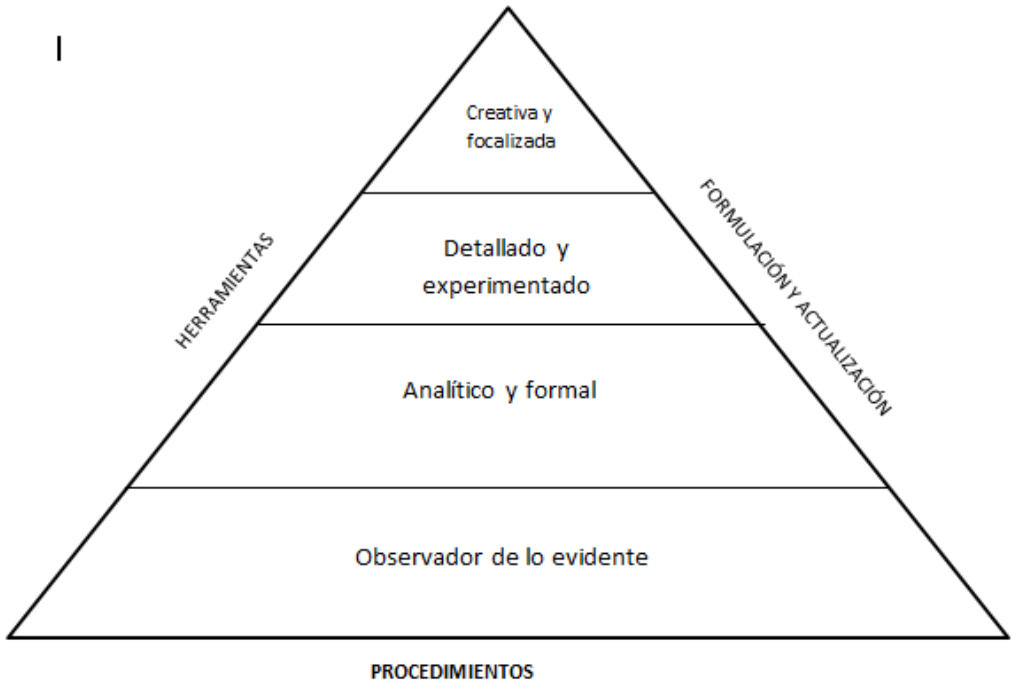



Ilustración 2.2- El perfil del investigador (Vieites, 2007)

## 2.6 Identificación de rastros de los ataques

Si la inseguridad informática es la constante de un mundo interconectado, la atención de incidentes debería ser la norma. En este sentido, no solamente es necesario estar preparados para aquellos eventos inesperados que se presenten en una infraestructura de cómputo o comunicaciones, sino comprender en profundidad el alcance de los ataques que se presenten.

En este contexto, se requiere desarrollar estrategias para contar con las evidencias de que algo ocurrió, el rastro del posible ataque que permita entender el comportamiento del intruso y sus movimientos dentro del sistema. En este orden de ideas, no insistiremos en las técnicas naturales de auditoria que se han generalizado en muchos sistemas de información, sino en el desarrollo de estrategias que busquen la trazabilidad de las acciones de los usuarios en el sistema y la autoprotección del sistema de registros de eventos del sistema mismo.

La sincronización, el control, la integridad de archivos y la confiabilidad en la generación de los registros de eventos son elementos requeridos para darle vida a

la trazabilidad o a la capacidad para rastrear, reconstruir o establecer relaciones entre los objetos monitoreados de un sistema. En la trazabilidad se hace referencia a un concepto sistémico, asociado con la necesidad de establecer relaciones y observar el todo del sistema atacado, y a uno sistemático, en la manera como se alcanza y se materializa el concepto en las aplicaciones corporativas, mediante el análisis de registros y trazas dejadas por el intruso.

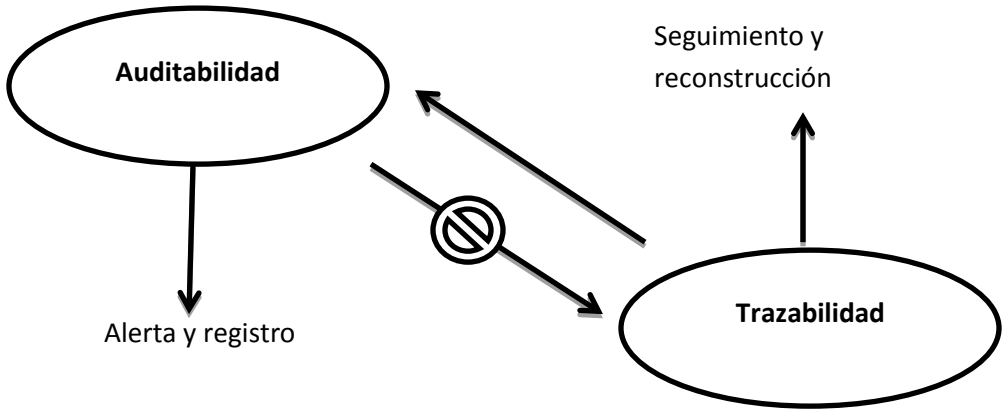



Ilustración 2.3: Auditabilidad y Trazabilidad (Martínez, 2009)

Para adelantar el análisis de rastros, conscientes de lo que queremos es alcanzar la trazabilidad de las acciones de intruso, es necesario tener prevista una serie de elementos de registro que va desde el sistema operacional hasta las políticas de seguridad, pasando por el sistema de archivos, los servicios de bases de datos, el tráfico de red, las aplicaciones y la memoria volátil.

En cada uno de ellos se pueden encontrar rastros de los eventos, dado que cualquier evento que se presente en una aplicación tendrá efectos sobre la memoria, las bases de datos o los sistemas de archivos donde ubica, lee o elimina información para su ejecución. Es claro que puede haber aplicaciones que ante fallas en su ejecución dejan abierta la posibilidad de acceso con control total, por una inadecuada configuración de su ejecución, pero precisamente esta falla debe

afectar las relaciones que tenga con los componentes de bases de datos –BD-, sockets de conexión y disponibilidad del servicio que serán alertas, que estarán a la vista de los administradores y usuarios de la mencionada aplicación.

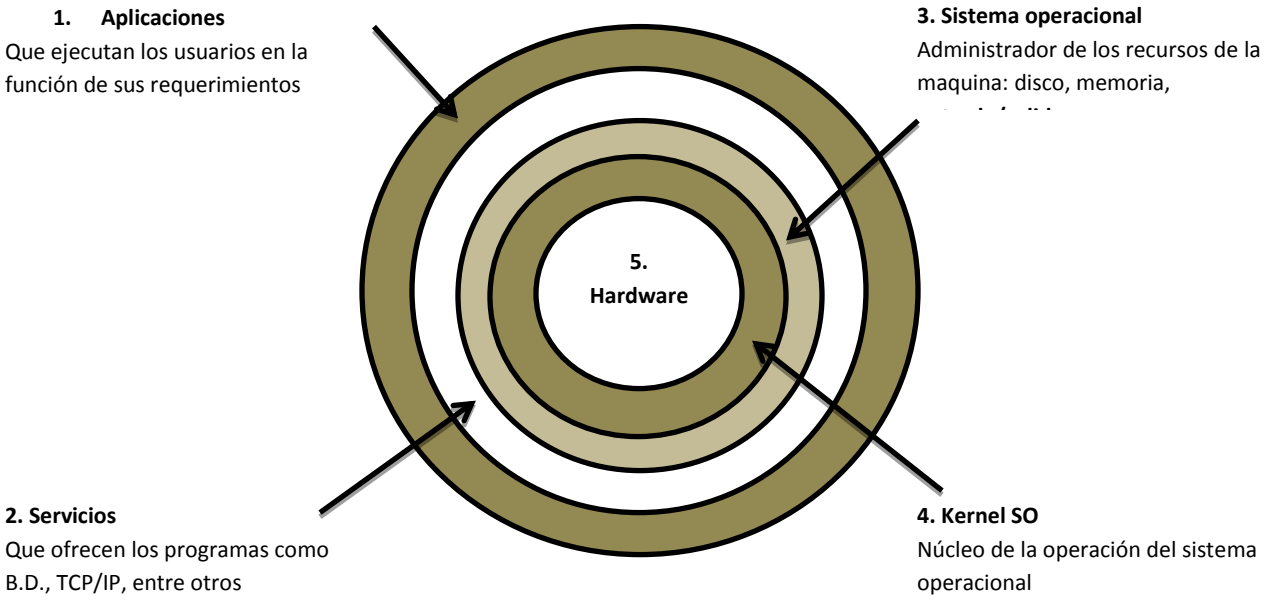



Ilustración 2.4: Análisis concéntrico de rastros (Martínez, 2009)

Al configurar el sistema operacional, es decir el software base con el cual funcionara la máquina, se requiere evidenciar y confirmar que tipo de aseguramiento o de afinamiento es necesario para establecer un ambiente confiable de ejecución, que implica un monitoreo y un registro de acciones básicas que permitan observar el correcto funcionamiento de las máquinas y aplicaciones allí residentes. Nada ganamos con tener aplicaciones fuertes y exigentes en

validaciones de control, si el sistema operacional que las contiene no cuenta con las características requeridas para una operación confiable. ¿Qué es un sistema operacional confiable? es la pregunta que surge. La respuesta a este Interrogante está asociada con las necesidades y configuraciones base establecidas por la organización, para sus sistemas de misión crítica.

Es cierto que en Internet existe un sinnúmero de guías de aseguramiento de sistemas operaciones que exigen controles y medidas, que podrían limitar la materialización de ataque conocidos, pero también podrían impedir que las aplicaciones corporativas se ejecuten correctamente. En este sentido, la respuesta a la pregunta anterior cobra más sentido, pues se hace necesario establecer un balance entre la operación y la seguridad de la misma. La inseguridad de la información es el resultado de una decisión que sabe a qué se expone, cuando decide sobre la configuración de una característica de un componente del sistema.

Ahora bien el sistema operacional y el sistema de archivos, esta última una estructura lógica que ordena y detalla los archivos, se encuentran residentes en la máquina. El sistema de archivos es manejado por funciones internas del sistema operacional, las cuales interactúan todo el tiempo con los procesos y memoria de la máquina para establecer la mejor forma de tener acceso a ellos y salvaguardarlos ante situaciones de falla de potencia eléctrica, o inconsistencias en manejo de los mismos por parte de las aplicaciones. El sistema de archivos es un componente sensible, que al ser lógico y articulado por el kernel del sistema operacional, es susceptible a fallas y a ataques especializaos por parte de los atacantes.

Los ataques directos al corazón del sistema operacional y a sus estructuras lógicas asociadas, como el sistema de archivos y controladores de componentes de hardware, son ataques cuyos rastros no son visibles o mejor aún imperceptibles, porque generalmente se encuentran en memoria o en archivos temporales que son volátiles. En este sentido, consecuente con lo planteado en las técnicas avanzadas de *hacking*, mientras más se acerquen los intrusos a las

funciones internas del sistema operación, mayores problemas de rastreo tendremos para conocer y detallar sus acciones.

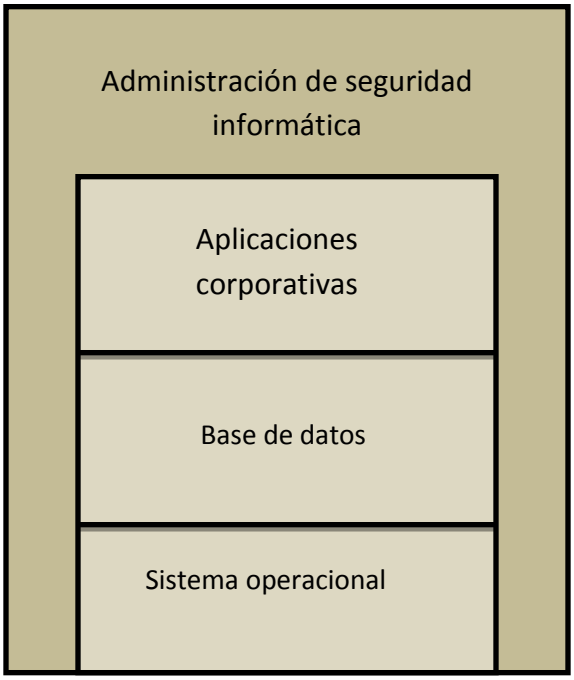



Ilustración 2-5: ¿Dónde ubicar los rastros? (Martínez, 2009)

Las aplicaciones y sus rastros dependen del diseño de las mismas. Generalmente las consideraciones sobre permisos de acceso a objetos y las medidas de seguridad en el desarrollo no son consideradas, lo cual aumenta a posibilidad de un ataque fundado en una inadecuada asignación de permisos para la aplicación que puede comprometer los datos de la compañía. Las aplicaciones debe responder a un modelo de seguridad y programación que defina y formalice las relaciones entre sus componentes, y así evidenciar los cambios y las acciones que se hacen del llamado de una función a un elemento del sistema. Esto exige disciplina de programación y validación de interfaces entre programas, antes de permitir la comunicación entre ellos.

En las bases de datos los rastros están asociados con los diseños previos que se hayan efectuado en el sistema manejador de bases de datos. Es decir, se debe haber configurado un sistema de alertas sobre los objetos críticos que afecten su funcionamiento y el de las aplicaciones que hacen uso de ella. Generalmente esta estrategia está fundada en disparadores cuando se alteran datos u objetos sensibles de la aplicación: tabla de usuarios, tabla de salarios, paquetes de programa, archivos de log, entre otros.

Sin embargo es frecuente encontrar que en las bases de datos no se cuente con mecanismos de monitoreo para los usuarios privilegiados de las mismas, como son los Database Administrators –Administradores de Bases de Datos. Estos profesionales, cuya responsabilidad es mantener la continuidad y la seguridad de los datos de la organización, generalmente no son monitoreados, lo que puede generar un escenario de falla, donde se utilice la carga de estos profesionales y materializar un evento, cuyas consecuencias pueden ser desafortunadas.

Por lo general, los sistemas manejadores de bases de datos cuentan con una estructura interna de monitoreo y control que vigila y registra todas las acciones del sistema sobre sus objetos, la cual es fuente de información tanto para los desarrolladores como para el proveedor del producto. Esta estructura es generalmente una tabla interna de acceso por parte de la cuenta superusuario de la base de datos, que no puede ser eliminada o alterada, pues de hacerse estaría comprometiendo la integridad del sistema. De igual forma, sus sistemas de bitácoras, que a pesar de no estar protegidos los archivos que se generan en el sistema operacional, se mantiene un mínimo de control de integridad que se valida antes de usarse para una recuperación de datos.

Hasta este momento hemos validado que existen elementos que se pueden revisar, para identificar rastros ante ataques en una máquina. Es impórtate anotar que estos elementos, previamente presentados, se deben extrapolar a un escenario de red, donde la variable comunicaciones establece un reto más a los análisis desarrollados. El tráfico de red es volátil y cambiante; a menos de que

exista un monitoreo del mismo, es poco factible identificar y recoger las comunicaciones que estén o haya tenido una maquina en su entorno de red.

Un nivel más de análisis podríamos evidenciarlo e las políticas de seguridad y la administración de seguridad de la organización. Este componente, más de corte administrativo se deja de lado cuando de recoger rastros se trata. En este componente se evidencian realmente las prácticas de la corporación en los temas de seguridad, y estas funcionan adecuadamente, debe haber actividades y acciones que se materialicen en la infraestructura. Sin una exigente administración de la inseguridad de la información, es decir una constante valoración de la exposición de los riesgos en los sistemas de misión crítica, no podrá haber una posición vigilante de los incidentes que sobre ella ocurra. La posición será reactiva y no proactiva.

La administración de la seguridad de la información, utilizando las buenas prácticas conocidas, no asegura la no ocurrencia de eventos inesperados o adversos, solamente nos indica las cosas mínimas que debemos hacer y, por lo tanto, son deberes que debemos comprender y repensar para tratar de estar pensando en las posibles fallas y las acciones que se deben tomar para minimizar los impactos. Por tanto, el diseño de registros de eventos y evaluaciones en los diferentes componentes revisados: sistema operacional, sistema de archivos, sistemas manejadores de bases de datos, aplicaciones y sistema de gestión de seguridad, son parte inherente del debido cuidado que hay que tener para enfrentar situaciones no previstas.

Considerando lo revisado en este aparte, detallamos un cuadro resumen de rastros en los diferentes componentes analizados, resultando algunos tipos de rastros y registros que pueden ser útiles para revisar cuando se está ante un incídete de seguridad del sistema.

| | Administración de la seguridad informática | Aplicaciones corporativas | Bases de Datos | Sistema operacional |
|---|---|---|---|---|
| Tecnologías | Software de monitoreo, control y correlación de logs | Pruebas de intrusión especificas | Software de monitoreo y control de acceso | Software de monitoreo y control de acceso<br>Análisis de vulnerabilidades |
| Procedimientos | Informes de auditoría internos y externo | Aseguramiento de la calidad del software: inspección de código fuente | Configuración de registros de auditoría y control de acceso | Aseguramiento del software base, según buenas prácticas de seguridad y control |
| Personas | Sesiones de entrenamiento y capacitación | Aseguramiento de la calidad del software: buenas prácticas de programación | Definición de permisos, privilegios y perfiles | Definición de usuarios y permisos |

Ilustración 2.6- Resumen general de Rastros en Sistemas Informáticos (Martínez, 2009)

## 2.7 Software útil para la informática forense

Las herramientas de análisis forense permiten asistir al especialista durante el análisis de un delito informático, automatizando buena parte de las tareas descritas en los apartados anteriores para facilitar la captura, preservación y posterior análisis de las evidencias digitales.

Además se distinguen por su capacidad de trabajar con distintos sistemas de ficheros: FAT y FAT32 de Windows, Ext2/3 de Linux, HFS de Macintosh, etcétera.

De las herramientas de análisis forense disponibles en el mercado podríamos considerar que las más populares serian EnCase, Autopsy, The Forensic Toolkit, The Sleuth Kit o The Coroner´s Toolkit, entre otras. (Vieites, 2007)

# Capítulo 3. Bases de Datos

## 3.1 Visión general de los medios físicos de almacenamiento

La mayoría de los sistemas informáticos presentan varios tipos de almacenamientos de datos. Estos medios se clasifican según la velocidad con la que se puede tener acceso a los datos, su coste de adquisición por unidad de datos y su fiabilidad. Entre los medios disponibles habitualmente figuran:

- *Caché.* La caché es el medio de almacenamiento más rápido y costoso. La memoria caché es pequeña; su uso lo gestiona el hardware del sistema informático. Los sistemas de bases de datos no la gestionan.
- *Memoria principal.* El medio de almacenamiento utilizado para los datos con los que se opera es la memoria principal. Las instrucciones máquina operan en la memoria principal. Aunque la memoria principal puede contener muchos megabytes de datos (un PC normal viene con 512 megabytes como mínimo), o incluso cientos de gigabytes de datos en grandes sistemas servidores suele ser demasiado pequeña(o demasiado cara) para guardar toda la base de datos. El contenido de la memoria principal suele perderse en caso de fallo del suministro eléctrico o de caída del sistema.
- *Memoria flash.* La memoria flash se diferencia de la memoria principal en que los datos no se pierden en caso de que se produzca un corte de la alimentación. La lectura de los datos de la memoria flash emplea menos de cien nanosegundos (un nanosegundo es una milésima de microsegundo), más o menos igual de rápida que la lectura de los datos de la memoria principal. Sin embargo, la escritura de los datos en la memoria flash resulta más complicada(los datos pueden escribirse una vez, lo que tarda de cuatro a diez microsegundos, pero no se pueden sobrescribir de

manera directa). Para sobrescribir la memoria es necesario borra simultáneamente todo un banco de memoria, el cual queda preparado para volver a escribir en él. Un inconveniente de la memoria flash es que solo permite un solo número limitado de cilcos de borrado, que varía en diez mil y un millón. Es un tipo de *memoria sólo de lectura programable y borrable eléctricamente (electically erasable programable read-only, EEPROM); otras variantes de EEPROM permiten el borrado y reescritura de posiciones individuales de la memoria, por su empleo no esta tan difundido.* (Abraham Silverschatz, 2006)

- *Almacenamiento en discos magnéticos.* Es el principal medio de almacenamiento persistente en conexión es el disco magnético. Generalmente se guarda en ellos toda la base de datos. Para acceder a los datos es necesario trasladarlos desde el disco a la memoria principal. Después de realizar la operación deseada se deben escribir en el disco los datos que se hayan modificado. (Abraham Silverschatz, 2006)
- *Almacenamiento óptico.* La forma más popular de almacenamiento óptico es el disco compacto (*Compact Disc*, CD), que puede almacenar hasta 700 megabytes de datos y un tiempo de reproducción de 80 minutos, y el disco de video digital (Digytal Video Disc, DVD), que puede almacenar 4.7 u 8.5 gigabytes de datos en cada cara del disco(o hasta 17 gigabytes en un disco de doble cara). También se utiliza el término disco digital versátil en lugar de disco de video digital, ya que los DVD pueden almacenar cualquier tipo de dato digital, no solo datos de video. Los datos se almacenan ópticamente en el disco y se leen mediante un láser. No se puede escribir en los discos ópticos empleados como discos compactos de solo lectura (CD-ROM) o como discos de video digital de solo lectura (DVD-ROM), pero se suministran con datos pregrabados. Existen también versiones “para una sola grabación” de los discos

compactos (denominados CD-R) y de los discos de video digital (DVD-R y DVD+R) en los que solo se puede escribir una vez; estos discos también se denominan de escritura única y lectura múltiple (write-once, read-many, WORM). Existen también versiones "para escribir varias veces" de los discos compactos (llamada CD-RW) y de los discos de video digital (DVD-RW, DVD+RW Y DVD-RAM) en lo que se puede escribir varias veces. Los *cambiadores automáticos* (*jukebox*) de discos ópticos contienen varias unidades y numerosos discos que pueden cargarse de manera automática en las diferentes unidades (mediante un brazo robotizado) a petición del usuario. (Abraham Silverschatz, 2006)

## 3.2 Características físicas de los discos magnéticos

Físicamente los discos son relativamente sencillos (Figura x). Cada *plato* del disco es de forma circular plana. Sus dos superficies están cubiertas por un material magnético en el que se graba la información. Los platos están hechos de metal rígido o de vidrio.

Mientras se utiliza el disco, un motor lo hace girar a una velocidad constante elevada (generalmente sesenta, noventa o ciento veinte revoluciones por segundo, aunque existen discos que giran a doscientas cincuenta revoluciones por segundo). Una cabeza de lectura y escritura está colocada justo encima de la superficie del plato. La superficie del disco se divide a efectos lógicos en *pistas*, que se subdividen en *sectores*. Un *sector* es la unidad mínimo de información que se puede leer o escribir en el disco. En los discos actuales, el tamaño de los sectores suele ser de quinientos doce bytes; hay entre cincuenta mil y cien mil pistas en cada plato y de uno a cinco platos por disco. Las pistas internas (las más cercanas al eje) son más cortas, y en los discos actuales las pistas exteriores contienen más sectores que las internas; suele haber unos quinientos sectores por pista en las pistas internas y alrededor de mil en las externas. Estos números pueden variar de un modelo a otro; los discos de mayor capacidad tienen más sectores por pista y más pistas en cada plato.

La *cabeza de lectura y escritura* guarda la información en los sectores en forma de inversiones de la dirección de magnetización del material magnético.

Cada cara de un plato del disco posee una cabeza de lectura y escritura que se desplaza por el plato para tener acceso a las diferentes pistas. El disco suele contener muchos platos y las cabezas de lectura y escritura de todas las pistas están montadas en un único dispositivo denominado *brazo del disco* y se mueven conjuntamente. El conjunto de los platos del disco montados sobre un mismo eje y las de todos los platos se desplazan conjuntamente, cuando la cabeza se halle en la pista i-ésima de un plato, las restantes también se encontraran en la pista i-ésima de sus platos respectivos. Por tanto, el conjunto de las pistas i-ésimas de todos los platos se denominan cilindro i-énesimo.

Actualmente dominan en el mercado los discos con un diámetro de plato de tres pulgadas y media. Tienen un menor coste y tiempos de búsqueda más cortos (debido al menor tamaño) que los discos de mayor tamaño (de hasta catorce pulgadas) que eran habituales en el pasado y, aun así, ofrecen gran capacidad de almacenamiento. Se usan discos de diámetro incluso menor en dispositivos móviles como las computadoras portátiles, las de mano y los reproductores de música de bolsillo.

Las cabezas de lectura y escritura se mantienen tan próximas como resulta posible a la superficie de los discos para aumentar la densidad de grabación. Las cabezas suelen flotar o volar tan solo a micras de la superficie de cada disco; el giro del disco crea una pequeña corriente de aire y el dispositivo de las cabezas se fabrica de manera que ese flujo de aire mantenga las cabezas flotando rasantes sobre la superficie de los discos. Como las cabezas flotan tan cercanas a la superficie, los platos se deben elaborar con esmero para que sean lisos.

Los choques de las cabezas con la superficie de los platos pueden suponer un problema. Si la cabeza entra en contacto con la superficie del disco, puede arrancar el medio de grabación, lo que destruye los datos que allí hubiera. En los modelos antiguos, el contacto de la cabeza con la superficie hacia que el material

arrancado flotase en el aire y se interpusiera entre las cabezas y los platos, lo que causaba más choques; por tanto, la caída de las cabezas podía dar lugar a un fallo de todo el disco. Los dispositivos actuales emplean como medio de grabación una fina capa de metal magnético. Son mucho menos susceptibles de fallar a causa del choque de las cabezas con las superficies de los platos que los antiguos discos recubiertos de óxido. (Abraham Silverschatz, 2006)

### 3.3 Acceso al almacenamiento

Cada base de datos se corresponde con varios archivos diferentes que el sistema operativo subyacente mantiene. Esos archivos residen permanentemente en los discos, con copias de seguridad en cinta. Cada archivo está dividido en unidades de almacenamiento de longitud constante denominadas *bloques*, que son las unidades de asignación de almacenamiento y de transferencia de datos.

Cada bloque puede contener varios elementos de datos. El conjunto exacto de elementos de datos que contiene cada bloque viene determinado por la forma de organización física de los datos que se utilice. (Abraham Silverschatz, 2006)

Uno de los principales objetivos del sistema de bases de datos es minimizar el número de transferencias de bloques entre el disco y la memoria. Una manera de reducir el número de accesos al disco es mantener en la memoria principal tantos bloques como sea posible. El objetivo es minimizar la posibilidad de que, cuando se acceda a un bloque, ya se encuentre en la memoria principal y, por tanto, no se necesite acceder al disco.

Dado que no resulta posible mantener en la memoria principal, todos los bloques, hay que gestionar la asignación del espacio allí disponible para su almacenamiento. La *memoria intermedia* (buffer) es la parte de la memoria principal disponible para el almacenamiento de las copias de los bloques del disco. Siempre se guarda en el disco una copia de cada bloque, pero esta copia puede ser una versión del bloque más antigua que la de la memoria intermedia. El subsistema responsable de la asignación del espacio de la memoria intermedia se denomina *gestor de la memoria intermedia*.

### 3.3.1 Gestor de la memoria intermedia

Los programas de los sistemas de bases de datos formulan solicitudes (es decir, llamadas) al gestor de la memoria intermedia cuando necesitan bloques del disco. Si el bloque ya se encuentra en la memoria intermedia, el gestor pasa al solicitante la dirección del bloque en la memoria principal. Si el bloque no se halla en la memoria intermedia, asigna en primer lugar espacio al bloque en la memoria intermedia, descartando algún otro, si hace falta, para hacer sitio al nuevo. El bloque descartado solo se vuelve a escribir en el disco si se ha modificado desde la última vez que se escribió. A continuación el gestor de la memoria intermedia lee el bloque solicitado en el disco, lo escribe en la memoria intermedia y pasa la dirección del bloque en la memoria principal al solicitante. Las acciones internas del gestor de la memoria intermedia resultan transparentes para los programas que formulan solicitudes de bloques de disco.

Si se está familiarizado con los conceptos de los sistemas operativos, se observara que el gestor de la memoria intermedia no parece ser más que un gestor de memoria virtual, como los que se hallan en la mayor parte de los sistemas operativos. Una diferencia radica en que el tamaño de las bases de datos puede ser mucho mayor que el espacio de direcciones de hardware de la máquina, por lo que las direcciones de memoria no resultan suficientes para direccionar todos los bloques del disco. Además, para dar un buen servicio al sistema de bases de datos, el gestor de la memoria intermedia debe utilizar técnicas más complejas que los esquemas habituales de gestión de la memoria virtual:

- *Estrategia de sustitución*. Cuando no queda espacio libre en la memoria intermedia hay que eliminar un bloque de ésta antes de que se pueda escribir otro nuevo. La mayor parte de los sistemas operativos utilizan un esquema de *menos recientemente utilizado ( Least Recently Used, LRU)*, en el que se vuelve a escribir en el disco y se elimina de la memoria intermedia el bloque al que se ha hecho referencia menos recientemente.

Este sencillo enfoque se puede mejorar para las aplicaciones de bases de datos.

- *Bloques clavados*. Para que el sistema de bases de datos pueda recuperarse de las caídas del sistema hay que restringir las ocasiones en que los bloques se pueden volver a escribir en el disco. Por ejemplo, la mayor parte de los sistemas de recuperación exigen que no se escriban en disco los bloques mientras se esté procediendo a su actualización. Se dice que los bloques que no se permite que se vuelvan a escribir en el disco están *clavados*. Aunque muchos sistemas operativos no permiten trabajar con bloques clavados, esta característica resulta fundamental para los sistemas de bases de datos resistentes a las caídas.
- *Salida forzada de los bloques*. Hay situaciones en las que hace falta volver a escribir los bloques en el disco, aunque no se necesite el espacio de memoria intermedia que ocupan. Este proceso de escritura se denomina *salida forzada* del bloque. (Abraham Silverschatz, 2006)

### 3.4 Organización de los archivos

Los *archivos* se organizan lógicamente como secuencias de registros. Estos registros se corresponden con los bloques del disco. Los archivos constituyen un elemento fundamental de los sistemas operativos, por lo que se supone la existencia de un *sistema de archivos* subyacente. Hay que tomar en consideración diversas maneras de representar los modelos lógicos de datos en términos de los archivos.

Aunque los bloques son de un tamaño fijo determinado por las propiedades físicas del disco y por el sistema operativo, el tamaño de los registros varía. En las bases de datos relacionales, las tuplas de las diferentes relaciones suelen ser de tamaño diferente. Un enfoque de la correspondencia entre la base de datos y los archivos es utilizar varios archivos y guardar los registros de la misma longitud en un mismo archivo. Una alternativa es estructurar los archivos de modo que puedan aceptar registros de longitudes diferentes; no obstante, los archivos con registros de longitud fija son más sencillos de implementar que los que tienen registros de

longitud variable. Muchas de las técnicas empleadas para los primeros pueden aplicarse a los de longitud variable. Por tanto, se comienza por tomar en consideración los archivos con registros de longitud fija. (Abraham Silverschatz, 2006)

# Capítulo 4. Propuesta metodológica

## 4.1 Metodología del examen y análisis de datos

Para realizar un análisis de datos forense es necesario seguir una serie de pasos para la obtención de la evidencia. A continuación se propone una guía metodológica que reúne y organiza una serie de actividades conducentes a la obtención de tal evidencia. (Reith & C. Gunsh G.) (Casey, 2002) (Morris, 2003) (Janiczek, 2004) (Luzinski & Kida J). En el caso de la guía metodológica propuesta, es necesario definir un conjunto de elementos requeridos que constituyen la información inicial para seguirla. Estos elementos son:

- Imágenes binarias de los dispositivos de almacenamiento digital comprometidos en el caso de sus respectivos compendios criptográficos.
- Descripción del caso ilustrando el marco circunstancial.
- Metadatos de cada una de las imágenes, es decir, todo tipo de información necesaria para determinar las características de la imagen, en particular, la existencia de una HPA(Host Protected Area)

El objetivo de esta guía metodológica es obtener un informe de hallazgos que describa la evidencia hallada y la forma como se obtuvo

### 4.1.2 Descripción de los pasos

1. *Creación del archivo de hallazgos*

Consiste en la creación y el aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado.

2. *Imagen de datos*

Consiste en la recepción de las imágenes de datos que conciernen al caso en investigación.

3. *Verificación de integridad*

Para cada imagen suministrada se debe calcular su compendio criptográfico (MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.

4. *Creación de una copia de la imagen suministrada*

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada, sino sobre su copia.

5. *Aseguramiento de la imagen suministrada*

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

6. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido.

Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso 2). De hecho, esta actividad es transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

7. *Identificación de las particiones actuales y anteriores (las que se pueda recuperar)*

La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

8. *Detección de información en los espacios entre las particiones*

Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables.

9. *Detección de un HPA*

Este paso debe realizarse solo si en los metadatos se indica la existencia del HPA, ya que de otro modo es imposible de identificar (Carrier, 2004). En el caso de que exista, se debe seguir el mismo procedimiento del paso anterior.

10. *Identificación del sistema de archivos*

Para cada una de las particiones identificadas en el paso 6, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar las actividades posteriores del análisis de datos.

11. *Recuperación de los archivos borrados*

Durante esta actividad se debe tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente, dado que es frecuente el borrado de archivos para destruir evidencia.

Dependiendo de las características técnicas y del estado del sistema de archivos, puede no ser posible la recuperación de la totalidad de los archivos eliminados; por ejemplo, si estos han sido sobrescritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

12. *Recuperación de información escondida*

En esta etapa se deben examinar exhaustivamente el slack space, los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Al igual que en la fase 10, los archivos protegidos también se tendrán en cuenta durante la fase de análisis de este tipo de archivos.

13. *Identificación de archivos existentes*

Seguidamente, se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte de la fase de análisis de archivos protegidos.

14. *Identificación de archivos protegidos*

Esta es la fase de consolidación de archivos protegidos identificados en las fases anteriores. Durante esta fase se pretende descifrar o romper tal protección de estos archivos, con el fin de adicionarlos al conjunto de archivos analizables. Los archivos cuya protección no pudo ser vulnerada formaran parte del conjunto de archivos sospechosos.

15. *Consolidación de los archivos potencialmente analizables*

Durante esta fase se reúnen todos los archivos encontrados durante las fases de: recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.

16. *Determinación del sistema operativo y las aplicaciones instaladas*

Al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de estos archivos de encontrarse en la imagen sometida a análisis.

17. *Filtrado basado en archivos buenos conocidos*

Con la lista de compendios criptográficos obtenida en el paso anterior, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, este se considera “bueno” y, por lo tanto, es descartado del proceso de análisis.

18. *Consolidación de archivos sospechosos*

Como resultado del filtrado de “buenos” conocidos, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamara archivos sospechosos.

19. Primera clasificación

Divide los archivos sospechosos en:

- Archivos “buenos” modificados: Son identificados en la fase de filtrado como archivos buenos cuya versión original (descrita por la lista obtenida en el paso 15) ha sido modificada.
- Archivos “malos”: Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos “malos” relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o ejecutan, por ejemplo: troyanos, backdoors y virus, entre otros.
- Archivos con extensión modificada: aquellos cuya extensión no es consistente con su contenido.

Los archivos que cumplen con alguna de las anteriores características se convierten en archivos prioritarios para el análisis. Los que no cumplen estas características se someten a la siguiente etapa de clasificación.

20. *Segunda clasificación*

Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con el usuario involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial.

El resultado de esta clasificación es seleccionar como prioritarios para el análisis los archivos que sean identificados bajo los anteriores criterios.

21. *Analizar los archivos*

Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador.

Es importante resaltar que los procesos de la segunda clasificación y análisis, pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente. En cada iteración cada archivo de alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.

Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o porque se agotan los datos por analizar.

22. *Archivos comprometidos en el caso*

Es el conjunto de archivos que forman parte de la evidencia del caso.

23. *Obtención de la línea de tiempo definitiva*

Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

Es importante resaltar que en algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que, como todos los hallazgos, debe ser consignada en el informe.

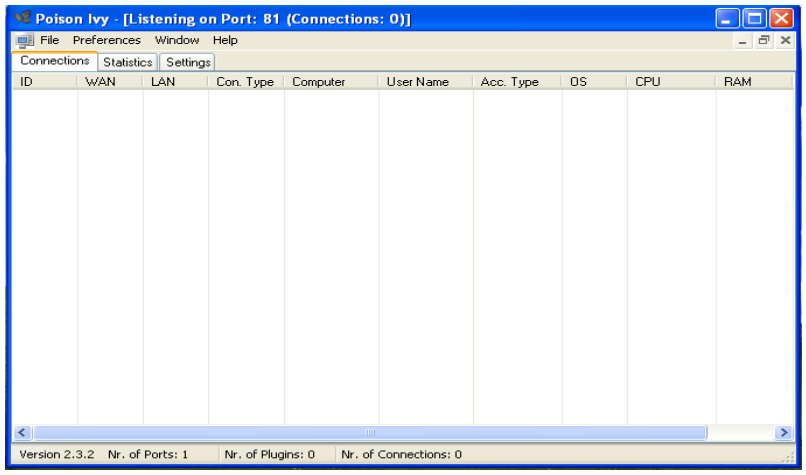
24. *Generación del informe*

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación metodológica. (Martínez, 2009)

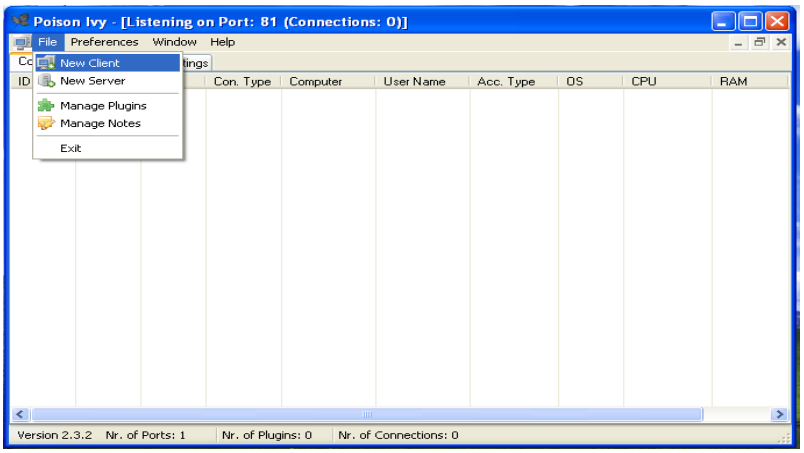
## 4.2 Caso práctico del proceso de intrusión a una PC

Para realizar el caso práctico y aplicar el método que se propone para recuperar la información dañada o perdida en un equipo de cómputo de algún usuario, se desarrolló un spyware por medio de un troyano con el fin de que con este se extraiga el archivo deseado vía remota sin que el usuario se dé cuenta de la infección; una vez obtenida la información se procederá a realizar el análisis forense.

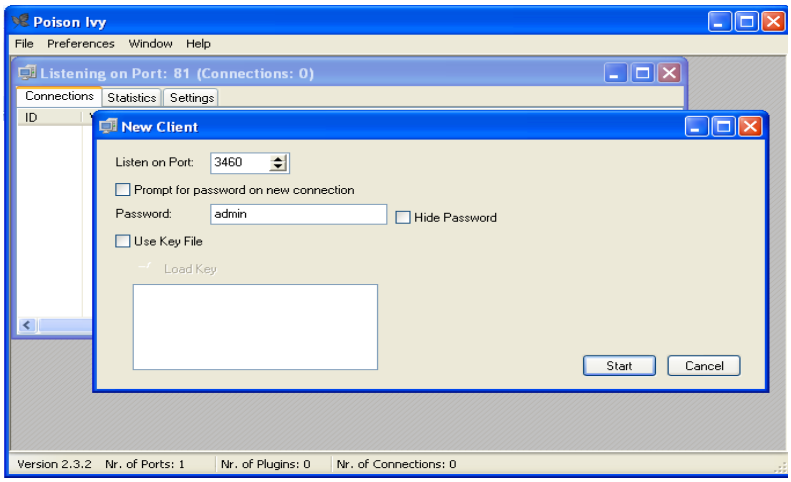
Para crear el spyware se utilizara un software llamado Poison Ivy en su versión 2.3.2

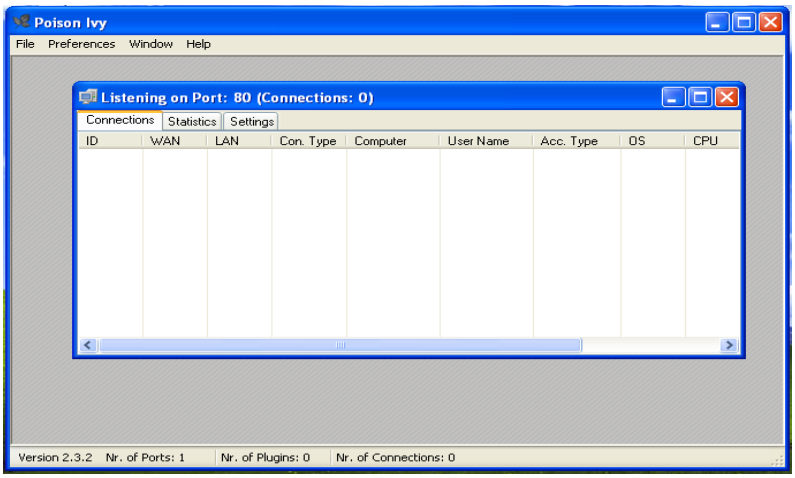


Una vez abierto el programa se creara un cliente nuevo y el procedimiento para esto es dar clic en File seguido de New Client.




Nos va a mostrar una ventana en la cual se puede seleccionar el puerto que se utilizara para el procedimiento de infección; el puerto 3460 es el que trae por default  pero habrá que cambiarlo por el puerto 80. Una vez seleccionado el puerto con el cual se va a trabajar solo falta seleccionar una contraseña y dar clic en el botón Start para dar por terminada la creación del cliente.



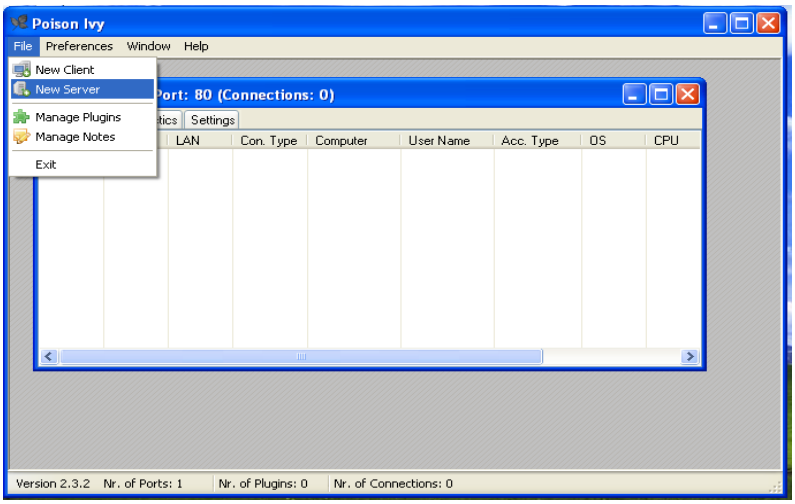



Nos muestra la ventana con el cliente creado y conectado al puerto escogido.

Una vez creado el cliente se procede a crear el server que va a ser con lo cual se infectara a la PC escogida para el ataque, para esto se realizarán los siguientes pasos:

1. - Clic en File.

2. - Clic en New Server.




3.- Crear Perfil: Se creó un perfil con el nombre Proyecto1 (Imagen 4.1).

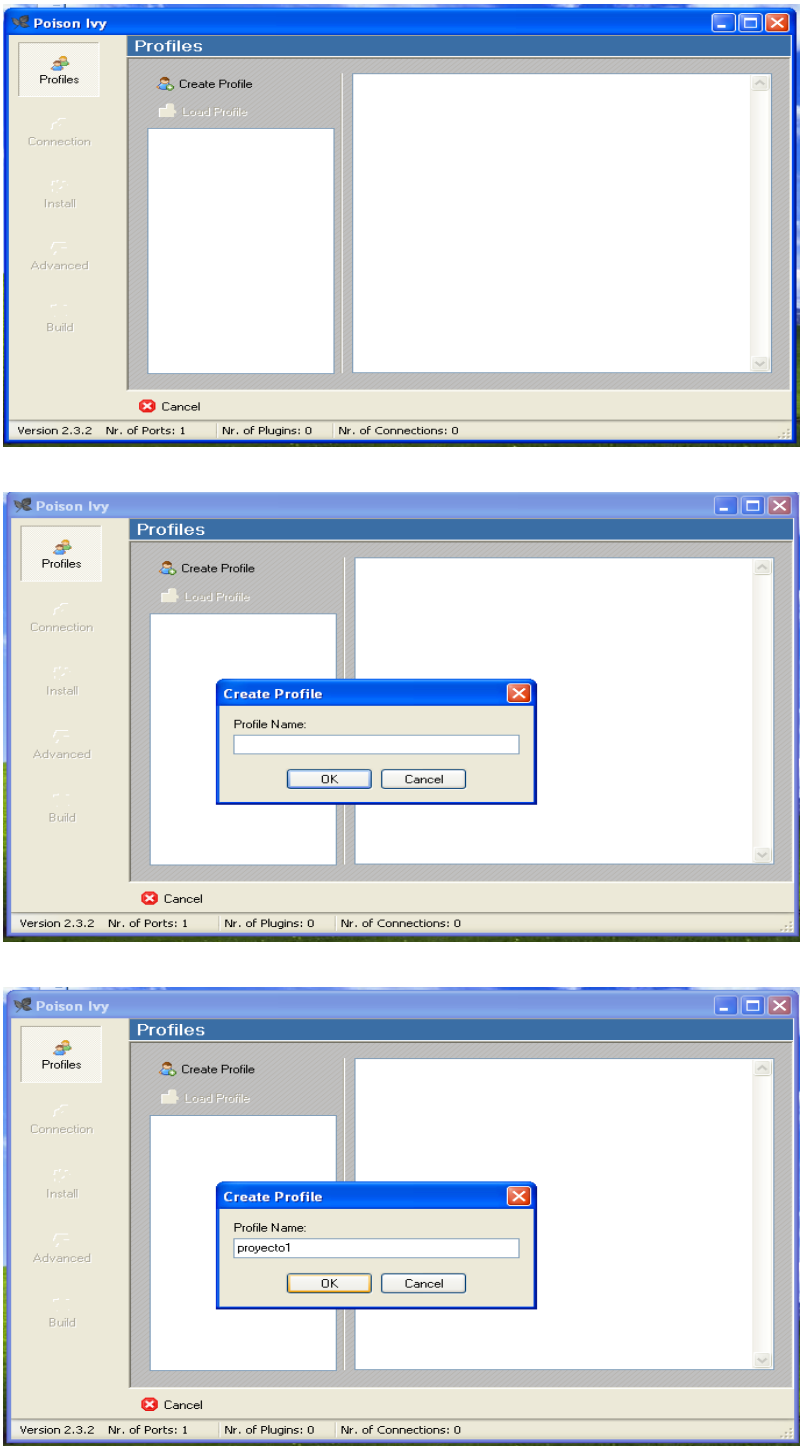
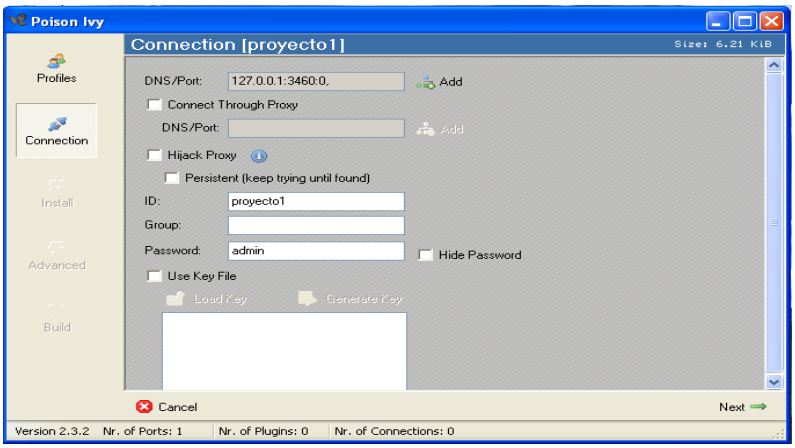
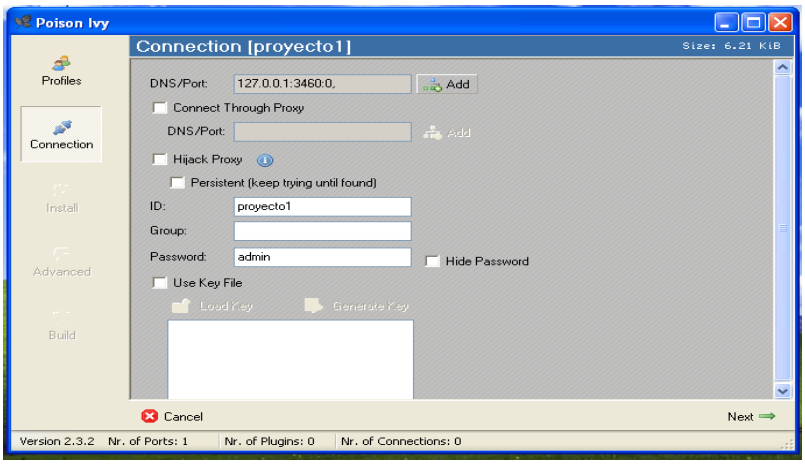


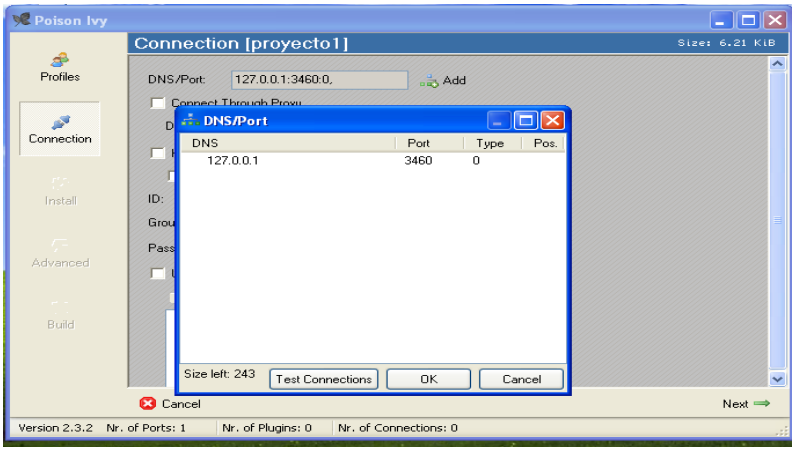

Ilustración 4.1: Creación del perfil

4.- Clic en ok para finalizar la creación del perfil y comenzar a configurarlo.




Para comenzar a configurarlo se pondrá la dirección IP de la maquina con la cual se realizara la intrusión en la casilla DNS/Port dando clic en agregar. Una vez ingresada la dirección IP habrá que cambiar el puerto que da por default al puerto 80 que es con el que se configuró el Cliente (Imagen 4.2).



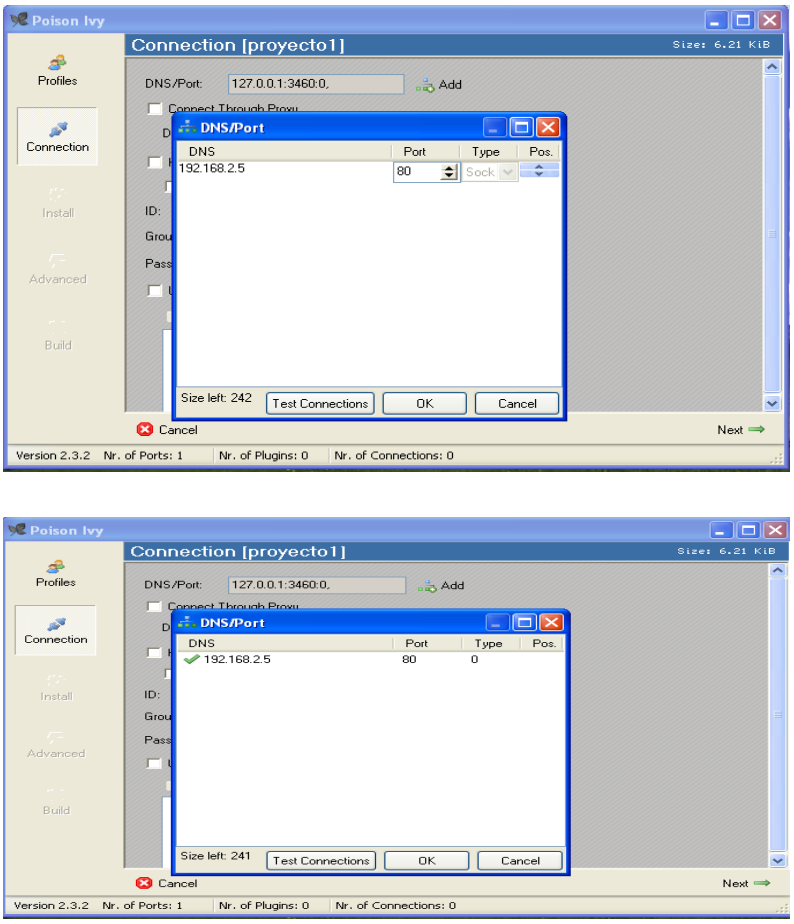
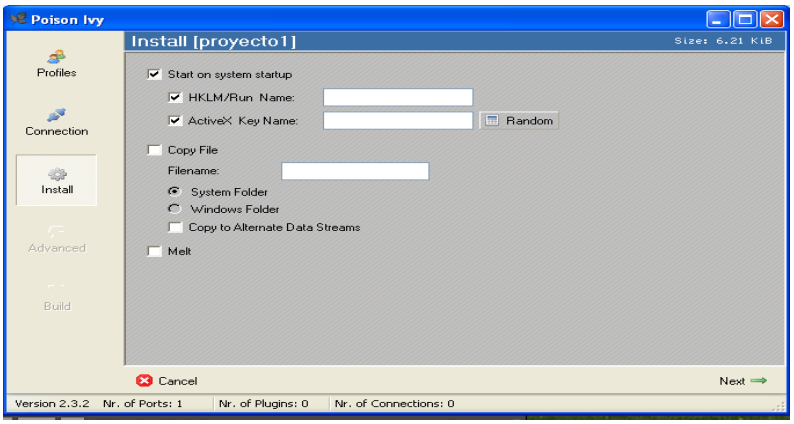
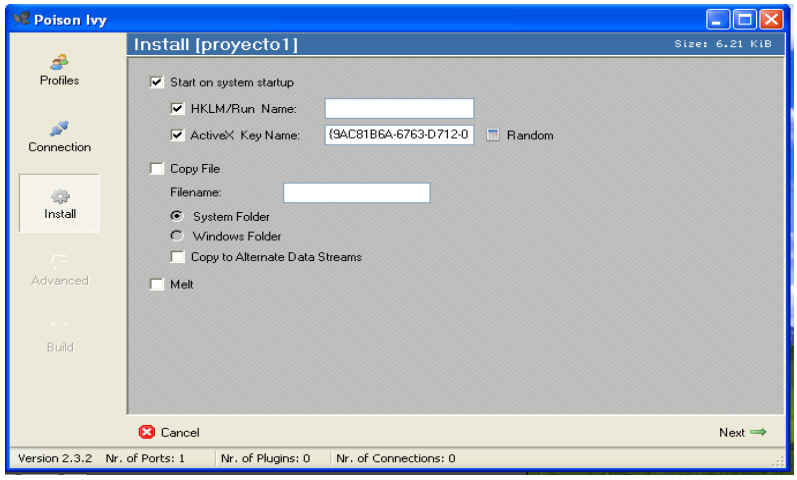


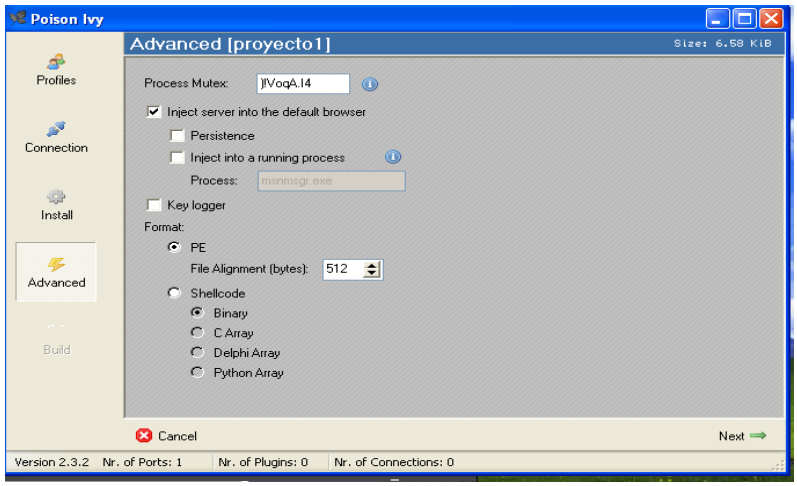

Ilustración 4.2: Configuración de IP y Puerto

5.- Una vez obtenida una correcta conexión se procede a tildar las siguientes casillas y algo muy importante es activar el ActiveX Key Name.

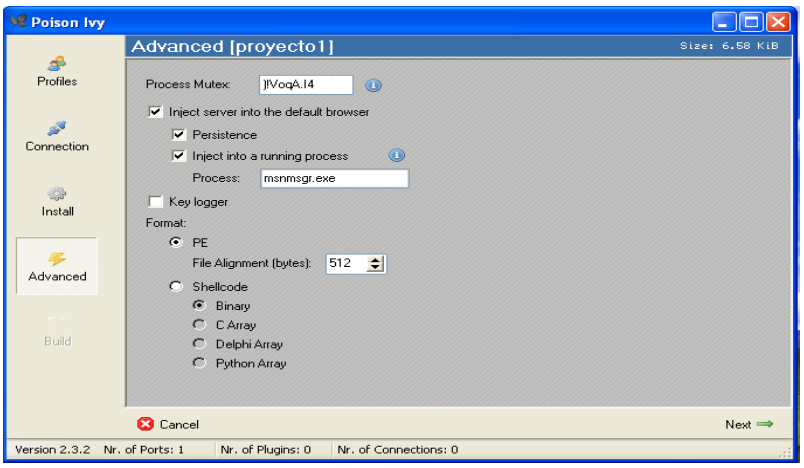




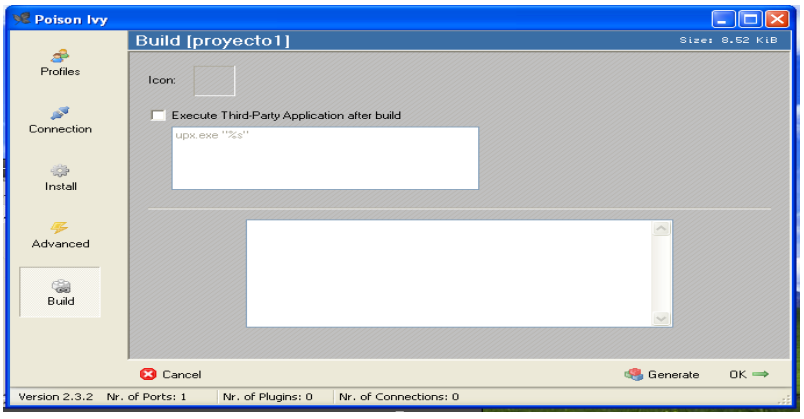

6.- Después de dar siguiente aparecerá una ventana en la que se deberá tildar la parte que dice Inject server into the default browser ya que esto hará que el troyano se active automáticamente cuanto el usuario de clic sobre él.



7.- Habrá que seleccionar como se va a ejecutar el virus, *en este caso se va a ejecutar con msnmsgr.exe* y después solo resta tildar la opción de persistencia para el equipo.




8.- Es importante que una vez dando clic en siguiente y aparezca la siguiente ventana, no tildar la casilla *ejecutar aplicaciones de terceros después de construir* ya que puede afectar seriamente al equipo en el cual se está creando este malware (Imagen 4.3). En esta ventana solo se deberá concluir el desarrollo del virus dando clic en *Generar* (Imagen 4.4). Una vez generado el troyano solo quedara introducir la ubicación en la cual quedará guardado y con esto se concluye el proceso de creación del virus.



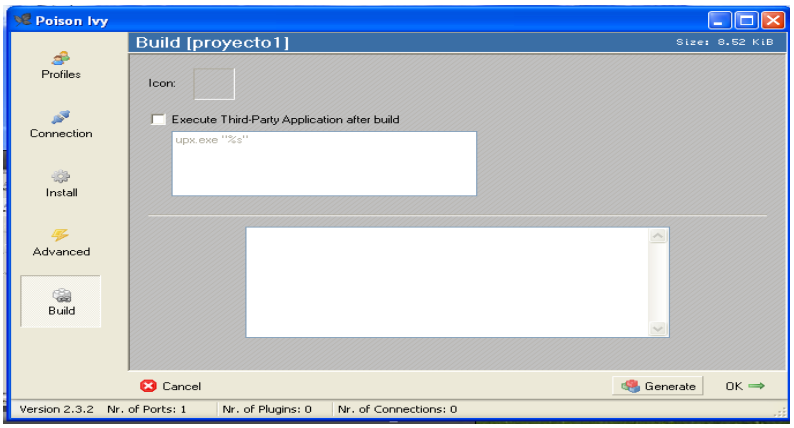
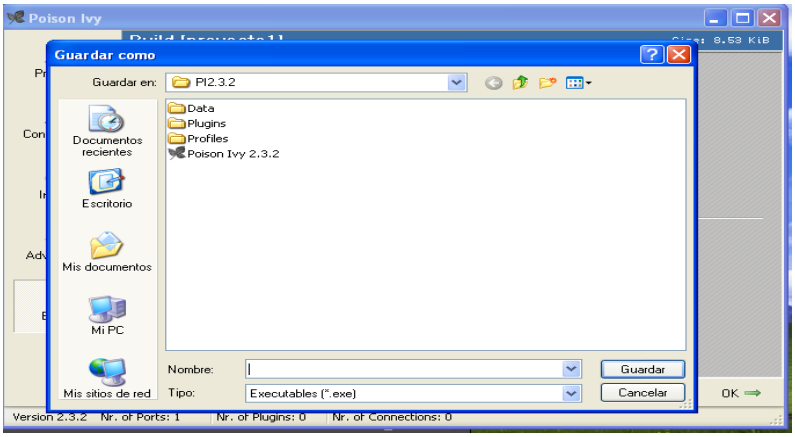



Ilustración 4.3: Ventana referente a ejecutar aplicaciones de terceros después de construir



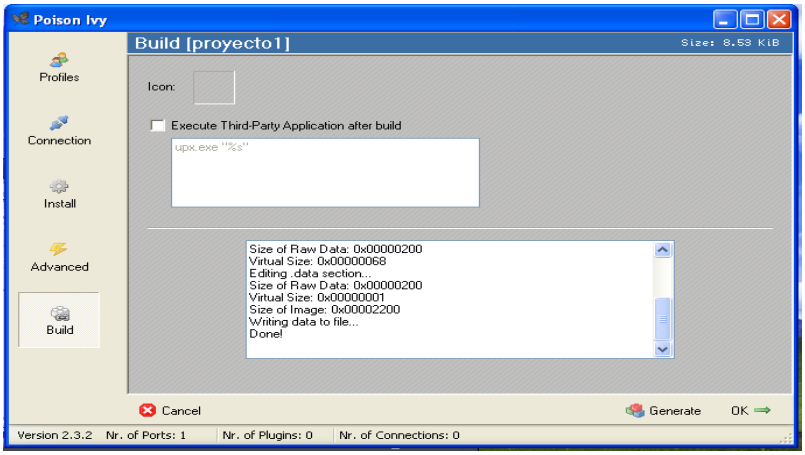
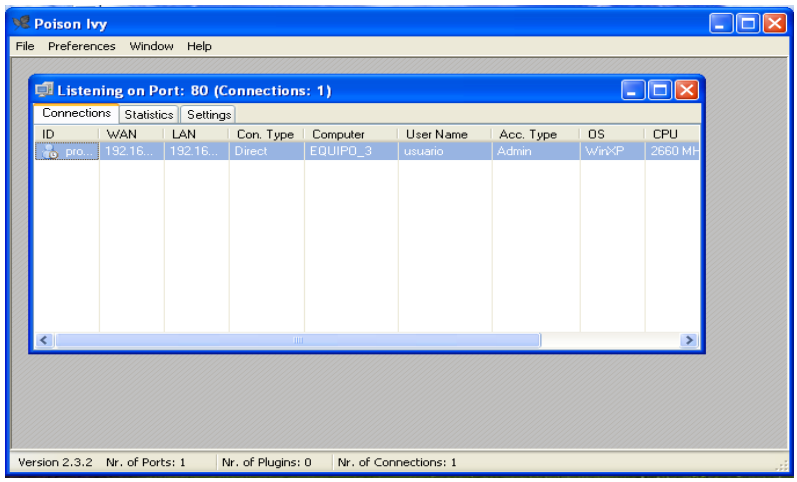




Ilustración 4.4: Ventana para generar el malware

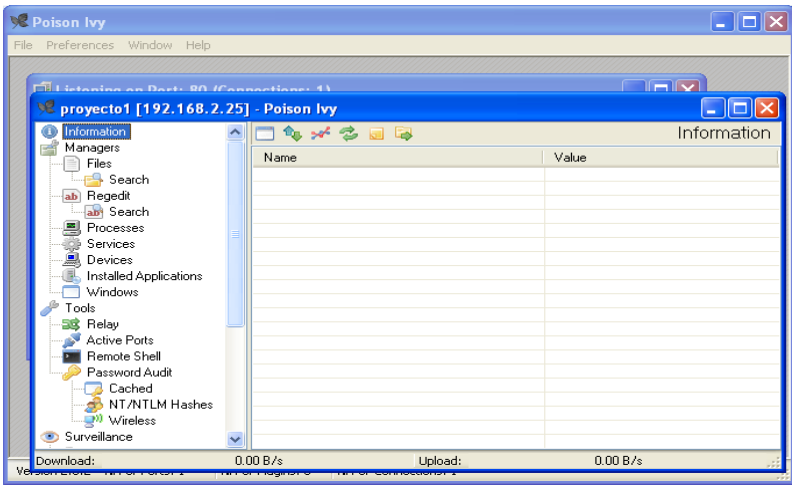
9.- Una vez guardado solo resta enviarselo a la victima para que este lo ejecute en su PC y el Spyware devuelva toda la informacion de la Pc infectada y entonces poder manipular todo lo referente a ella via remota.

Lo que se muestra a continuación es la parte de lo que devuelve el troyano una vez ejecutado en la PC de la cual se extraera información. Lo primero que muestra el software al ingresar a el es el numero de PCs que han sido infectadas con el troyano y con las cuales tiene comunicación, en este caso solo una que es la que previamente se infectó.



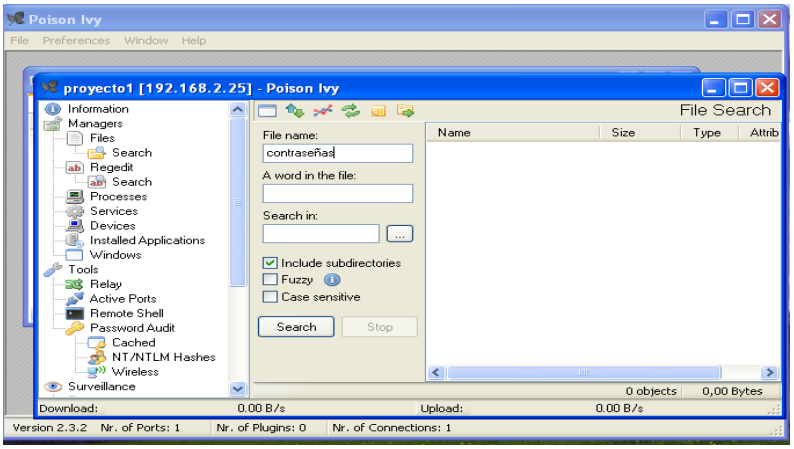

Al dar doble clic sobre la PC identificada nos mostrará la dirección IP de la máquina y todo lo referente a ella:

- Sistema Operativo
- Sistema de Archivos
- Claves
- Procesos activos
- Acceso a la camara en tiempo real sin ser identificados




En este caso para el fin práctico se procedera a extraer un documento que el usuario nombró contraseñas y para esto se seguirán los siguientes pasos:

1.- En la opción Buscar se pondra el nombre del documento ”*contraseñas*” para que comience la búsqueda real de la ubicación del documento.




2.- Para esto se seleccionaran los dispositivos en los cuales se desea la búsqueda que como se puede ver en la Imagen 4.5, la PC no tiene conectados en el momento dispositivos flash por lo tanto se seleccionara el Disco Duro.

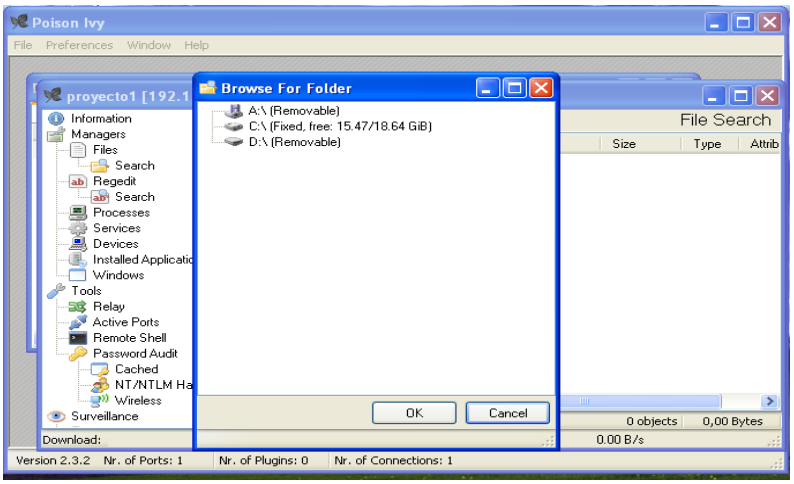
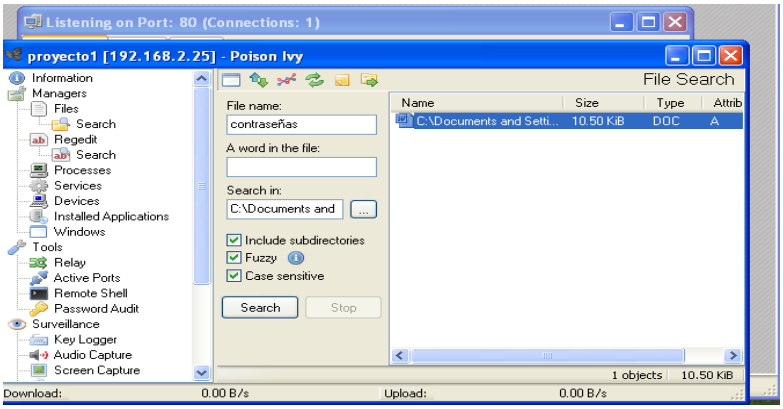



Ilustración 4.5: Dispositivos conectados

3.- Como se ve en la siguiente imagen se ha encontrado el archivo




4.- Como se requiere visualizar el contenido y afectar al usuario lo siguiente es dar clic derecho sobre la dirección del archivo y descargarlo como se ve a continuación en la Imagen 4.6.

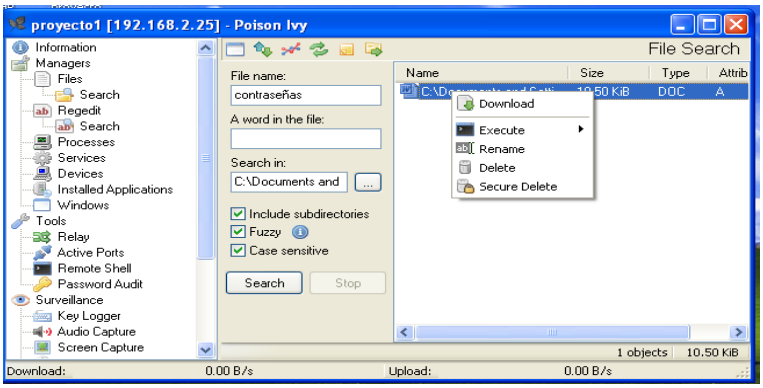
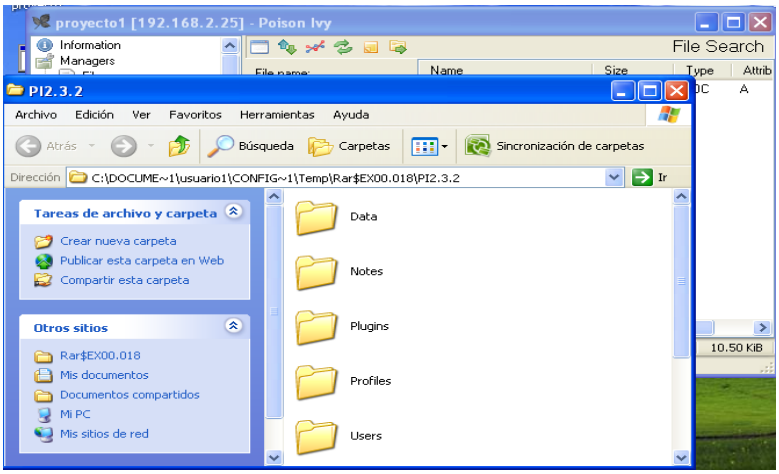
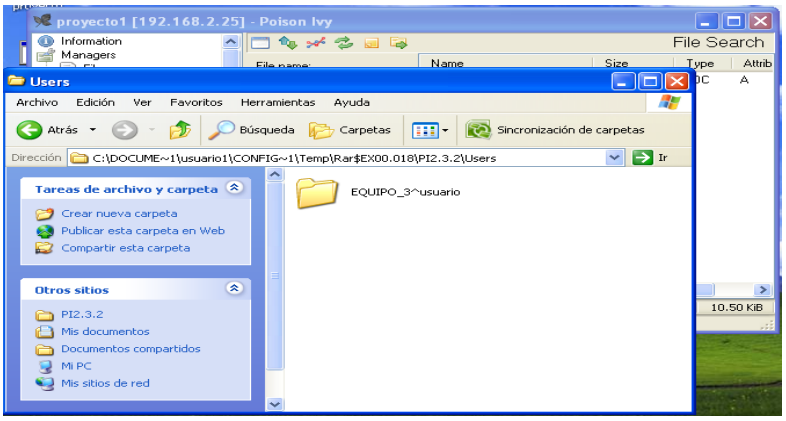
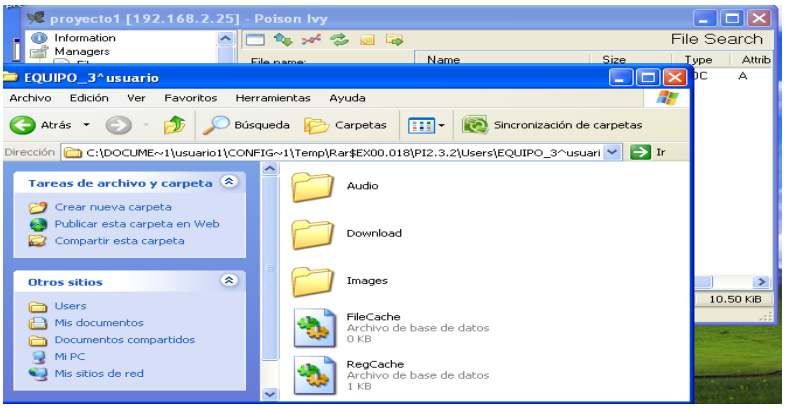


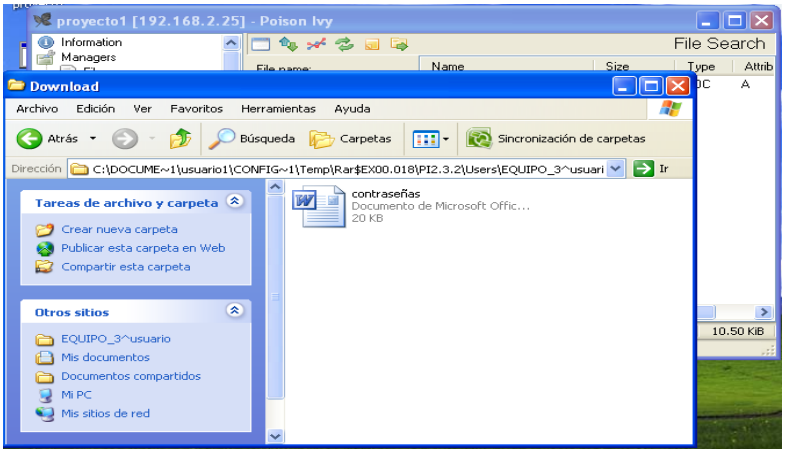

Ilustración 4.6: Ventana para la descarga del archivo

5.- Lo siguiente es ver que se halla extraido correctamente y para esto se dará clic en el icono ver posicion el cual abrira la direccion de las carpetas en la cual se guardara todo lo que se realice con el software. Toda la información que se descargue se encontrará en la carpeta Users en donde se alojaran por separado las PCs infectadas con sus respectivas subcarpetas como se muestra en las siguientes imágenes.






6.- Una vez encontrado la descarga del archivo la Imagen 4.7 muestra lo que se encontró

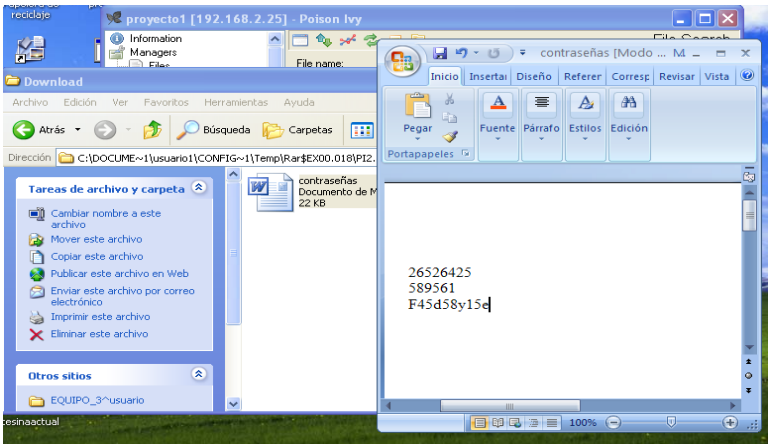
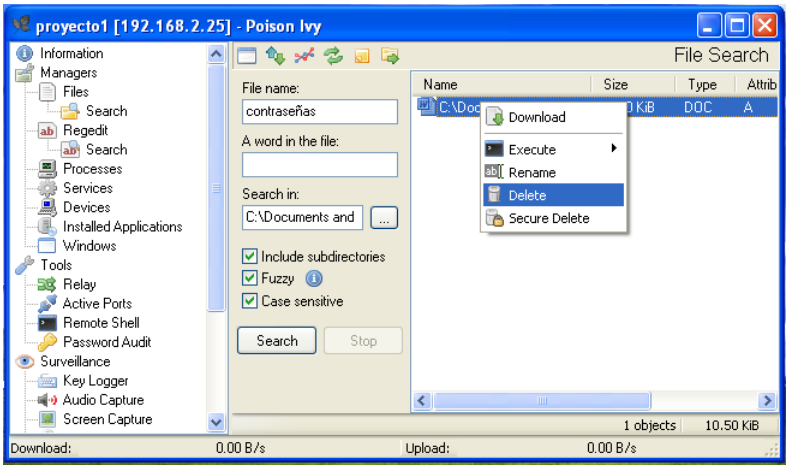



**Ilustración 4.7: Archivo descargado**

7.- Solo queda eliminar el archivo de la Pc del usuario infectado (Imagen 4.8) y de este modo se realizó la intrusión y eliminación de datos de importancia para el usuario.



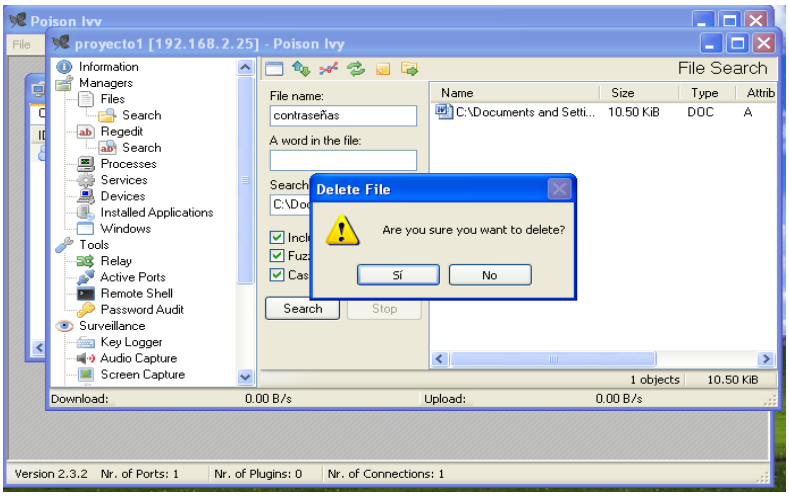



Ilustración 4.8: Eliminación de archivo

## 4.3 Desarrollo del proceso de Análisis Forense

Lo primero que se va a realizar es extraer el Disco Duro de la PC infectada e instalarlo en modo esclavo en la PC en la que se realizará el análisis.

En la Imagen 4.9 se muestra el Disco Duro ya montado en la PC.

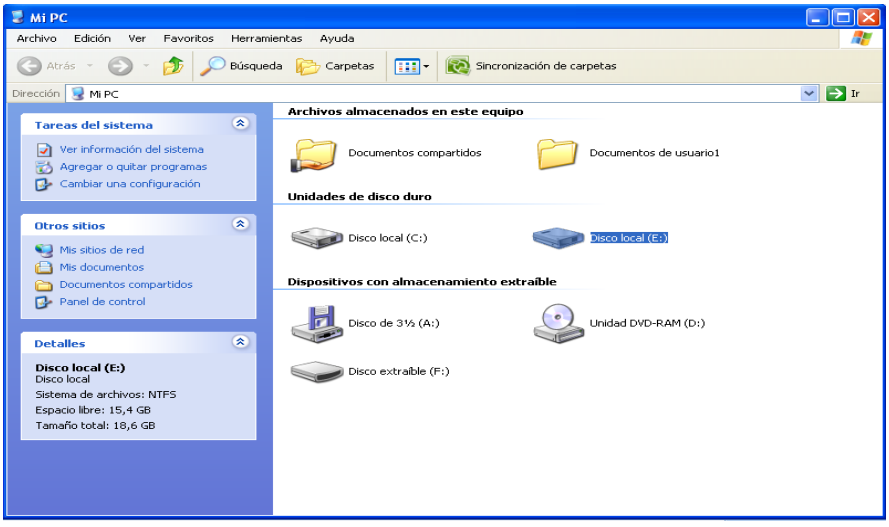



Ilustración 4.9: Disco Duro montado

Lo siguiente es crear una carpeta en donde alojaremos todo lo referente al análisis que se realizará y este será en la carpeta Mis Documentos (Imagen 4.10).

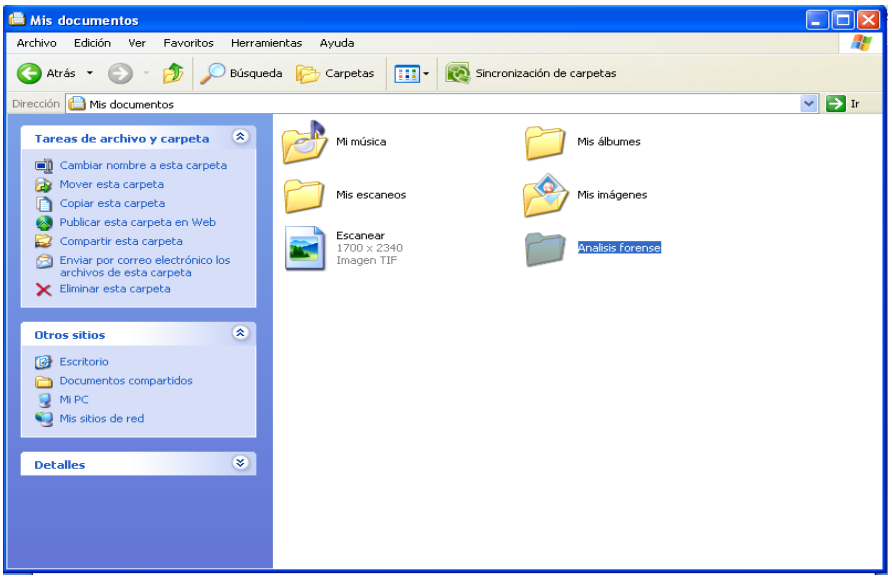



Ilustración 4.10: Carpeta creada en Mis Documentos

Como el archivo por el cual se realizara el análisis ya no está visible en el Disco Duro porque fue extraída y eliminada; y además de esto el usuario no cuenta con alguna copia se comenzará este análisis sin alguna imagen de datos. Por lo cual se comenzará el método en el paso 6.

La Imagen 4.11 muestra la Herramienta EnCase con la cual se realizará el análisis.

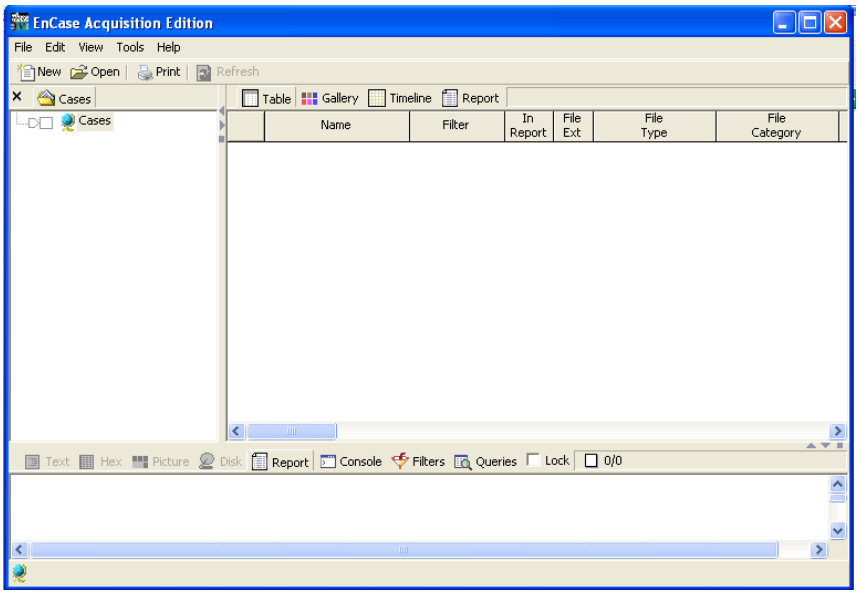
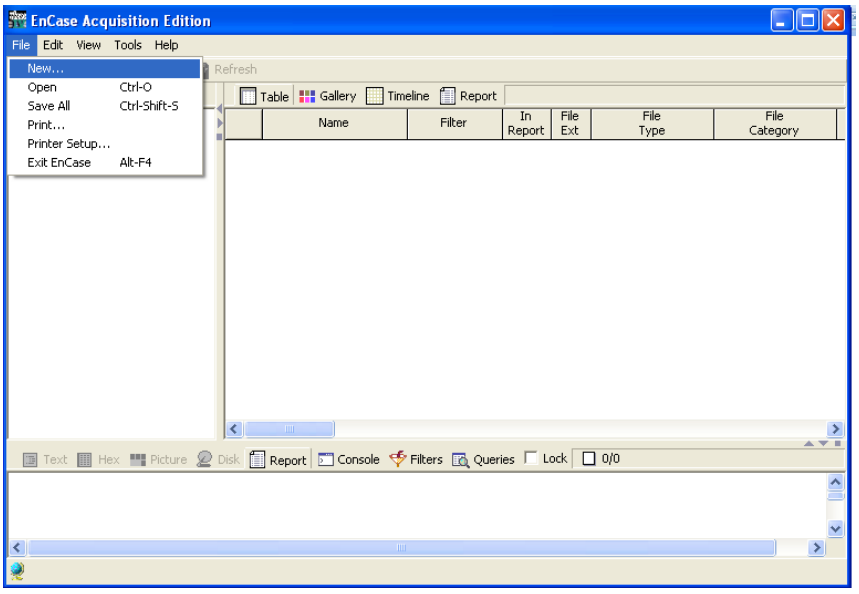



Ilustración 4.11: EnCase

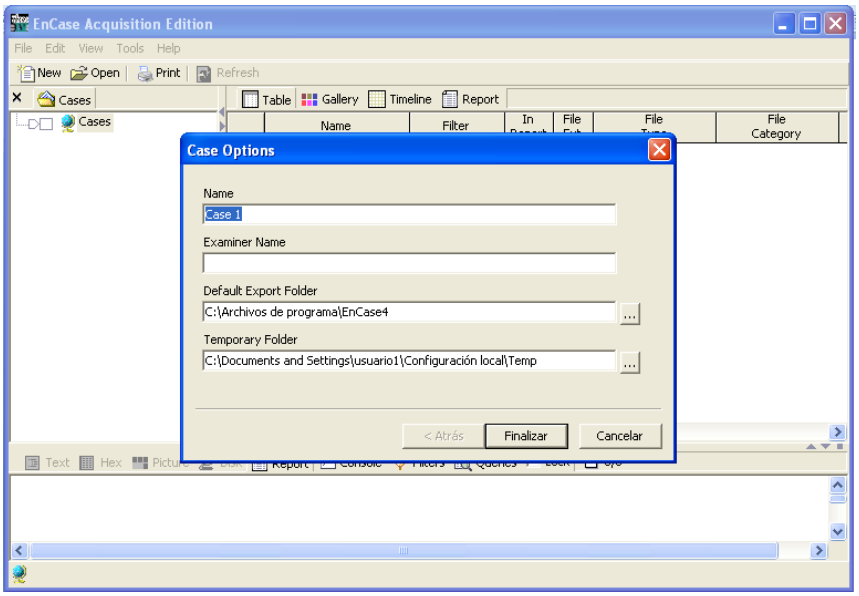
Para comenzar el desarrollo del método se creará un nuevo caso y para esto se seguirán los siguientes pasos:

1.-File.

2.-New.




3.-Aparecerá una nueva ventana en la cual se ingresará el *nombre del caso* y *nombre del investigador.*




5. Una vez ingresados los datos habrá que dar clic en *Finalizar* para terminar el proceso de creación del nuevo caso (Imagen 4.12).

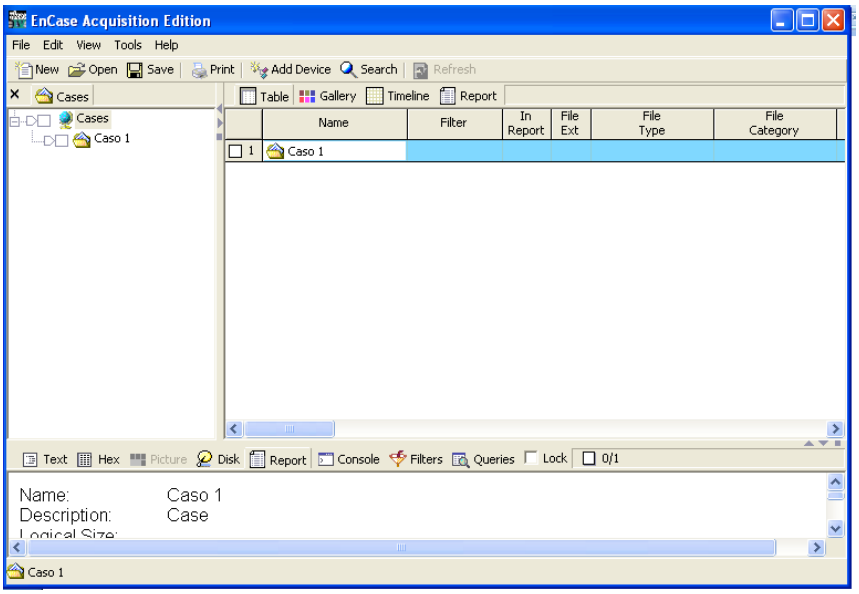
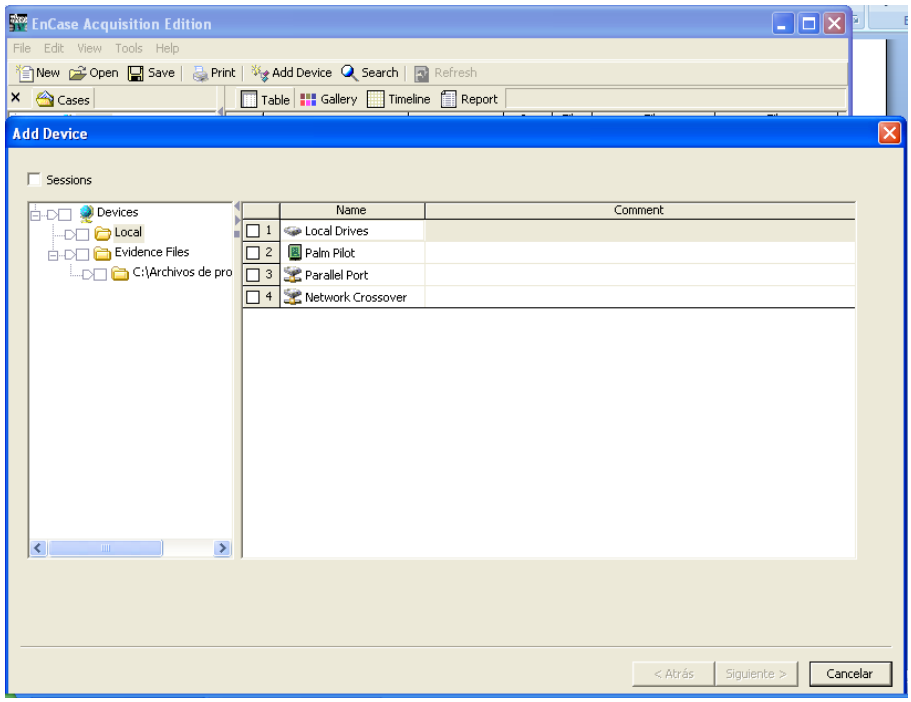


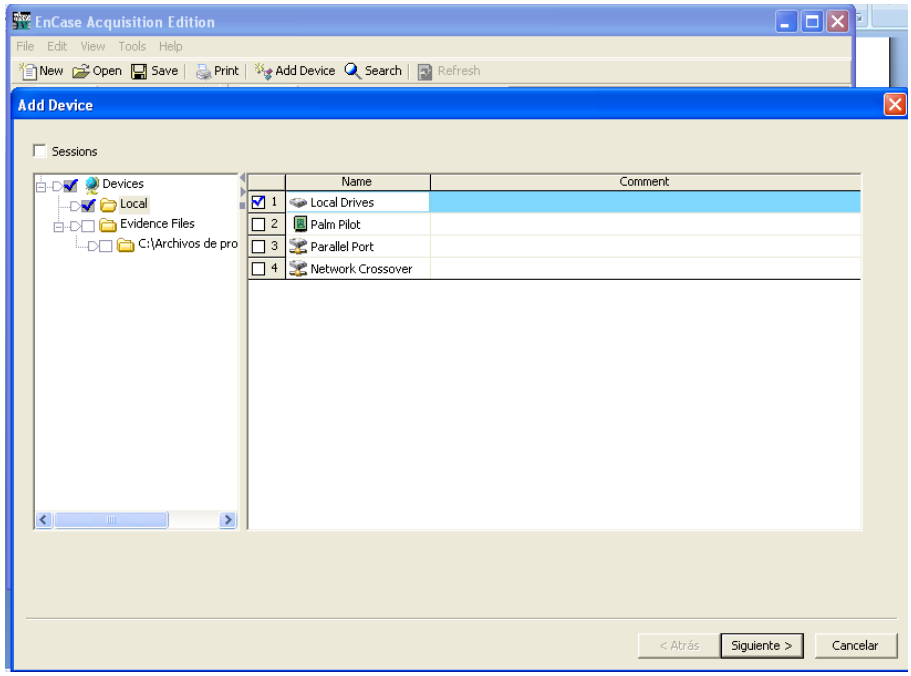

**Ilustración 4.12: Nuevo caso**

Ya creado el Caso se deberá agregar el dispositivo a analizar que en este caso es el Disco Duro de la PC afectada. Para esto se seguirán los siguientes pasos:

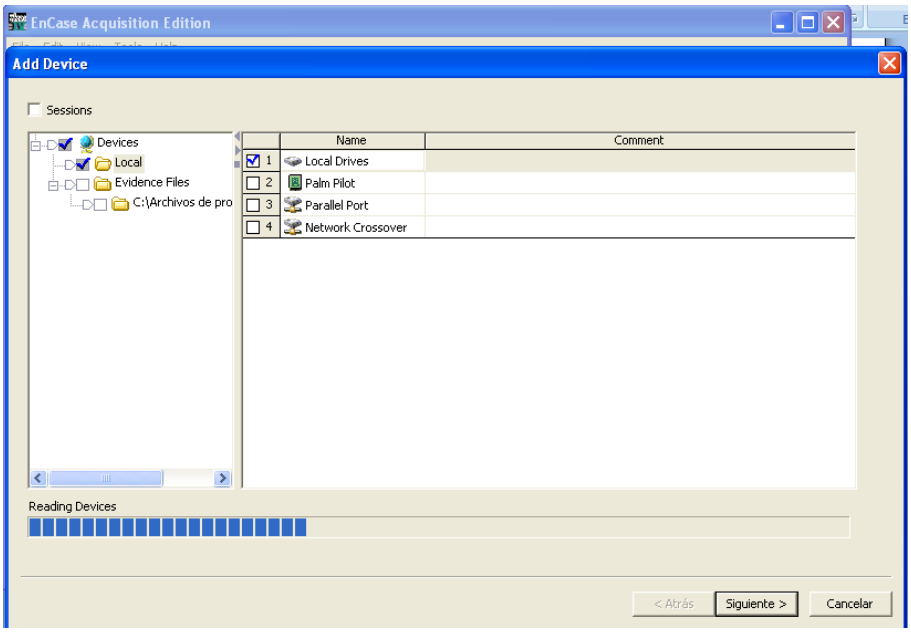
1. Add Device.

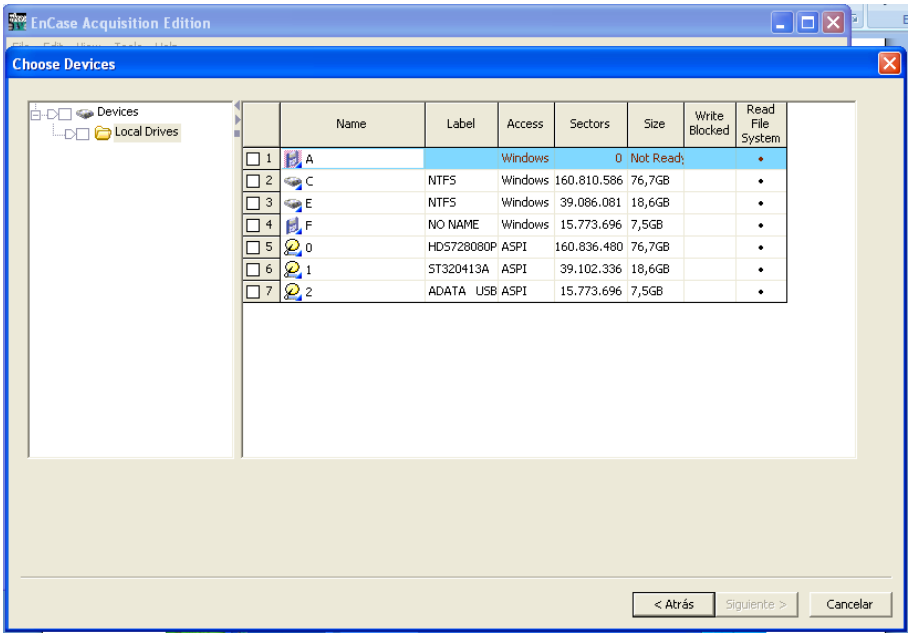



2.- Local Drivers.




3.-Al darle siguiente comenzará a buscar los dispositivos conectados.




4.- Se deberá tildar el Disco Duro de la PC afectada y al dispositivo virtual que se crea en automático (Imagen 4.13).

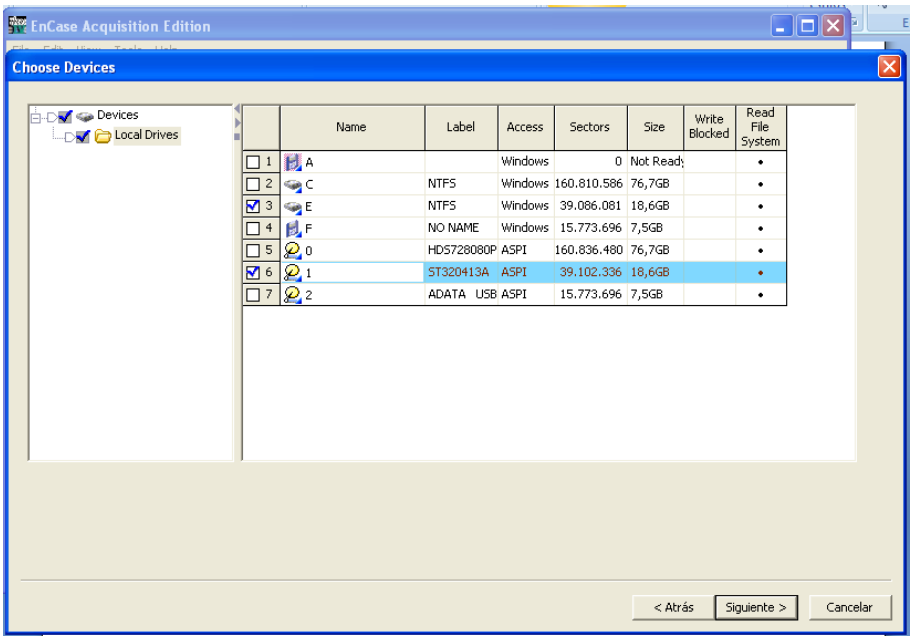
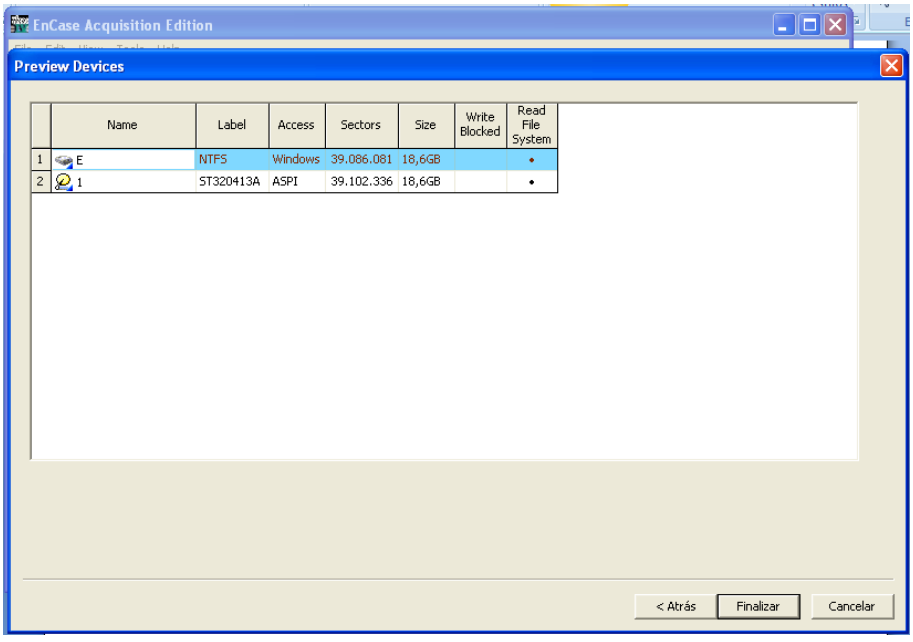



Ilustración 4.13: Selección de dispositivos

6. Al dar siguiente se verán las unidades seleccionadas a analizar y solo resta dar clic en finalizar




En la siguiente ventana aparecerán las unidades seleccionadas y con ellas todo lo que contienen (Imagen 4.14).

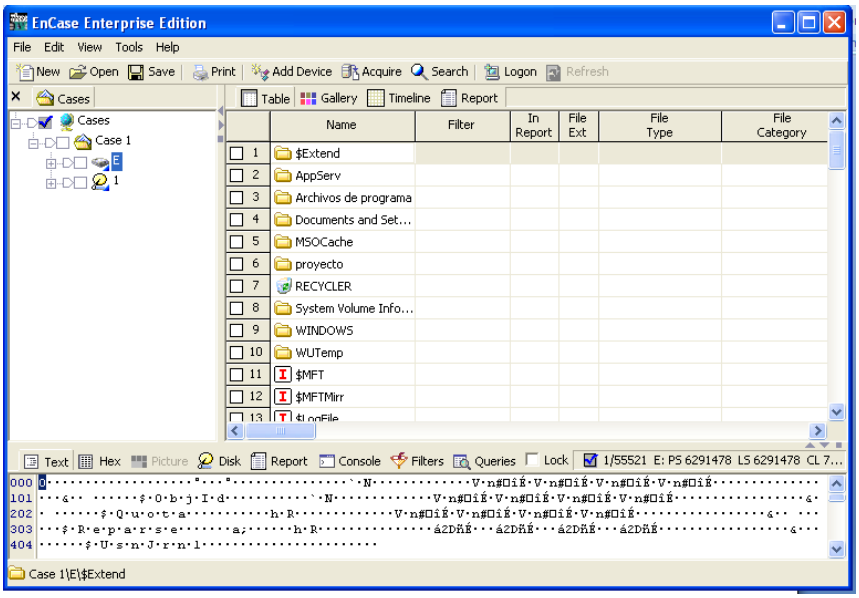



**Ilustración 4.14: Dispositivos montados a la herramienta EnCase**

Para visualizar los archivos que se encuentran dentro de la unidad y que corresponde a la *Identificación de las particiones actuales y anteriores* del método habrá que tildar la flecha que identifica a la misma y entonces se muestran todas las carpetas y particiones del Disco Duro (en este caso la Herramienta EnCase no identifico ninguna *partición*) Imagen 4.15

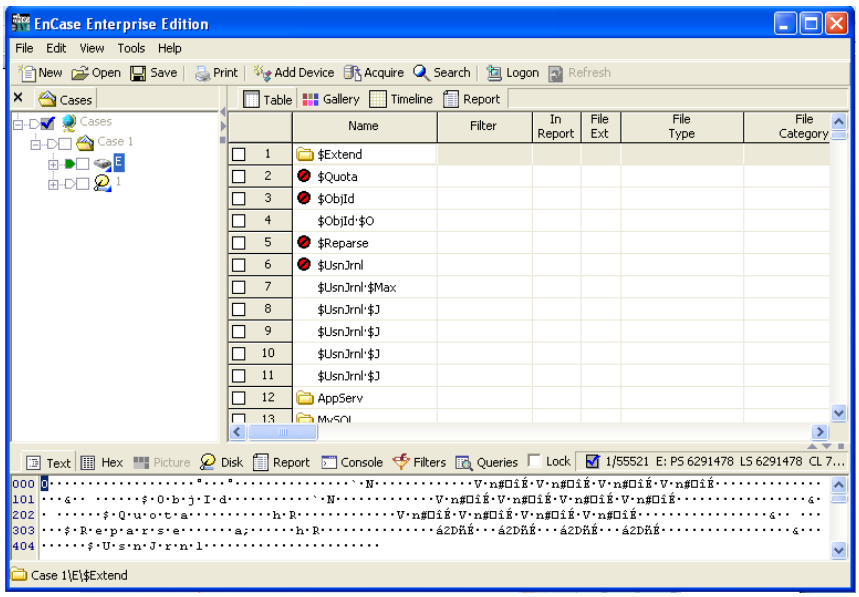



**Ilustración 4.15: Contenido de las unidades montadas y particiones**

A partir de aquí se comenzará a buscar el archivo extraído Imagen 4.16 y 4.17.

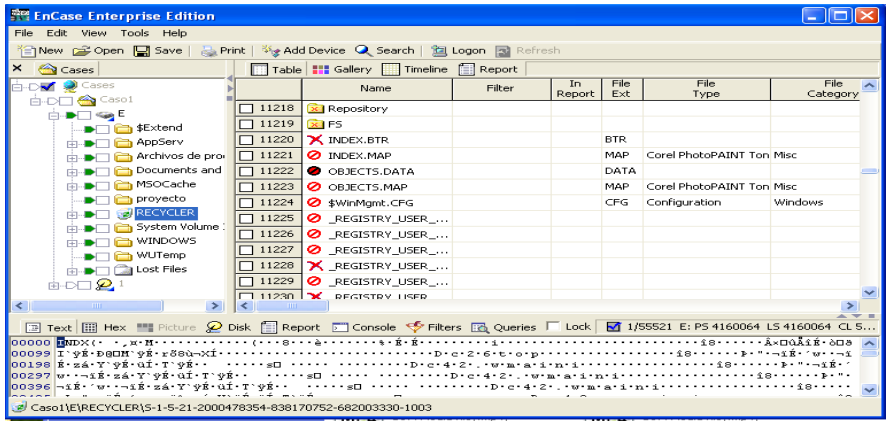



**Ilustración 4.16: Búsqueda de la información**

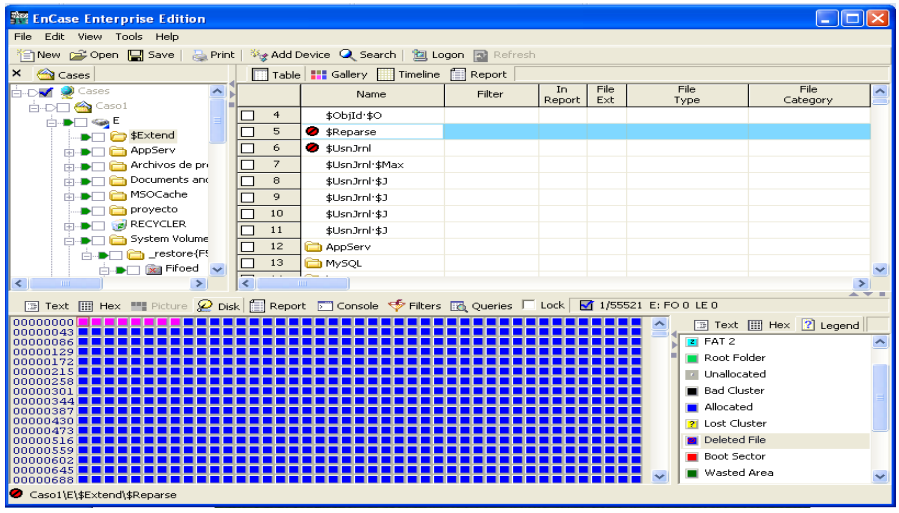
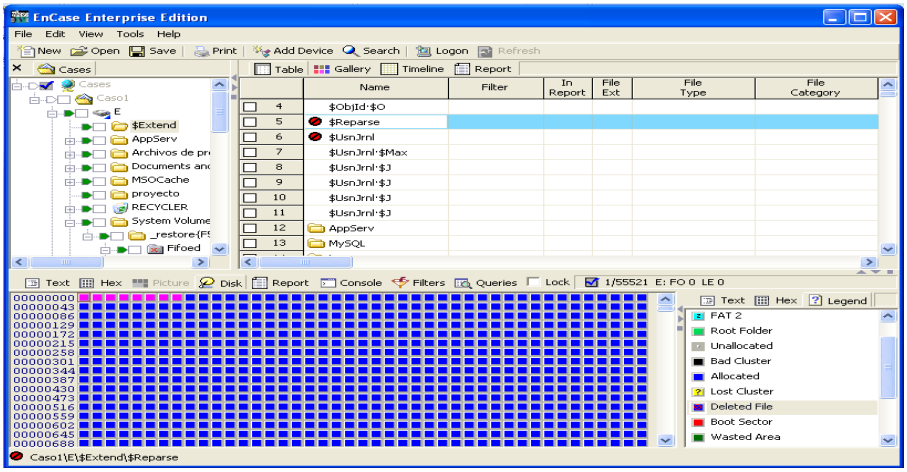



**Ilustración 4.17: Búsqueda de la información**

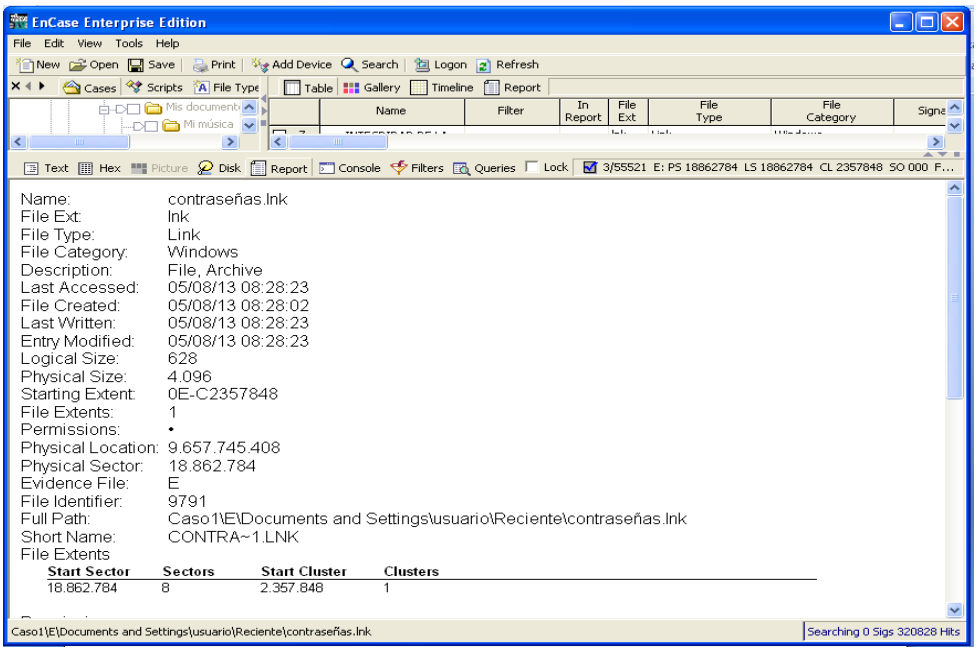
*Detección de información en los espacios entre las particiones e Identificación del sistema de archivos*.

Al no haber encontrado particionado el disco no existe espacio entre particiones que puedan ser analizadas y la herramienta muestra que es un sistema de archivos *NTFS*.



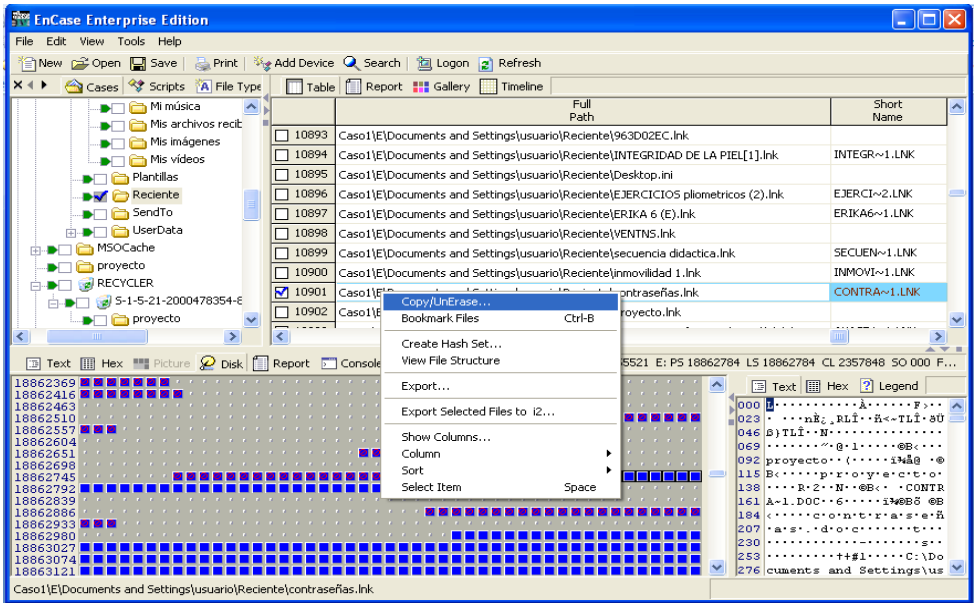

*Recuperación de archivos borrados.*

Después de una exhaustiva búsqueda se logró encontrar el archivo contraseñas en la siguiente ubicación.



Ahora se procederá a recuperarlo. Para esto seguiremos los siguientes pasos:

1. Dar clic derecho sobre el archivo y clic en Copy/UnErase




2. Aparecerá la siguiente ventana (Imagen 4.18) y en esta se tildará la opción de Archivo de Alta Calidad.

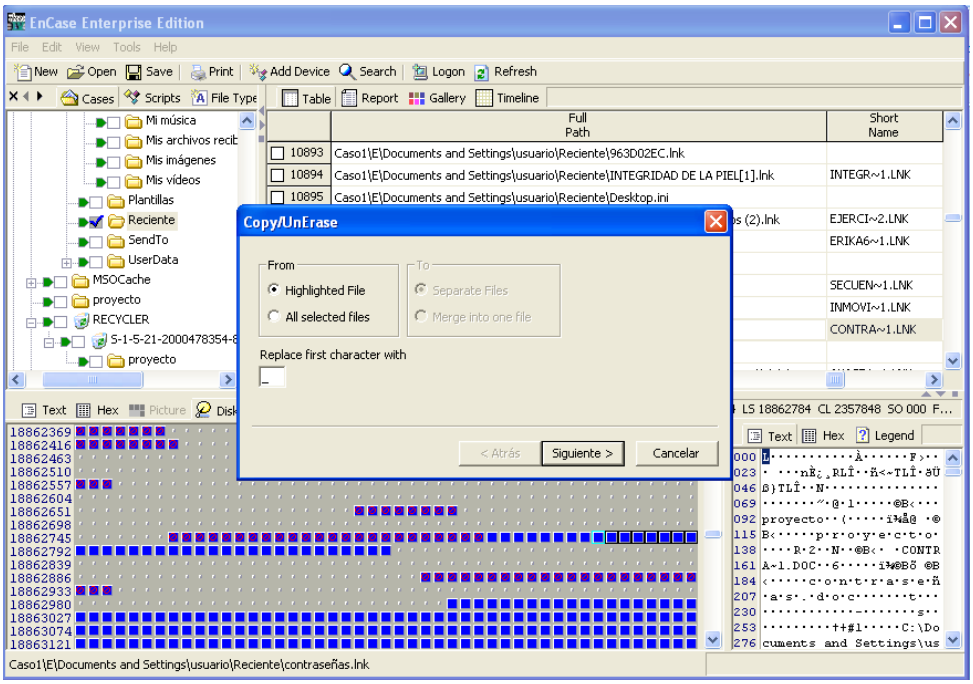
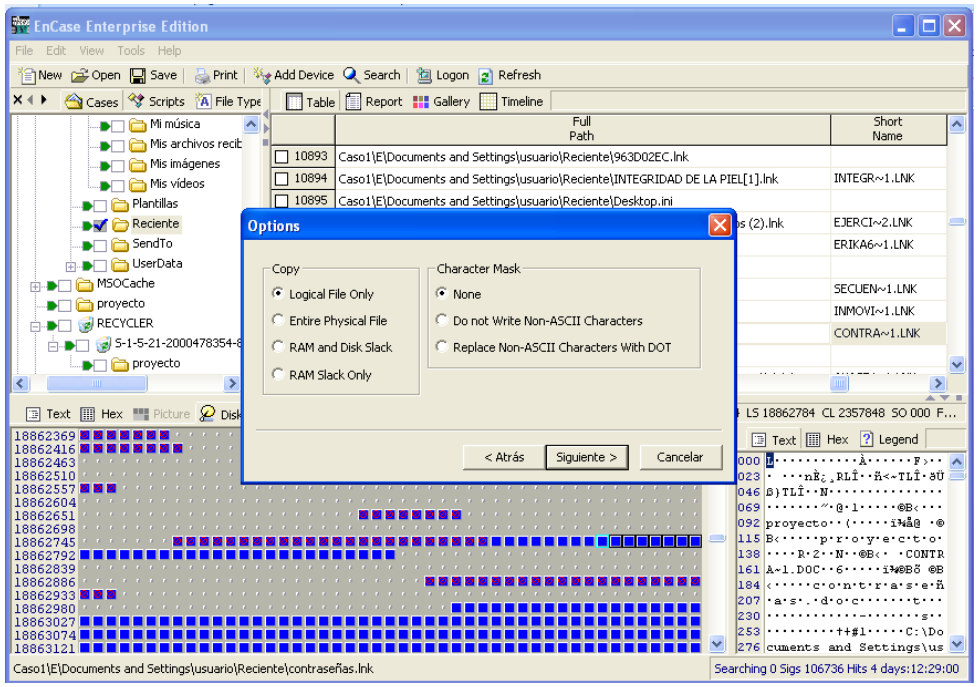



Ilustración 4.18: Propiedades del archivo a recuperar

3. Lo siguiente se deja como aparece por default y se le dará siguiente.




Nos muestra que el proceso ha sido finalizado.

Por ultimo mostrara que el Guardado ha finalizado y es hora de ir a la carpeta que se creó para guardar lo obtenido por el programa (Imagen 4.19).

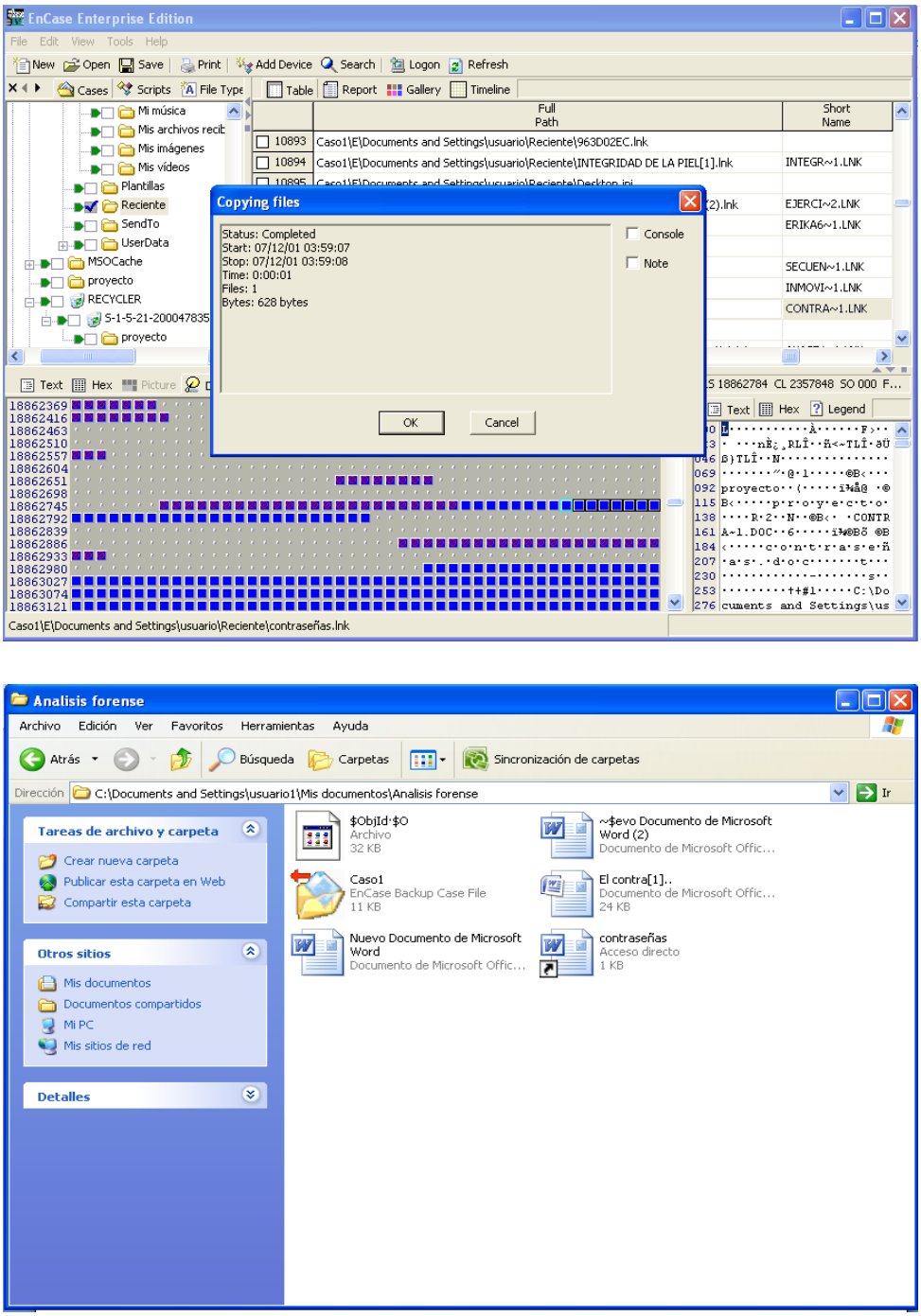
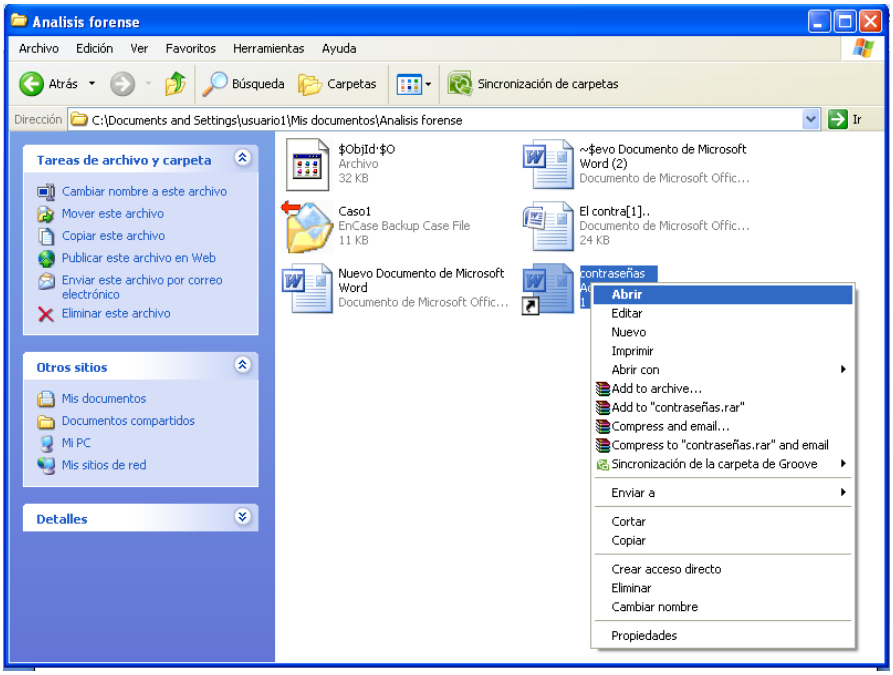



Ilustración 4.19: Documento descargado

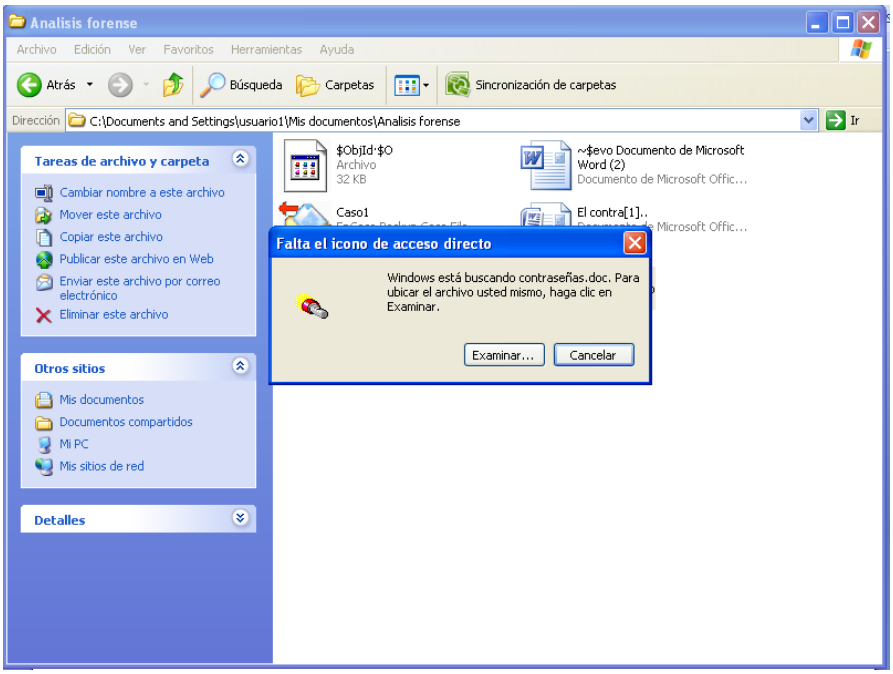
Ya en la carpeta en donde se almacena lo referente al análisis la herramienta solo logro recuperar un acceso directo del archivo contraseñas ya que como la información fue extraída por la PC que atacó el sistema y después la borro, el archivo se reubicó.

Para recuperarla se realizará lo siguiente:

1.-Clic derecho en el acceso directo y clic en Abrir.




Windows comenzará a buscar el archivo *contraseñas*.



Como no lo va a encontrar porque ya no está, el sistema va a pedir que se repare el acceso directo para hacer referencia al documento. Se le dará reparar (Imagen 4.20)

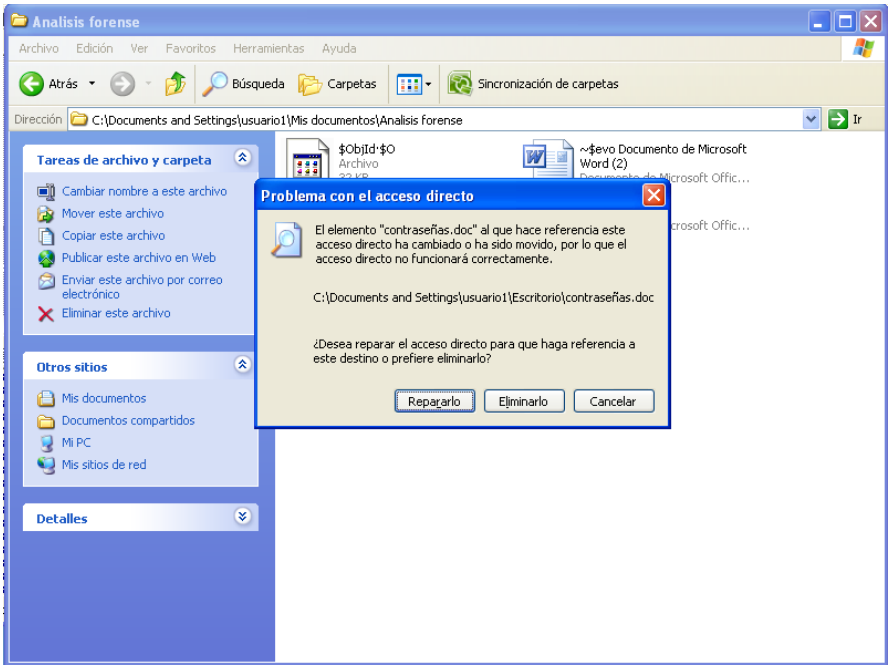
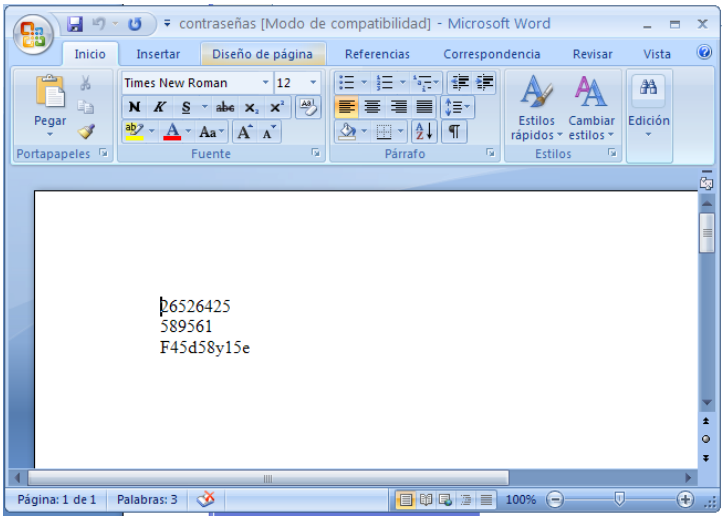



Ilustración 4.20: Leyenda del sistema Windows para reparar el archivo

Una vez que esto pase se podrá abrir el archivo nuevamente y ver si hay modificaciones o alteraciones a la información contenida en él.



*Recuperación de información escondida y Consolidación de archivos potencialmente analizables.*

En este caso se analizarán todos los archivos de la carpeta *Reciente* en la cual se encontró el documento *contraseñas.* A su vez no se encontró ningún clúster dañado para ningún archivo con estas propiedades.

*Identificación de archivos protegidos.*

No se identificó ningún archivo protegido con contraseña.

*Determinación del sistema operativo y las aplicaciones instaladas.*

En este punto se el usuario afectado dispone de la información del sistema operativo y las aplicaciones instaladas en su Disco Duro. Por lo cual solo se realizó un análisis visual en la carpeta *archivos de programa* para buscar algún programa no identificado por el usuario.

*Filtrado basado en archivos buenos conocidos y Consolidación de archivos sospechosos*

Al haber un ataque ya identificado todos los archivos de la carpeta *Reciente* son potencialmente sospechosos.

*Primera clasificación.*

Se encontró un archivo llamado *~$evo Documento de Microsoft* que puede ser el medio por el cual el atacante pudo tener acceso al sistema de archivos del usuario afectado.

*Segunda clasificación.*

Se analizó el documento *~$evo Documento de Microsoft* y solo se logró saber que era un archivo dañado.

*Analizar los archivos.*

No se pudieron determinar inconsistencias en los archivos encontrados en la carpeta *Reciente*. Esto se realizó mediante la herramienta *md5sum*. (Imagen 4.21)

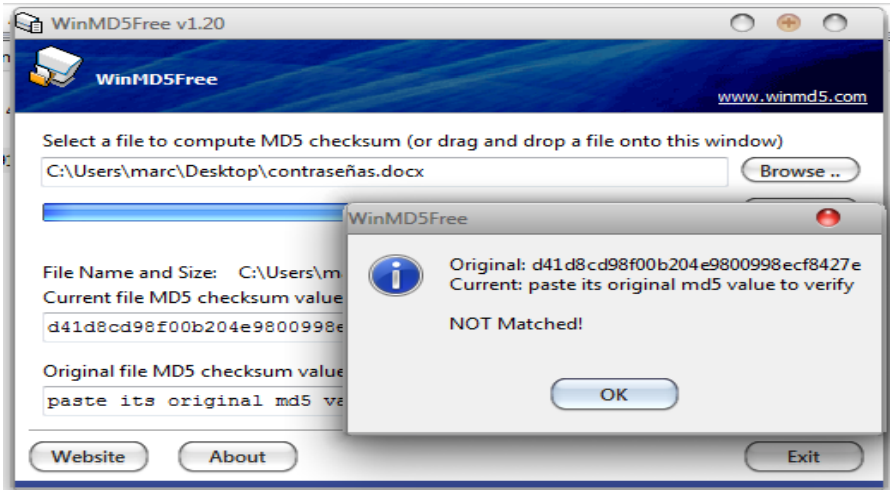
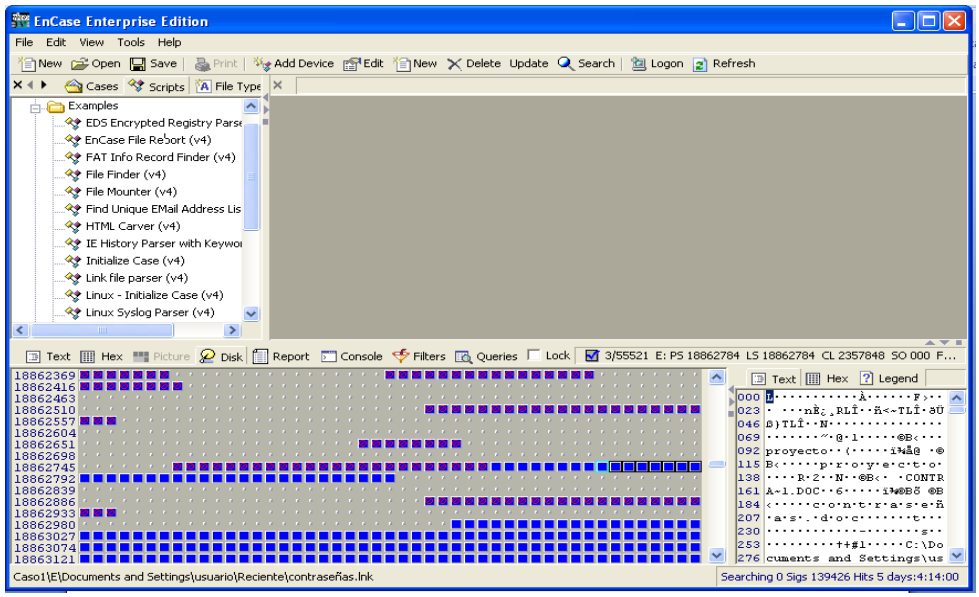



Ilustración 4.21: Herramienta md5sum con archivo contraseñas comprobado

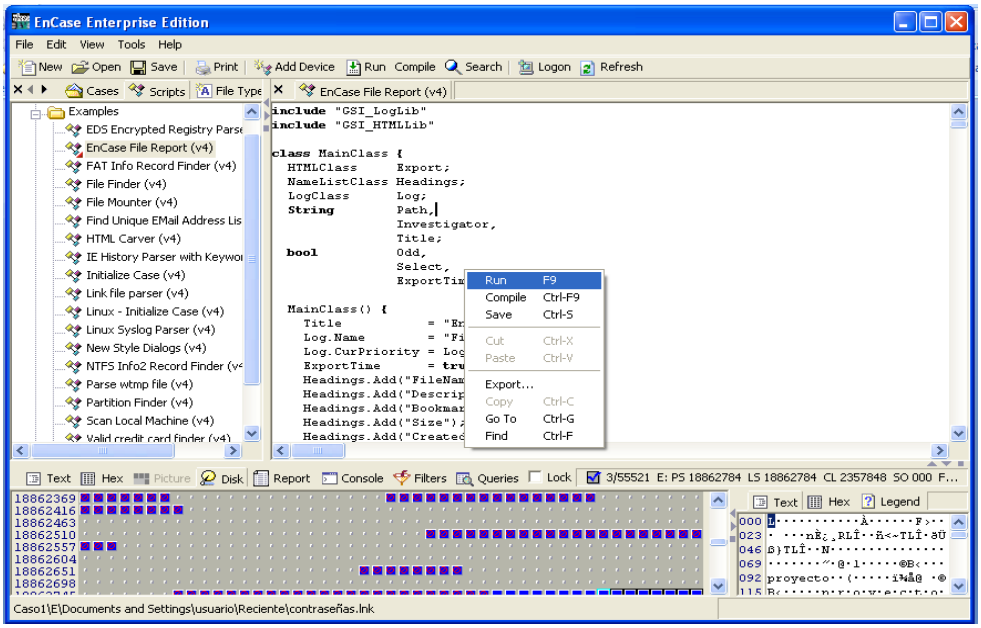
*Creación del reporte*

Esta parte del análisis se realizara en la pestaña Scripts de EnCase

1. Clic en la carpeta Examples
2. Doble clic en EnCase File Report



3.- EnCase devolverá un código que es el que nos creará el reporte. Se le dará clic derecho seguido de la opción *Run*




4.- Se proporcionará el *nombre del investigador, nombre del caso y dirección en la cual se guardará el reporte*; tal como se ve en la siguiente ventana (Imagen 4.22)

5.- El proceso terminará al dar clic en *Siguiente.*

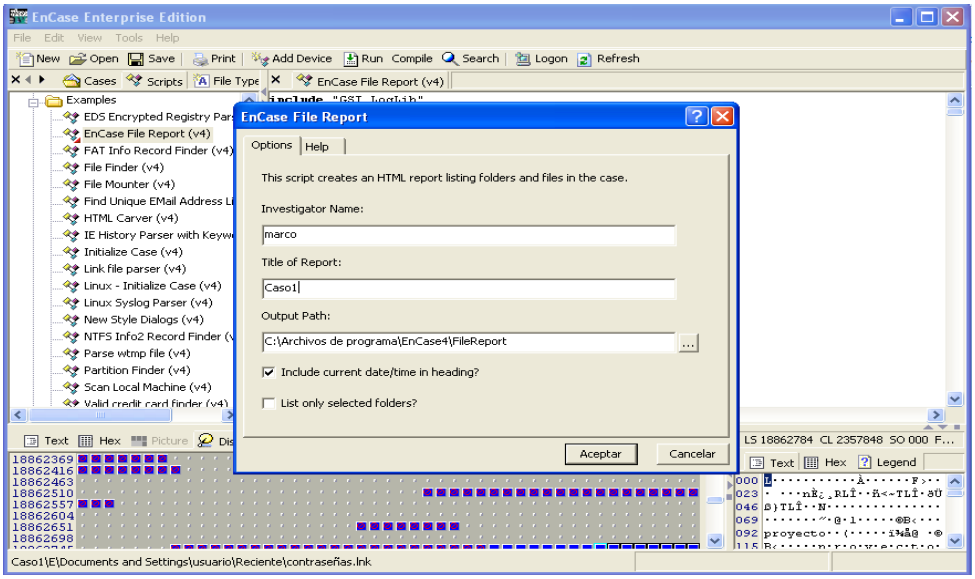
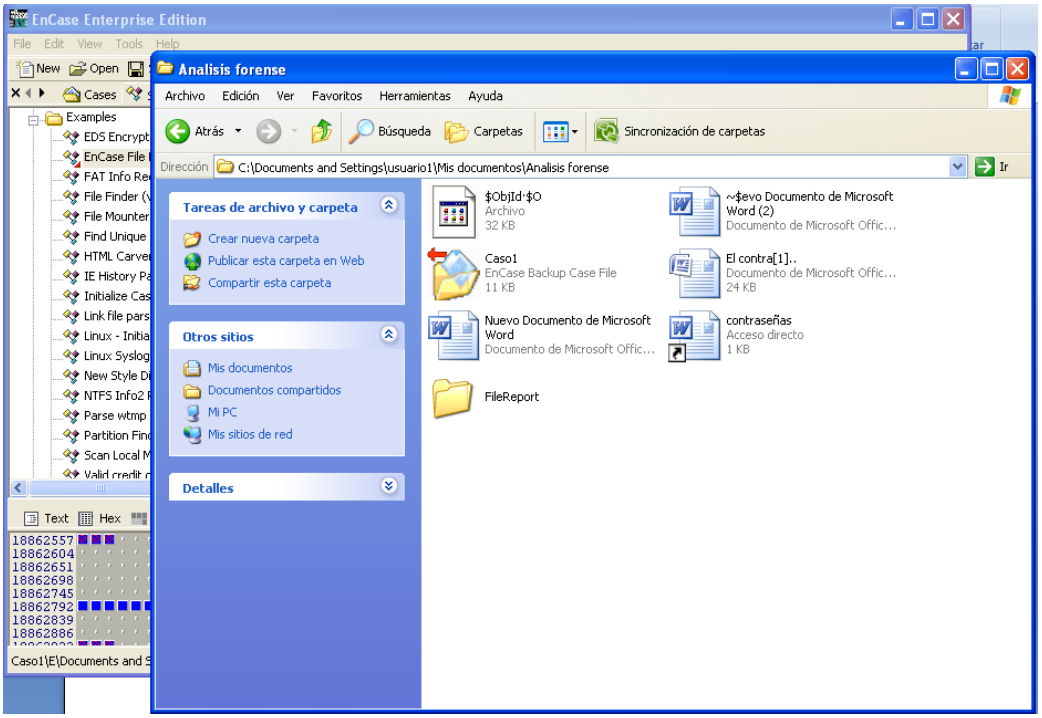


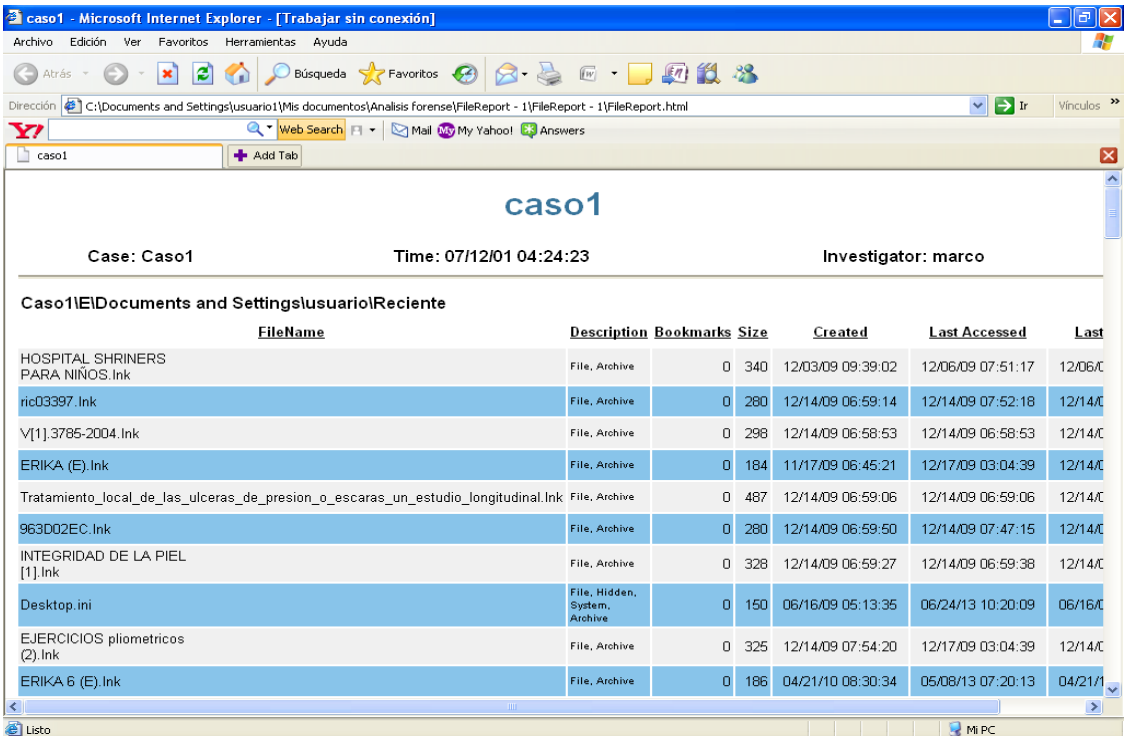

**Ilustración 4.22: Datos para generar el reporte**

Una vez creada habrá que ir a la carpeta en donde estamos guardando todo lo referente al análisis y aparece en la carpeta que dice FileReport




Solo resta dar doble clic en el archivo HTML ubicado dentro de la carpeta y aparecerá lo siguiente en donde nos mostrará:

- Caso
- Fecha del análisis
- Investigador
- Nombre del archivo
- Descripción del archivo
- Bookmarks
- Tamaño del archivo
- Fecha de creación del archivo
- Ultimo acceso al archivo
- Última modificación del archivo
- Ultima fecha de acceso al archivo




En la Imagen 4.23 se visualiza lo referente al archivo *contraseñas*

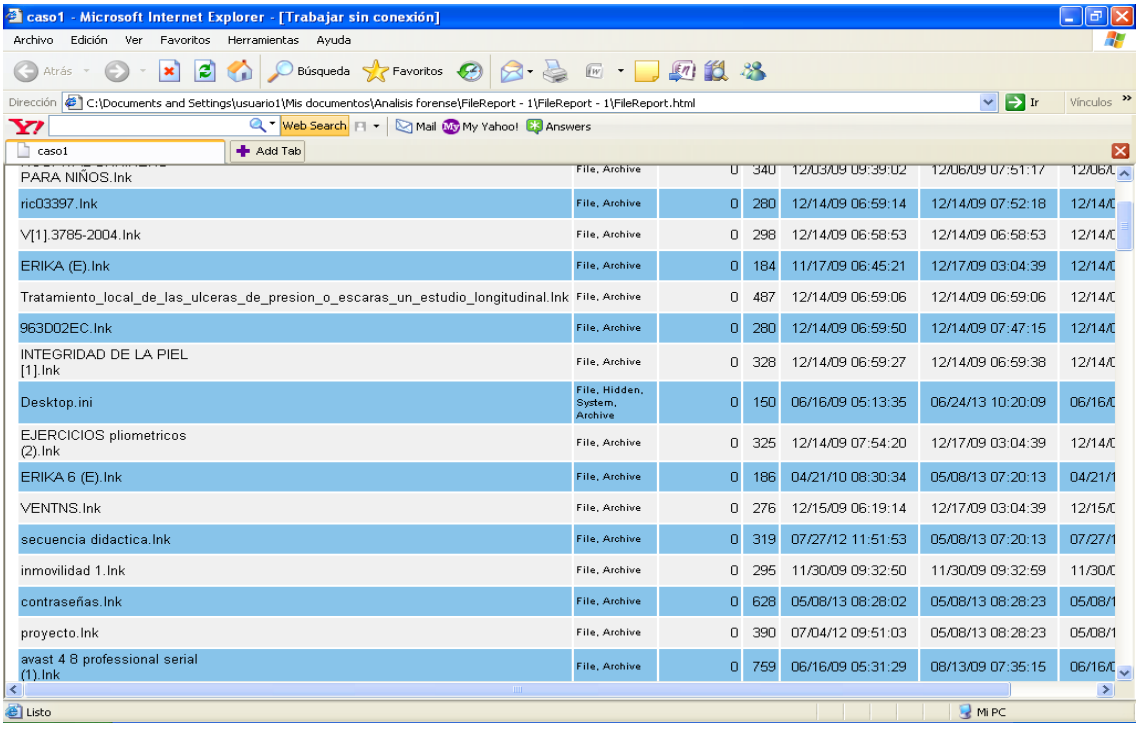



**Ilustración 4.23: Datos correspondientes al archivo *contraseñas***

## Resultados

Una vez que se aplicó el método se obtuvieron los resultados y productos siguientes:

1. Se logró encontrar y recuperar el archivo que fue extraído con anterioridad sin autorización del usuario.(Imagen 5.1 y 5.2)

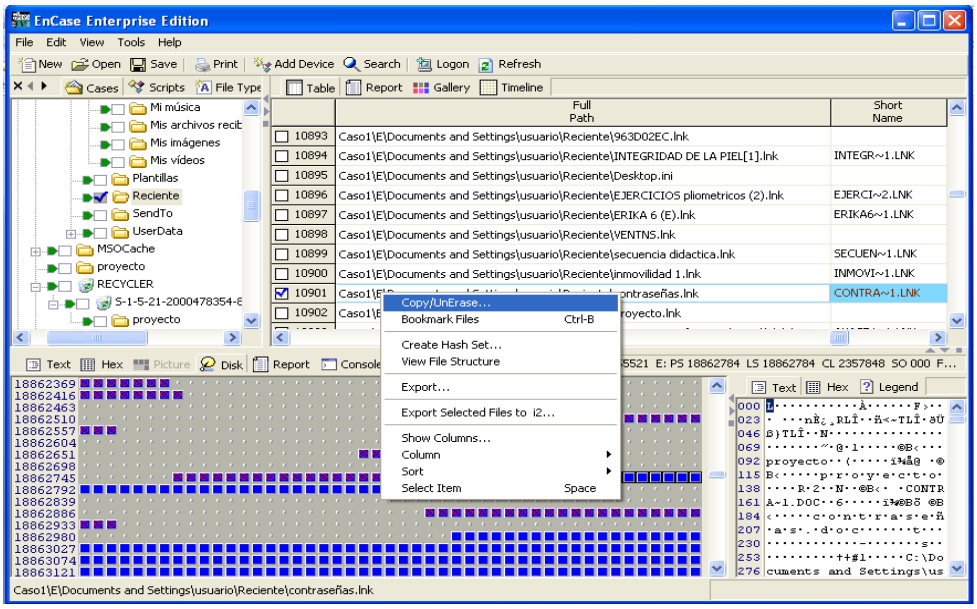



Ilustración 5.1: Archivo “contraseñas” encontrado

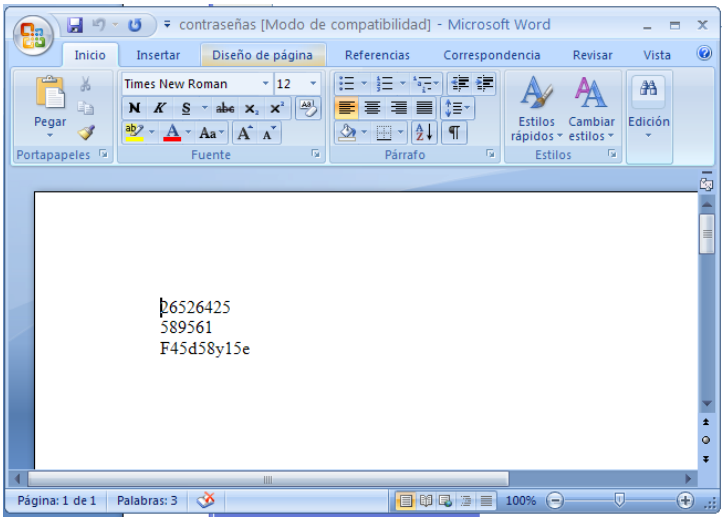



Ilustración 5.2: Archivo encontrado

2. Se aseguró el archivo y se determinó que no sufrió alteraciones.(Imagen 5.3)

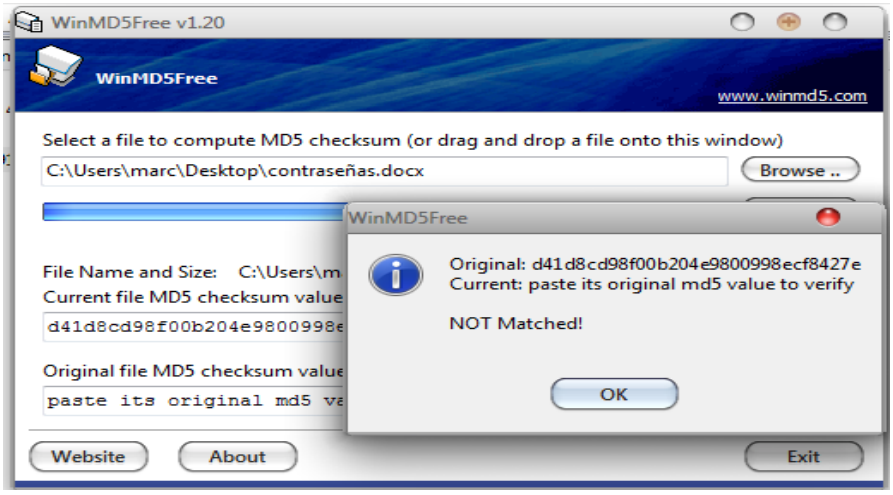
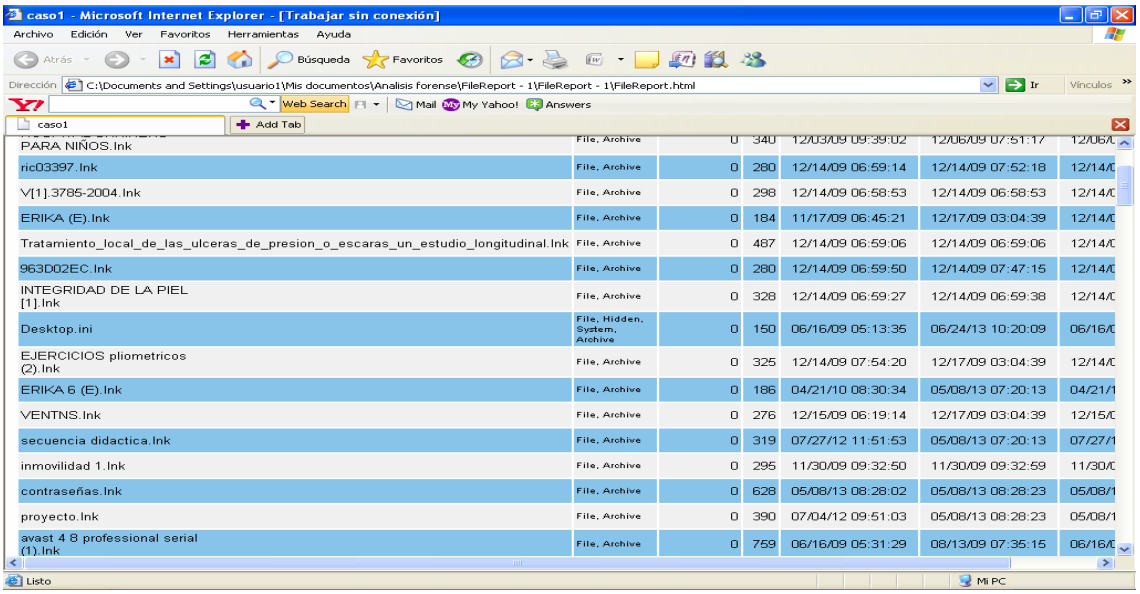



Ilustración 5.3: Determinación de alteraciones en el archivo

3. Se generó un reporte en donde se plasman propiedades que arroja el análisis realizado en EnCase acerca del archivo *contraseñas.*



## Conclusiones

La informática forense sin duda es una técnica que ha ido ganando terreno por sobre otras ramas de la computación ya que la era digital va evolucionando y con esto trágicamente ha ido incrementando la inseguridad en los dispositivos inteligentes. La informática forense es una serie de pasos con los cuales el investigador llega a recabar cierta información que ayuda a encontrar y dar seguimiento a delitos informáticos.

Para investigar el caso de esta investigación se desarrolló el método propuesto por Martínez en la PC del usuario al cual le fue extraído un archivo de suma importancia para mantener integro su equipo de trabajo; fue correctamente llevado a cabo y con esto dio buenos resultados a la hora de recuperar la información eliminada, cumpliendo a su vez con cada uno de los objetivos planteados para el desarrollo de esta investigación, los cuales se fueron desarrollando de forma secuencial y congruente desde tipificar las afectaciones a la información, pasando por el desarrollo del método hasta llegar a concluir el método con resultados satisfactorios.

Entonces en conclusión el objetivo se cumplió ya que se desarrolló correctamente el método propuesto y se logró recuperar la información del usuario afectado comprobando de esta forma si la información recuperada sufrió alteraciones.

## Bibliografía


Abraham Silverschatz, H. F. (2006). *Fundamentos de Bases de Datos.* McGRAW-HILL.

Carrier, B. (15 de noviembre de 2004). *sleuthkit.* Obtenido de www.sleuthkit.org/informer/sleuthkit-informer-17.html

Casey, E. (2002). *Handbook of Computer Crime Investigation.* Elsevier Academis Press 2002.

Janiczek, M. (2004). Principios Basicos de Analisis Forense. En *Hackin9* (págs. 62-79).

Kshetri, N. (2006). *The simple economics of cybercrime.* IEEE Security & Privacy.

Lopez Calvo, P., & Gómez Silva, P. (2003). *Investigacion criminal y criminalistica.* Temis.

Luzinski, & Kida J, T. (s.f.). *Managing your Evidence yourEvidence Problems associated with proper collection procedures.* Obtenido de www.paladintek.com/WhitePaper/Managing_Your_evidence.pdf

Martínez, J. J. (2009). *Computación Forense.Descubriendo los rastros informáticos.* México: Alfaomega Grupo Editor.

MCKemmish, R. (1999). *What is forensic computing?Australian Institute of Criminology.* Issues and Trends in crime and criminal justice.

Morris, J. (11 de febrero de 2003). Forensics on de Windows Platform Part Two. (www.securityfocus.com/infocus/1661, Ed.)

Osterburg, J., & Ward, R. (2000). *Criminal Investigation.* Anderson Publishing.

Reith, M. C., & C. Gunsh G. (s.f.). *An examination of Digital Forensic Models.* Obtenido de www.ijde.org/archives/02_fall_art2.html.Symantec

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet.* Pearson-Prentice Hall.

Soria, M. (2006). *La psicologia de invetsigación criminal: perfiles psicologicos criminales y hallazgos criminológicos forense.* En Soria, M y Sáiz,D.

Sundt, C. (2006). *Information security and the law.* Information Security Technical Report.

Vieites, Á. G. (2007). *Enciclopedia de la Seguridad Informática.* México: Alfaomega Grupo Editor.

Walden, I. (2007). *Computer crimes and digital investigations.* Oxford Press.