UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

“EVOLUCIÒN Y DESARROLLO DE LA INFORMÁTICA FORENSE.”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

PRESENTA:

MARLENE DEL CARMEN FRANCISCO MORA

ASESOR DE TESIS:
M. A. RAÚL DE JESÚS OCAMPO COLÍN

Coatzacoalcos, Veracruz **Enero 2011.**

Índice

Portada

Dedicatoria

Titulo

Problema…….....1

Hipótesis……..4

Objetivo General y Objetivo Especifico……..5

Justificación…….....6

Introducción…….....8

Capítulo I Introducción a la Informática Forense

1.1. Introducción a la Informática Forense……11
1.2. Definiciones…….....12
1.3. Evidencia digital…….....14
1.4. Procedimientos……15
1.4.1. Esterilidad de los medios de informáticos de trabajo……16
1.4.2. Verificación de las copias en medios informáticos……..16
1.4.3. Documentación de los procedimientos, herramientas y resultados……..16
sobre los medios informáticos analizados
1.4.4. Mantenimiento de la cadena de custodia de las evidencias digitales……..17
1.4.5. Informe y presentación de resultados de los análisis de los……17
medios informáticos
1.4.6. Administración del caso realizado……..18
1.4.7. Auditoría de los procedimientos realizados en la investigación……18
1.5. Herramientas……19
1.6. Retos……19
1.6.1. El reconocimiento de la evidencia digital como evidencia formal y válida…20
1.6.2. Los mecanismos y estrategias de validación y confiabilidad de las……...20
herramientas forenses en informática
1.6.3. La formación de especialistas en informática forense……..21

Capítulo II Informática Forense

2.1. Antecedentes de la Informática Forense…….....24
2.2. Causas y origen de la auditoria forense……...27
2.3. ¿Qué es la Informática Forense?.....28
2.4. Importancia de la Informática Forense…….28
2.4.1 Objetivos de la Informática Forense……...29
2.4.2 Usos de la Informática Forense……29
2.5. La Investigación Tecnológica……30
2.5.1. Evidencia Digital……30
2.5.2. Grabación en Medios Magnéticos: Principios Físicos……32
2.5.2.1.Escribiendo Datos Magnéticos……33
2.5.2.2.Leyendo Datos Magnéticos……..36
2.5.3. Análisis de Discos……37
2.5.3.1. File Slack……38
2.5.3.2. Archivo Swap de Windows……..39
2.5.3.3. Unallocated File Space……40
2.6. Eliminación de datos……40
2.6.1. Eliminación de Datos en un Medio Magnético……40
2.6.1.1 Degaussing de Medios Magnéticos……41
2.6.2 Eliminación de Datos en CDs……43
2.7. Pasos para la Recolección de Evidencia……44
2.7.1 Hardware……44
2.7.2 Cuidados en la Recolección de Evidencia……45
2.8. Herramientas de Investigación Forense……..45
2.8.1 Herramientas para la Recolección de Evidencia……45
2.8.1.1 EnCase……..46
2.8.2. Herramientas para el Monitoreo y/o Control de Computadores……..50
2.8.2.1. KeyLogger……..50
2.8.3. Herramientas de Marcado de documentos……51
2.8.4 Herramientas de Hardware……51
2.9. Dificultades del Investigador Forense……51

Capítulo III EnCase Forensic

3.1. Que es Encasé Forensic……54
3.2. Cómo funciona EnCase® Forensic……...55
3.3. Requisitos del sistema para EnCase® Forensic……56
3.4. El Estándar en Computación Forense……..56
3.5. Alto rendimiento de procesamiento y confiabilidad……57
3.6. Adquisiciones forenses confiables……57
3.7. Flexibilidad extrema: EnScript……57
3.8. Características de EnCase Edición Forense……...58
3.8.1. Múltiple administración de casos……58
3.9. Soporte Unicode……...58
3.10. Configuración dinámica de discos……..58
3.11. Búsqueda y análisis: palabras claves, búsqueda de hash y firmas, y filtros…58
3.12. Opciones de adquisición múltiple……59
3.13. Sistemas de archivos (file systems) interpretados por EnCase……59
3.14. Soporte para correo electrónico PST……59
3.14.1. Visor de galería……...59
3.14.2. Visor de escala de tiempo……59
3.14.3. Visor de reportes……60
3.15. EnCase módulo del sistema de archivos de cifrado……60
(Encrypting File System . EFS)

3.15.1. EnCase módulo del sistema de archivos virtuales……60
(Virtual File System . VFS)
3.15.2. Módulo del servidor de autenticación en red……60
(Network Authentication Server . NAS)
3.16. Acerca de Guidance Software……61
3.17. Acerca de Internet Solutions……61
3.18. Capturas de Pantalla……61
3.18.1. EnCase® Forensic Screenshots……..61
3.18.2. The EnCase Forensic GUI……62
Conclusión……68
Glosario……..70
Bibliografía……....75
Anexos…….. 80

Índice de Tablas y Figuras

Capítulo I Introducción a la Informática Forense

Figura 1.4.6. Administración del caso realizado……..18
Figura 1.6.1. El reconocimiento de la evidencia digital como evidencia……20
formal y válida
Figura 1.6.3. La formación de especialistas en informática forense……22

Capítulo II Informática Forense

Figura 2.5.2.1. Escribiendo Datos Magnéticos……33
Figura 2.5.2.1.1. Escribiendo datos en un medio de almacenamiento……35
Figura 2.5.2.2. Leyendo datos magnéticos……37

Capítulo III EnCase Forensic

Figura 3.1. Que es Encasé Forensic……55
Figura 3.2. Cómo funciona EnCase® Forensic……..55
Figura 3.18.1. EnCase® Forensic Screenshots……61
Figura 3.18.2. The EnCase Forensic GUI……62
Figura 3.18.2.1. The EnCase Forensic GUI……62
Figura 3.18.2.2. The EnCase Forensic GUI……62
Figura 3.18.2.3. The EnCase Forensic GUI……63
Figura 3.18.2.4. The EnCase Forensic GUI……63
Figura 3.18.2.5. The EnCase Forensic GUI……64
Figura 3.18.2.6. The EnCase Forensic GUI……64
Figura 3.18.2.7. The EnCase Forensic GUI……64
Figura 3.18.2.8. The EnCase Forensic GUI……65
Figura 3.18.2.9. The EnCase Forensic GUI……65
Figura 3.18.2.10. The EnCase Forensic GUI……..66
Figura 3.18.2.11. The EnCase Forensic GUI……..66
Figura 3.18.2.12. The EnCase Forensic GUI……..67
Figura 3.18.2.13. The EnCase Forensic GUI……..67

Dedicatoria

A mi padre: Guillermo Francisco Ruiz
A quien le debo todo en la vida, le agradezco el cariño, comprensión, paciencia, los ejemplos de perseverancia y constancia, por haberme infundado siempre el valor de salir adelante y por el apoyo brindado para culminar mi carrera profesional.
¡Toda mi admiración, cariño y respeto para ti papá!

A mi Madre: Maria Cristina Mora Macias
Por haberme apoyado en todo momento, por tus consejos, los valores que me inculcaste, por la motivación constante que me ha permitido ser una persona de bien, pero sobre todo, por tu amor y por la confianza que depositaste en mí.
¡Gracias mamá te quiero mucho!

A quienes me han heredado el tesoro más valioso que puede dársele a un hijo: Amor. A quienes sin escatimar esfuerzo alguno, han sacrificado gran parte de su vida para formarme y educarme.
A quienes la ilusión de su vida ha sido convertirme en persona de provecho. A quienes nunca podré pagar todos sus desvelos ni aun con las riquezas mas grandes del mundo.

Por esto y más… gracias.

A mis hermanos y sobrinos: Magui, Mauro, Pati, Tere, Luis y Xiadani. Yuridi y Eduardo.
Por que siempre he contado con ustedes de distintas formas, gracias a la confianza que siempre nos hemos tenido; por el cariño y apoyo constante durante todo este tiempo, ya que esta etapa de mi vida ha sido muy importante y su apoyo ha sido igual de valioso. ¡Gracias! Los quiero mucho.

A Dios Porque hiciste realidad este sueño, me diste salud y fortaleza para lograr mis objetivos, por tu infinita bondad y amor con el que me rodeas y porque me tienes en tus manos.

"Poned el mayor empeño en añadir a vuestra fe la virtud, a la virtud el conocimiento, al conocimiento la templanza, a la templanza la tenacidad, a la tenacidad la piedad, a la piedad el amor fraterno, al amor fraterno la caridad." (2Pedro, 1:5-6-7)

A todos mis profesores
No solo a los de la carrera sino de toda la vida, mil gracias porque de alguna manera forman parte de lo que ahora soy….
Por la paciencia, disposición y el apoyo que cada uno me brindo en todo momento, por los consejos que cada día fueron haciéndome una persona dedicada y responsable.

¡Mil gracias!

Titulo

Evolución y Desarrollo de la Informática Forense

Problema

Brindar los conocimientos necesarios para desarrollar las competencias para la identificación, las modalidades delictivas y un correcto manejo de la escena y la evidencia física o digital, para que pueda ser admitida posteriormente como evidencia válida, y las posibilidades que actualmente ofrece la tecnología forense.

En la actualidad se invierte una cantidad considerable de capital, tiempo y esfuerzo en el procesamiento, recolección y distribución de información. La computadora y los sistemas informáticos, en general, son piezas fundamentales de la sociedad moderna para el manejo de la información y son, por lo tanto, herramientas que favorecen el progreso de la organización, escuela o casa.

Desafortunadamente, estas mismas herramientas tecnológicas que han conquistado a la sociedad moderna están siendo explotadas por personas que tienen como fin cometer agravios en contra de organizaciones o propiedades.

Así como el ser humano se ha dedicado gradualmente a fabricar bienes, ahora se está enfocando a trabajar más en el procesamiento de la información, así también las actividades de sustracción han pasado de una dimensión física, en la cual las investigaciones están descritas en términos tangibles, a una dimensión electrónica, en la cual la evidencia sólo existe digitalmente, y las investigaciones son conducidas a través de Internet.

En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios.

Las organizaciones dependen en su totalidad de tener la Información exacta en el momento preciso, las compañías que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años, la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y lista para ser utilizada.

Sin embargo, la mayoría de las organizaciones han fallado al no aprovechar el ambiente existente e implementar ideas innovadoras para mejorar el papel que juegan los sistemas de información dentro de sus organizaciones.

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

Por exceso de confianza en su personal o sus programas de seguridad, las empresas enfrentan el robo de información o daños a equipos.
Los empresarios creen que nada le pasará a la información de su red, hasta que un día, los crackers (*persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño.*) o trabajadores de la empresa penetran a sus archivos extrayendo información contable, administrativa, de estudios de mercado, de proyectos, así como dinero de sus cuentas bancarias y otra información que es relativa a la empresa.

En la actualidad el valor de la información en nuestra sociedad, y sobre todo en las empresas, es cada vez más importante para el desarrollo de negocios de cualquier organización.

La informática forense provee el conocimiento y los instrumentos para estudiar y solucionar este nuevo tipo de transgresiones.

Así pues, en la informática forense se busca la respuesta a cuestiones que se refieren al método, intento, medios, culpabilidad, motivo y pérdidas resultantes de un ataque informático.

Conociendo la situación problemática en la que se encuentran las empresas y/o sociedad estamos consientes de que los avances tecnológicos plantean nuevos desafíos en diversos campos y materia.

Estos adelantos pueden llevarnos a soluciones más avanzadas, también pueden volverse en contra y dar más facilidades a aquellas personas que se dedican sustraer información ya sea con fines de lucro o solamente para ocasionar algún daño.

Esta problemática es la que origina que se lleve a cabo esta investigación para proponer soluciones a las empresas y obtengan resultados positivos al proteger su información, así mismo puedan tener la confianza que se realizaran las acciones técnicas necesarias para impedir que dichas amenazas afecten cualquiera de los recursos organizacionales que se encuentren en riesgo ya que esto significa una inversión muchas veces alta y que mejorará su competitividad en el mercado.

Hipótesis

Evolución de la forma en como se ha venido llevando la investigación de la Informática Forense, y como proponen desarrollar una metodología específica de Inspección Ocular Informática Forense, que incluya el Fundamento científico, Marco Legal, Estructura Informática General (Análisis de Sistemas), Estructura Criminalística General (Inspección Ocular Criminalística), Estructura Informática Particular (Herramientas y Métodos de Análisis Informático Forenses específicos), Como elemento integrador el accionar mancomunado con otros peritos y una clara estructura lógica de investigación aplicada al hecho particular *sub peritia.*

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

Objetivo General

- Brindar los conocimientos necesarios para desarrollar las competencias para la identificación y correcta tipificación de ciberdelitos, modalidades delictivas y un correcto manejo de la escena y la evidencia física o digital, para que pueda ser admitida posteriormente como evidencia válida, basados en la legislación nacional e internacional y las posibilidades que actualmente ofrece la tecnología forense.

Objetivo Específico

- Describir las distintas causas que dieran Origen a la Auditoría Forense.
- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.
- Desarrollar habilidades a partir del conocimiento de las posibilidades que brinda la informática forense en la actualidad para la adquisición, análisis, valoración y preservación de la evidencia.

Justificación

Conociendo la necesidad de las empresas de protegerse contra las amenazas de la inseguridad informática, es cada vez más necesario la implementación de técnicas y la utilización de herramientas destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Este estudio se enfoca en la importancia de la informática forense para la seguridad de las empresas, con el fin de mostrar la vulnerabilidad que tienen las organizaciones de amenazas informáticas debido a la existencia de personas ajenas a la información, también conocidas como piratas informáticos o crackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Además de mostrar algunas herramientas tecnológicas que podría adquirir una empresa para la protección de sus datos e información confidencial.

En delitos como el fraude informático o falsificación electrónica, los medios de prueba generalmente son de carácter material o documental, esto en razón de que esta clase de infracciones son del tipo ocupacional. Esto significa que la persona o personas que cometen esta variedad de actos en un noventa por ciento trabajan dentro de la organizaciones afectadas; en consecuencia la prueba de estos delitos se encuentra generalmente en los equipos y programas informáticos, en los documentos electrónicos y en los demás mensajes de datos que utilizan e intercambian estas personas en la red de trabajo.
Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de pesos.

Los conocimientos y habilidades requeridos para la práctica de la investigación digital forense hacen que los recursos humanos sean escasos y esto, ante la gran cantidad de incidentes de seguridad ocurridos. Es por esto que es importante la utilización de las herramientas que provee la informática forense y así se pueda, con este conocimiento, concluir resultados que ayuden al investigador a discernir rápidamente las causas del ataque, con base en el realce de evidencia relevante, sin tener que realizar el análisis completo y exhaustivo a través de procesos manuales.

En el aspecto teórico-metodológico se considera indispensable el dominio teórico para que exista una práctica consciente y estimulante, que promueva un cambio profundo en la manera de percibir y practicar la seguridad dentro de las empresas, por lo general la mayoría de usuarios particulares y de empresas poseen la percepción de que la seguridad de la información es una tarea difícil de aplicar, que exige gran cantidad de dinero y de tiempo.
En realidad, con muy poco esfuerzo se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad de particulares y de pequeñas y medianas empresas y de la cual se pueden obtener grandes beneficios, como es la protección de su información.

En el orden práctico implica la introducción de una nueva manera de conocer cómo se puede asegurar la información, mediante una serie de técnicas que aplicadas debidamente permitirán a las empresa manejar de una forma óptima sus archivos que se generan en el proceso de sus actividades, así de esta manera también hacer una cultura en los usuarios en la forma que implementan las herramientas o procedimientos para resguardar su información y que están sean ejecutadas confidencialmente de tal forma que mantengan su integridad y disponibilidad.

Introducción

En la nueva era de la información y la tecnología es necesario que las empresas que utilizan Internet como recurso principal para realizar sus operaciones cuenten con un sistema de seguridad de alta calidad. Esto se debe tomar para evitar ataques de delincuentes cibernéticos, que quieran usurpar archivos confidenciales o bien detener por completo los sistemas de la organización dañando el software o el hardware de la misma.

Estas y otras muchas amenazas forman parte de los peligros a los que se ven expuestas las empresas, no solo por parte de personas ajenas a la institución, sino que hasta los mismos trabajadores de la empresa.

La información es el activo más valioso que poseemos en la sociedad actual. Ésta es cada vez más importante para el desarrollo de las empresas y de negocios exitosos a través de la implementación de sistemas de información.

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos. Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos de 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 hacia 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 para 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.
Para proteger la información surge una nueva ciencia, la Informática Forense; ésta persigue objetivos preventivos así como reactivos, una vez que se ha dado una infiltración en el sistema.

La informática forense se ocupa de la investigación de acontecimientos sospechosos relacionados con sistemas informáticos, el esclarecimiento de situaciones creadas y sus autores, a través de la identificación, preservación, análisis y presentación de evidencias digitales.

La finalidad de esta investigación es brindar una perspectiva más amplia acerca de la informática forense a fin de sentar las bases de la investigación científica en esta materia, resaltando en primer lugar su importancia, sus objetivos y su finalidad, así mismo las diversas herramientas y técnicas que utiliza.

De esta forma, la informática forense constituye una herramienta gerencial que asiste a cualquier tipo de investigación relacionada con las más diversas irregularidades que puedan presentarse en una empresa: desde un simple hurto hasta la malversación de fondos, el tráfico de datos o la competencia desleal.

El Primer Capítulo corresponde a la Introducción de la Informática Forense, su definición, una introducción y los métodos para la evidencia digital, en el Segundo Capitulo es la Informática Forense aquí se da a conocer a grandes términos el enfoque de la tesis, con ellos se da a conocer en el Capitulo Tres se habla de Encasé Forensic un programa para detectar este tipo de situación como el robo o el extravió de información aquí se da a conocer los métodos y requerimientos que se necesitaran en la Informática Forense.

Capítulo I. Introducción a la Informática Forense

Capitulo I Introducción a la Informática Forense

1.1. Introducción a la Informática Forense

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos.

Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos de 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 hacia 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 para 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.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garantía de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En consecuencia, este breve documento busca ofrecer un panorama general de esta especialidad técnicolegal, para ilustrar a los lectores sobre los fundamentos generales y bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, unos nuevos científicos que a través de la formalidad de los procesos y la precisión de la técnica buscan decirle a los intrusos informáticos que están preparados para confrontarlos y procesarlos.

1.2. Definiciones

Existen múltiples definiciones a la fecha sobre el tema forense en informática. 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.

Es importante anotar, que al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asumen dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen como son: identificación, preservación, extracción, análisis, interpretación, 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 e

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, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los 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, que en equipos particulares, es poco frecuente.

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 en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) 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 convergen en todos los casos hacia la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de evidencia digital para detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado. No obstante lo anterior, es pertinente

anotar 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.

1.3. Evidencia digital

La evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".
En este sentido el documento mencionado establece que la evidencia digital puede ser dividida en tres categorías a saber:
1. Registros almacenados en el equipo de tecnología informática (P.e. correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.)
2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (Hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).
La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno.
La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

1. Es volátil
2. Es anónima
3. Es duplicable
4. Es alterable y modificable

5. Es eliminable

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

Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

1.4. Procedimientos

Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso bien sea legal u organizacional. En este sentido, detallamos de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado:

1.4.1. Esterilidad de los medios de informáticos de trabajo

Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, sin pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

1.4.2. Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia.

Adicionalmente, es preciso que el software u aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad científica, para que conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

1.4.3. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos.

Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

1.4.4. Mantenimiento de la cadena de custodia de las evidencias digitales

Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar

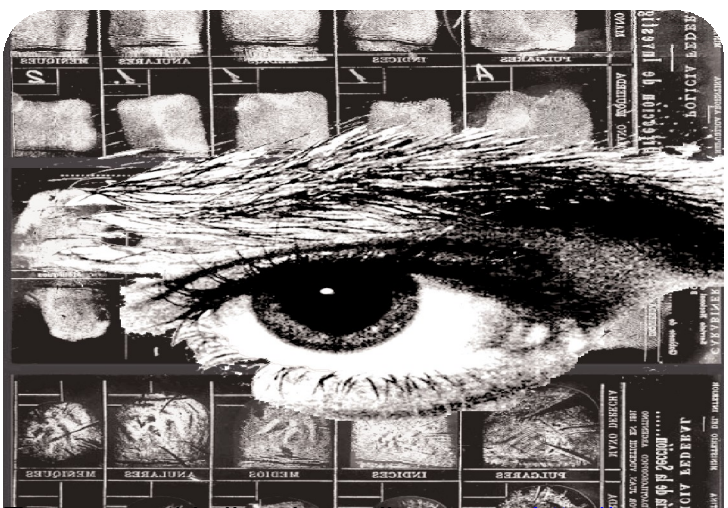
claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

1.4.5. Informe y presentación de resultados de los análisis de los medios informáticos

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

1.4.6. Administración del caso realizado

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



1.4.7. Auditoría de los procedimientos realizados en la investigación

Finalmente y no menos importante, es recomendable que el profesional investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.

1.5. Herramientas

Hablar de informática forense sin revisar algunas ideas sobre herramientas es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general de los lectores, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática.

1.6. Retos

La informática forense es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la

conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o fraudes en las organizaciones.

En este sentido, se tienen agendas de investigación a corto y mediano plazo para que se avancen en temas de especial interés en la conformación y fortalecimiento de las ciencias forenses aplicadas a los medios informáticos. Dentro de los temas seleccionados están:

1.6.1. El reconocimiento de la evidencia digital como evidencia formal y válida

La evidencia digital en la administración de justicia en muchas partes del mundo continua siendo una situación problemática por resolver. Dada las características mencionadas previamente, se hace un elemento que requiere un tratamiento especial, más allá de las características legales requeridas, pues éstas deben estar articuladas con los esfuerzos de seguridad de la información vigentes en las organizaciones.

Figura 1.6.1. El rec idencia formal y válida

1.6.2. Los meca y confiabilidad de las herramientas fo

Las herramientas utilizadas actualmente en investigaciones forenses en informática están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos. Sin embargo, la fragilidad inherente del software, la vulnerabilidad presentes en las mismas y las limitaciones propias de los lenguajes y prácticas de programación hacen que la comunidad

académica y científica redoble sus esfuerzos para hacer de estos programas, herramientas más confiables y predecibles para los cuerpos de investigaciones judiciales y organizacionales.

1.6.3. La formación de especialistas en informática forense

La formación de especialistas en informática forense que apoyen labores de peritaje informático tanto en la administración de justicia como en investigaciones organizacionales internas.

Al ser la informática forense una ciencia aplicada naciente, se hace necesario iniciar las reflexiones sobre la formación de un especialista en informática forense.

Esta formación necesariamente deberá ser interdisciplinaria y para ello se requiere el concurso de los profesionales del derecho, la criminalística, las tecnologías de información y la seguridad informática, como mínimo, sin perjuicio de que otras disciplinas académicas puedan estar presentes en la estrategia de profesionalización de estos nuevos especialistas.

A lo largo de este documento hemos querido mostrar de manera básica y concreta una aproximación a la informática forense, no con el ánimo de sugerir un curso de acción sobre el tema, sino de ilustrar los diferentes escenarios y elementos que componen esta naciente disciplina auxiliar de la criminalística.

Es preciso aclarar, que los conceptos expresados responden a una revisión de la práctica internacional sobre el tema y que el análisis para el caso requiere aún un estudio particular.

La informática forense es la respuesta natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos) con el fin de enviar un mensaje claro a los intrusos: estamos preparados para responder a sus acciones y continuamos aprendiendo para dar con la verdad de sus acciones.

Figura 1.6.3. La formación de especialistas en informática forense

Capítulo II. Informática Forense

Capítulo II. Informática Forense

2.1. Antecedentes de la Informática Forense

A través de la historia se han realizado distintos tipos de auditoría, tanto al comercio como a las finanzas de los gobiernos. El significado del auditor fue persona que oye, y fue apropiado en la época durante la cual los registros de contabilidad gubernamental eran aprobados solamente después de la lectura pública en la cual las cuentas eran leídas en voz alta. Desde tiempos medievales, y durante la revolución Industrial, se realizaban auditorías para determinar si las personas en posiciones de responsabilidad oficial en el gobierno y en el comercio estaban actuando y presentado información de forma honesta.

Durante la Revolución Industrial a medida que el tamaño de las empresas aumentaba sus propietarios empezaron a utilizar servicios de gerentes contratados. Con la separación de propiedad y gerencia, los ausentes propietarios acudieron a los auditores para detectar errores operativos y posibles fraudes. Los bancos fueron los principales usuarios externos de los informes financieros. Antes del 1900 la auditoría tenía como objetivo principal detectar errores y fraudes, con frecuencia incluían el estudio de todas o casi todas las transacciones registradas.

A mediados del siglo XX, el enfoque del trabajo de auditoría tendió a alejarse de la detección de fraude y se dirigió hacia la determinación de si los estados financieros presentaban razonablemente la posición financiera y los resultados de las operaciones. A medida que las entidades corporativas se expandían los auditores comenzaron a trabajar sobre la base de muestras de transacciones seleccionadas y en adición tomaron conciencia de la efectividad del control interno.

La profesión reconoció que las auditorías para descubrir fraudes serían muy costosas, por estos el control interno fue reconocido como mejor técnica.

A partir de la década de los 60s en Estados Unidos la detección de fraudes asumió un papel más importante en el proceso de auditoría.

Este desplazamiento en la detección de fraude fue el resultado de: un incremento del Congreso para asumir una mayor responsabilidad por los fraudes en gran escala, una diversidad de procesos judiciales exitosos que reclamaban que los informes financieros fraudulentos habían quedado inapropiadamente sin detección por parte de los auditores independientes y la convicción por parte de los contadores públicos de que debería esperarse de las auditorías la detección de fraude material.

En 1996 la Junta de Normas de Auditoría, emitió una guía para los auditores requiriendo una evaluación explícita del riesgo de errores en los estados financieros en todas las auditorías, debido al fraude. El uso de sistemas de computación no ha alterado la responsabilidad del auditor en la detección de errores y fraude. El Congreso y los reguladores estaban convencidos de que la clave para evitar problemas era la reglamentación de leyes efectivas y las exigencias por parte de los auditores, en el cumplimiento de las provisiones de esas leyes y regulaciones.

Como consecuencia de diversos actos fraudulentos las principales organizaciones de contabilidad patrocinaron la Comisión Nacional sobre Presentación de informes Financiero Fraudulentos, muchas de las recomendaciones a los auditores fueron reglamentadas por la Junta de Normas y Auditoría, una de la más importante fueron sobre la efectividad del control interno y la demanda de la atestación de los auditores.

En estos tiempos de cambios en el mundo, la sociedad y la empresa, la auditoría ha evolucionado para adaptarse a estos nuevos procesos y enfrentar las grandes transformaciones en los diferentes ambientes, como son las iniciativas de fusiones, cambios tecnológicos, lanzamientos de nuevos productos, definición de nuevos servicios, entre otros.

Dentro de esta evolución la auditoría se ha especializado para ofrecer nuevos modelos de auditorías, entre estos encontramos la Forense que surge como un nuevo apoyo técnico a la auditoría gubernamental, debido al incremento de la

corrupción en este sector. Esta auditoría puede ser utilizada tanto, el sector público como en el privado.

Los distintos tipos de auditorías son importantes porque proveen confiabilidad en la información financiera lo que permite a las entidades la asignación de forma eficiente de los recursos, la contribución del auditor es proporcionar credibilidad a la información, para los Accionistas, Acreedores, Clientes Reguladores Gubernamentales entre otros.

Con frecuencia se considera que las auditorías se clasifican en tres grandes categorías: Auditoría de Estado Financieros, Auditorías de Cumplimiento y Auditorías Operacionales. A continuación las auditorías utilizadas en la actualidad.

- Auditorías Gubernamental
- Auditorías de Estados Financieros
- Auditorías de Cumplimiento
- Auditorías de Gestión y Operacionales
- Auditorías Internas
- Auditorías Especiales
- Auditorías de Control Interno

2.2. Causas y origen de la auditoria forense

La corrupción es una de las principales causas del deterioro del Patrimonio Público. La auditoría forense es una herramienta para combatir este flagelo. La auditoría forense es una alternativa porque permite que un experto emita ante los jueces conceptos y opiniones de valor técnico, que le permiten a la justicia actuar con mayor certeza, especialmente en lo relativo a la vigilancia de la gestión fiscal.

Queremos presentar el modelo de la Auditoría Forense, sus características y su importancia como modelo de control y de investigación gubernamental, con el fin de tener una nueva herramienta que ayude a detectar y combatir los delitos cometidos contra los bienes del Estado por parte de empleados públicos

deshonestos o patrocinadores externos, de esta manera contribuimos, a mejorar las economías de nuestros países y por tanto el bienestar de todos nuestro pueblos hermanos.

El perito o sujeto investigador debe ser elegido como un elemento imparcial, debe ser competente, se requiere de un experto para exponerle a un juez percepciones ordinarias que efectúe sobre determinados hechos, sino de emitir conceptos de valor técnico.

El propósito fundamental de la auditoría gubernamental no es detectar fraude, sino más bien prevenirlos, porque es la responsabilidad propia de la administración de la entidad pública.

Debe tenerse en cuenta que la naturaleza y alcance de la auditoría del sector público pueden verse afectados por la legislación, reglamento, ordenanzas y disposiciones ministeriales deben estar relacionadas con la detección de fraude. Estos requerimientos pueden afectar la capacidad de la auditoría para aplicar su criterio.

Además de las responsabilidades formalmente asignadas respecto a la detección de fraude, el uso de fondos públicos tiene a imponer un nivel superior a los temas de fraudes y el auditor puede verse requerido a responder a las expectativas del público con respecto a la detección de fraudes.
El auditor debe diseñar acciones de manera que ofrezca garantía razonable de que se detecten errores, irregularidades o actos ilícitos que pudiera repercutir substancialmente sobre los valores que figuran los estados financieros. La auditoría financiera constituye un aspecto esencial de la fiscalización pública ya que persigue velar por la integridad y validez de las cuentas y el presupuesto, del mismo modo las auditorías de gestión se plantea el manejo de los recursos públicos de la conformidad de las leyes y reglamentos vigentes.

2.3. ¿Qué es la Informática Forense?

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.
Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

2.4. Importancia de la Informática Forense

"High-tech crime is one of the most important priorities of the Department of Justice". Con esta frase podemos ver cómo a poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes.
Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática. Sin embargo, la importancia real de la informática forense proviene de sus objetivos.

2.4.1 Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:
1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

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

2.4.2 Usos de la Informática Forense

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

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

2.5. La Investigación Tecnológica

Los investigadores de la computación forense usan gran cantidad de técnicas para descubrir evidencia, incluyendo herramientas de software que automatizan y aceleran el análisis computacional.

2.5.1. Evidencia Digital

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

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo *checksums* o *hash* MD5.
La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además definen que los principios desarrollados para la recuperación estandarizada de evidencia computarizada se deben gobernar por los siguientes atributos:

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

2.5.2. Grabación en Medios Magnéticos: Principios Físicos

En general, los medios de almacenamiento magnético se basan directamente en cuatro fenómenos físicos:

A. Una corriente eléctrica produce un campo magnético
B. Algunos materiales se magnetizan con facilidad cuando son expuestos a un campo magnético débil. Cuando el campo se apaga, el material de desmagnetiza rápidamente. Se conocen como *Materiales Magnéticos Suaves*.
C. En algunos materiales magnéticos suaves, la resistencia eléctrica cambia cuando el material es magnetizado. La resistencia regresa a su valor original cuando el campo magnetizante es apagado.
Esto se llama Magneto-Resistencia, o efecto MR. La Magneto-Resistencia Gigante, o efecto GMR, es mucho mayor que el efecto MR y se encuentra en sistemas específicos de materiales de películas delgadas.
D. Otros materiales se magnetizan con dificultad (es decir, requieren de un campo magnético fuerte), pero una vez se magnetizan, mantienen su magnetización cuando el campo se apaga. Se llaman *Materiales Magnéticos Duros*, o *Magnetos Permanentes*.

Estos cuatro fenómenos son explotados por los fabricantes de cabezas grabadoras magnéticas, que leen y escriben datos, para almacenar y recuperar datos en unidades de disco, de cinta y otros dispositivos de almacenamiento magnético.

Aplicaciones en almacenamiento de datos:

• **Cabezas de Escritura:** Cabezas usadas para escribir bits de información en un disco magnético giratorio, dependen de los fenómenos A y B para producir y controlar campos magnéticos fuertes.

• **Cabezas de lectura:** Éstas dependen de los fenómenos A, B y C y son sensibles a los campos magnéticos residuales de los medios de almacenamiento magnetizados (D).

• **Medios de Almacenamiento:** (Como discos de computador) Los medios de almacenamiento magnético son magnetizados de manera permanente en una dirección (Norte o Sur) determinada por el campo de escritura. Estos medios explotan el fenómeno D.

2.5.2.1. Escribiendo Datos Magnéticos

La vista superior de una cabeza de escritura (izquierda) muestra un rollo espiral, envuelto entre dos capas de material magnético suave; a la derecha está un corte transversal de esta cabeza, vista de lado. En el extremo inferior, hay un espacio entre las capas, y en el extremo superior, las capas están unidas.

Las capas superior e inferior de material magnético se magnetizan con facilidad cuando fluye una corriente eléctrica en el rollo espiral, de tal forma que estas capas se vuelven los polos Norte y Sur magnéticos de un pequeño electro-magneto. (En una cabeza real, la distancia desde el espacio hasta la parte superior del rollo es de aproximadamente 30 mm).

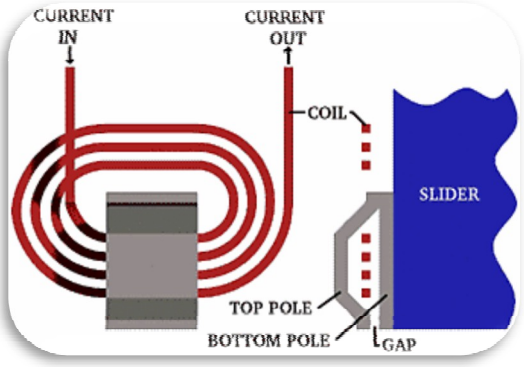


Figura 2.5.2.1. Escribiendo Datos Magnéticos

Los polos N-S en el extremo de la separación de la cabeza de escritura concentran el campo para hacer de esta región el “extremo de negociación”, que es el área en donde el campo de escritura sale al espacio por fuera de la

cabeza. Cuando un medio de almacenamiento magnético (por ejemplo, un disco giratorio en un computador) es ubicado muy cerca de la cabeza de escritura, el material magnético duro en la superficie del disco queda magnetizado de manera permanente (escrito) con una polaridad que corresponde a la del campo de escritura.

Si la polaridad de la corriente eléctrica se invierte, la polaridad magnética en la separación también se invierte.
Los computadores almacenan datos en un disco giratorio en la forma de dígitos binarios, o bits transmitidos a la unidad de disco en una secuencia de tiempo correspondiente a los dígitos binarios (*bits*) uno y cero.
Estos bits son convertidos en una onda de corriente eléctrica que es transmitida por medio de cables al rollo de la cabeza de escritura.

En su forma más simple, un *bit* uno corresponde a un cambio en la polaridad de la corriente, mientras que un *bit* cero corresponde a una ausencia de cambio en la polaridad de la corriente de escritura. Entonces, un disco en movimiento es magnetizado en la dirección positiva (Norte) para una corriente positiva y es magnetizado en la dirección negativa (Sur) para un flujo de corriente negativo. En otras palabras, los unos almacenados aparecen en donde ocurre una inversión en la dirección magnética en el disco, y los ceros residen entre los unos.

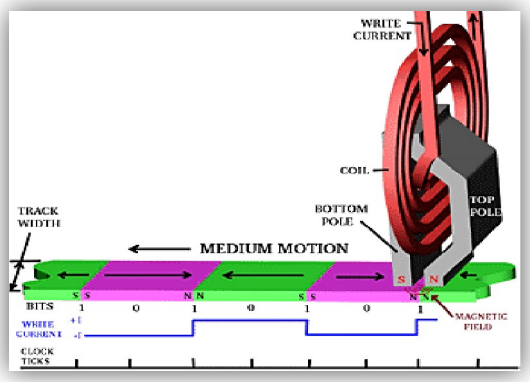


Figura 2.5.2.1.1. Escribiendo datos en un medio de almacenamiento

Un reloj de regulación está sincronizado con la rotación del disco y existen *celdas de bit* para cada *tick* del reloj; algunas de estas celdas de bits representarán un *uno* (una inversión en la dirección magnética, tal como N cambiando a S o S cambiando a N) y otras representarán *ceros* (polaridad N constante o S constante).
Una vez escritos, los bits en la superficie del disco quedan magnetizados permanentemente en una dirección o la otra, hasta que nuevos patrones sean escritos sobre los viejos.

Existe un campo magnético relativamente fuerte directamente sobre la localización de los *unos* y su fuerza se desvanece rápidamente a medida que la cabeza de grabación se aleja.

Un movimiento significativo en cualquier dirección que se aleje de un *uno* causa una dramática pérdida en la fuerza del campo magnético, lo que implica que para detectar bits de datos de manera confiable, es extremadamente importante que las cabezas de lectura vuelen muy cerca de la superficie del disco magnetizado.

2.5.2.2. Leyendo Datos Magnéticos

En la actualidad, las cabezas de lectura leen datos magnéticos mediante resistores magnéticamente sensitivos llamados *Válvulas Spin* que explotan el efecto GMR.

Estas cabezas *GMR/Válvula Spin* son situadas muy cerca del disco de almacenamiento magnético rotatorio, exponiendo el elemento GMR a los campos magnéticos de *bit* previamente escritos en la superficie del disco.

Si la cabeza GMR se aleja ligeramente del disco (2 o 3 millonésimas de pulgada) la intensidad del campo cae por fuera de un nivel útil, y los datos magnéticos no pueden ser recuperados fielmente.

Cuando una corriente atraviesa el elemento GMR, los cambios en la resistencia (correspondientes a los cambios en los estados magnéticos que surgen de los bits escritos N y S) son detectados como cambios en el voltaje. Estas fluctuaciones de voltaje –es decir, la señal- son conducidas a las terminales sensoras del GMR.

Sin embargo, el ruido eléctrico está presente en todos los circuitos eléctricos (las cabezas GMR no son la excepción), por lo que la señal combinada con el ruido de un lector GMR son enviados por medio de cables los circuitos electrónicos de la unidad de disco, para decodificar la secuencia de tiempo de los impulsos (y los espacios entre los impulsos) en unos y ceros binarios.

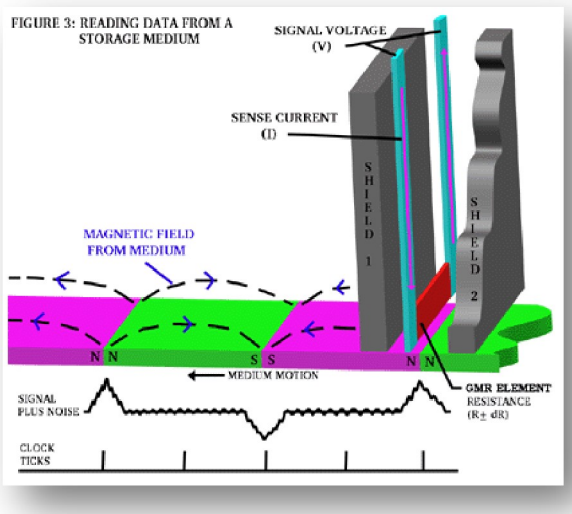


Figura 2.5.2.2. Leyendo datos magnéticos

2.5.3. Análisis de Discos

La clave de la computación forense es el análisis de discos duros, disco extraíbles, CDs, discos SCSI, y otros medios de almacenamiento. Este análisis no sólo busca archivos potencialmente incriminatorios, sino también otra información valiosa como *passwords*, *logins* y rastros de actividad en Internet.

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

Los investigadores forenses, utilizan herramientas especiales que buscan archivos "suprimidos" que no han sido borrados en realidad, estos archivos se convierten en evidencia. En las siguientes secciones, se explican algunas de las características poco conocidas del almacenamiento de la información en un computador, que son explotadas por los expertos en informática forense para recuperar datos que se creían eliminados.

2.5.3.1. File Slack

Los archivos son creados en varios tamaños dependiendo de lo que contengan. Los sistemas basados en DOS, Windows 95/98/ME/XP y Windows NT/2000 almacenan los archivos en bloques de tamaño fijo llamados clusters, en los cuales raramente el tamaño de los archivos coinciden perfectamente con el tamaño de uno o muchos clusters.

El espacio de almacenamiento de datos que existe desde el final del archivo hasta el final del cluster se llama "file slack". Los tamaños de los clusters

varían en longitud dependiendo del sistema operativo involucrado y, en el caso de Windows 95/98/ME/XP, del tamaño de la partición lógica implicada.

Un tamaño más grande en los clusters significan más file slack y también mayor pérdida de espacio de almacenamiento. Sin embargo, esta debilidad de la seguridad del computador crea ventajas para el investigador forense, porque el file slack es una fuente significativa de evidencia y pistas.

El file slack, potencialmente contiene octetos de datos aleatoriamente seleccionados de la memoria del computador. Esto sucede porque DOS/Windows escribe normalmente en bloques de 512 bytes llamados sectores.

Los clusters están compuestos por bloques de sectores, si no hay suficientes datos en el archivo para llenar el ultimo sector del archivo, DOS/Windows diferencia hacia arriba(los datos) completando el espacio restante con datos que se encuentran en ese momento en la memoria del sistema.

2.5.3.2. Archivo Swap de Windows

Los sistemas operativos Microsoft Windows utilizan un archivo especial como un "cuaderno de apuntes" para escribir datos cuando se necesita memoria de acceso aleatorio adicional. En Windows 95/98/ME/XP, a estos archivos se les conoce como Archivos Swap de Windows. En Windows NT/2000 se conocen como directorios de página de Windows pero tiene esencialmente las mismas características que los de Win9x.

Los archivos de intercambio son potencialmente enormes y la mayoría de los usuarios de PC son inconscientes de su existencia. El tamaño de estos archivos puede extenderse desde 20MB a 200MB, el potencial de estos es contener archivos sobrantes del tratamiento de los procesadores de texto, los mensajes electrónicos, la actividad en Internet (cookies, etc.), logs de entradas a bases de datos y de casi cualquier otro trabajo que haya ocurrido durante las últimas sesiones. Todo esto genera un problema de seguridad,

porque el usuario del computador nunca es informado de este almacenamiento transparente.
Los Archivos Swap de Windows actualmente proporcionan a los especialistas en computación forense pistas con las cuales investigar, y que no se podrían conseguir de otra manera.

2.5.3.3. Unallocated File Space

Cuando los archivos son borrados o suprimidos en DOS, Win9x, WinNT/2000, el contenido de los archivos no es verdaderamente borrado. A menos que se utilice algún software especial que ofrezca un alto grado de seguridad en el proceso de eliminación, los datos "borrados", permanecen en un área llamada espacio de almacenamiento no-asignado (Unallocated File Space). Igual sucede con el file slack asociado al archivo antes de que éste fuera borrado. Consecuentemente, siguen existiendo los datos, escondidos pero presentes, y pueden ser detectados mediante herramientas de software para el análisis de la computación forense.

2.6. Eliminación de datos

Hasta el momento, se ha hablado de la forma de almacenar y leer los datos en un disco de computador, sin embargo pueden darse casos legítimos en donde sea necesario *destruir* información sin dejar rastro alguno. En este numeral, se describen las prácticas adecuadas para la eliminación de información.

2.6.1. Eliminación de Datos en un Medio Magnético

Borrar de manera definitiva los datos en un medio magnético tiene toda una problemática asociada. Como se vio en una sección anterior, la información es escrita y leída aprovechando las características de magnetización de un material determinado.

Sin embargo, y dependiendo del medio usado (unidades de disco, cintas, diskettes, etc.), el proceso de eliminación total de los datos se ve afectado por diversos factores.

El Departamento de Defensa de los Estados Unidos (DoD) cuenta con toda una serie de recomendaciones sobre cómo “sanitizar” un medio magnético, esto es, el proceso por el cual la información clasificada es removida por completo, en donde ni siquiera un procedimiento de laboratorio con las técnicas conocidas a la fecha o un análisis pueda recuperar la información que antes estaba grabada.

Aunque en un comienzo los procedimientos a seguir pueden parecer algo paranoicos, la (relativa) facilidad con la que se puede recuperar información que se creía borrada hace necesario tomar medidas extremas a la hora de eliminar datos confidenciales o comprometedores.
En enero de 1995, el DoD publicó un documento, el “National Industrial Security Program Operating Manual” (NISPOM), más comúnmente referenciado como “DoD 5220.22-M”, que detalla toda una serie de procedimientos de seguridad industrial, entre ellos, cómo eliminar datos contenidos en diferentes medios.

A partir de los lineamientos presentes en 5220.22-M , otro organismo estadounidense, el Defense Scurity Service, publicó una “Matriz de Sanitización y Borrado” que explica de manera práctica los pasos a seguir para remover por completo información sensitiva. En las siguientes secciones se hacen algunas precisiones técnicas, y en el apéndice A se muestra y se explica la Matriz.

2.6.1.1 Degaussing de Medios Magnéticos

La Matriz de Limpieza y Sanitización es una acumulación de métodos conocidos y aprobados para limpiar y/o sanitizar diversos medios y equipo. Cuando NISPOM fue publicado, el Rango Extendido Tipo II, Tipo III y los *degaussers* de Propósito Especial no existían.
Esto resultaba en la necesidad de destruir todos los medios con un factor de coercividad (cantidad de fuerza eléctrica requerida para reducir la fuerza magnética grabada a cero) mayor que 750 oersteds (unidad que mide la fuerza magnetizante necesaria para producir una fuerza magnética deseada a

lo largo de una superficie) y la mayoría de discos magnéticos cuando ya no fueran necesarios como soporte para una misión clasificada. Ahora, la "National Security Agency norteamericana" (NSA) ha evaluado *degaussers* de cinta magnética que satisfacen los requerimientos del gobierno para sanitizar cintas magnéticas de hasta 1700 oersteds.

Las cintas magnéticas se encuentran divididas en Tipos. La cinta magnética de Tipo I tiene un factor de coercividad que no excede los 350 oersteds y puede ser usada para sanitizar (*degauss*) todos los medios de Tipo I.
La cinta magnética de Tipo II tiene un factor de coercividad entre 350 y 750 oersteds y puede ser usada para sanitizar todos los medios Tipo I y II.

La cinta magnética Tipo II de Rango Extendido tiene un factor de coercividad entre 750 y 900 oersteds y puede ser usada para sanitizar todos los medios Tipo I, Tipo II y Rango Extendido. Finalmente, las cintas magnéticas Tipo III, comúnmente conocidas como cintas de alta energía (por ejemplo, cintas de 4 ó 8mm), tiene un factor de coercividad actualmente identificado como entre 750 y 1700 oersteds y puede ser usada para sanitizar todos los tipos de cintas magnéticas.

Para sanitizar (degauss) todos los medios de disco, rígidos o flexibles (por ej., *diskettes*, Bernoulli, Syquest y unidades de Disco Duro) se deben usar *degaussers* de Unidad de Disco. Para este tipo de dispositivos la NSA tiene una nueva categoría de *degaussers*, conocida como *Degaussers* de Propósito Especial.

DSS, como todas las agencias del DoD, referencia el "Information Systems Security Products and Services Catalog" como guía de sanitización de memoria y medios. NSA publica el "Information Systems Security Products and Services Catalog" entre sus productos y servicios de seguridad para sistemas de información. La lista de productos *degausser* (DPL) está dedica a los *degaussers* de discos y cintas magnéticas. La DPL hace un excelente trabajo identificando los fabricantes de *degaussers* y los diferentes tipos de éstos.

2.6.2 Eliminación de Datos en CDs

Los datos de un CD están almacenados en la parte superior del CD por medio de una capa reflectiva que es leída por un láser. Los CDs ofrecen buenas alternativas para almacenar información por largos periodos de tiempo, pero puede ser necesario destruirlos. Se mencionan algunos medios para hacer esto:

1. **Retiro de la lámina reflectiva:** Se puede retirar la lámina con algún elemento cortante, sin embargo se debe destruir la lámina reflectiva, y aún así pueden quedar algunos rastros de datos en el policarbonato.
2. **Cortar en pedazos:** Con una cortadora industrial de papel, el CD podría ser destruido, sin embargo, la lámina reflectiva podría separarse del CD y no ser cortada correctamente.
3. **Destruir el CD por medios químicos:** Una posible alternativa es introducir el CD en Acetona, lo cual dejaría la lámina superior inservible, sin embargo es posible que la lámina de policarbonato aún contenga algunos rastros de información.
4. **Destrucción por Incineración:** Probablemente es el método más rápido y eficiente, pero es realmente nocivo para el medio ambiente. El humo del policarbonato puede ser perjudicial para la salud de las personas.
5. **Destrucción por medio de un horno microondas:** Introduciendo el CD en un microondas por unos 3 segundos puede destruir gran parte del CD, sin embargo no todas las partes serán destruidas. Este método no se recomienda, especialmente porque puede dañar el horno debido a los campos magnéticos que usa el horno y que pueden causar un cortocircuito debido a que el CD contiene metales.
6. **Reescritura:** Para los CDs re-escribibles, es posible volverlos a escribir de tal forma que el proceso dañe los datos. Sin embargo, no se sabe si por mecanismos especiales sea posible recuperar la información.
7. **Rayado Simple:** A menos que uno quiera ser realmente precavido, la forma mas fácil de destruir un CD es rayando la parte superior. La razón por la que se debe rayar la parte superior es porque es esta la que mantiene los datos. Si

es rayada la parte inferior es fácil recuperar la capa y corregir el problema, utilizando productos comerciales para recuperar CDs.

2.7. Pasos para la Recolección de Evidencia

El procedimiento para la recolección de evidencia varía de país a país, y por lo tanto, un análisis exacto y completo está fuera de los límites de este documento. Sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense:

2.7.1 Hardware

El hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen (por Ej. contrabando o robo), es por eso que se deben tener consideraciones especiales. Lo primero que se debe preguntar el investigador es qué partes se deben buscar o investigar.

2.7.2 Cuidados en la Recolección de Evidencia

La recolección de evidencia informática es un aspecto frágil del la computación forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- ✓ Se debe proteger los equipos del daño.
- ✓ Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
- ✓ Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

2.8. Herramientas de Investigación Forense

En la actualidad existen cientos de herramientas [14], las cuales se pueden clasificar en cuatro grupos principales.

2.8.1 Herramientas para la Recolección de Evidencia

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

1. La gran cantidad de datos que pueden estar almacenados en un computador.
2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.

3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de computadores.
6. Mecanismos de encripción, o de contraseñas.

2.8.1.1 EnCase

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. Permite asistir al especialista forense durante el análisis de un crimen digital.
Se escogió mostrar esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense.

Algunas de las características más importantes de EnCase se relacionan a continuación:

Copiado Comprimido de Discos Fuente. Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los

archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales).

Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismos tiempo, examinando la evidencia y buscando en paralelo.

Búsqueda y Análisis de Múltiples partes de archivos adquiridos. EnCase permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos "zip" y otros tipos de dispositivos de almacenamiento de la información. Con Encase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista. En varios casos la evidencia puede ser ensamblada en un disco duro grande o un servidor de red y también buscada mediante EnCase en un solo paso.

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

Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo. EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

Análisis Compuesto del Documento. EnCase permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno y los datos del espacio unallocated.

Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de E-Mail.

Firmas de archivos, Identificación y Análisis. La mayoría de las graficas y de los archivos de texto comunes contiene una pequeña cantidad de bytes en el comienzo del sector los cuales constituyen una firma del archivo. EnCase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechosos haya escondido un archivo o simplemente lo haya renombrado, EnCase detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.

Análisis Electrónico Del Rastro De Intervención. Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computador. EnCase proporciona los únicos medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente. Con la característica de ordenamiento, el análisis del contenido de archivos y la interfaz de EnCase, virtualmente toda la información necesitada para un análisis de rastros se puede proporcionar en segundos.

Soporte de Múltiples Sistemas de Archivo. EnCase reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVD- R. Con EnCase un investigador va a ser capaz de ver, buscar y ordenar archivos desde estos discos concurridos con otros formatos en la misma investigación de una manera totalmente limpia y clara.

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

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

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

EnCase es un software costoso, y en Estados Unidos los costos se dividen así:

- Gobierno y Educación US$1,995
- Sector Privado US$2,495

Actualmente EnCase se encuentra en su versión 3.0.

2.8.2. Herramientas para el Monitoreo y/o Control de Computadores

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

2.8.2.1. KeyLogger

"KeyLogger" es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por *e-mail*. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas.

En el apéndice B se puede observar un ejemplo de un *log* generado por este programa.

2.8.3. Herramientas de Marcado de documentos

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

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

2.8.4 Herramientas de Hardware

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

2.9. Dificultades del Investigador Forense

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.
2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
3. Será difícil encontrar toda la información valiosa.
4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.
5. Los errores cometidos pueden costar caro para la persona o la organización que representa.
6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.
8. Dificultad para conducir la investigación de manera objetiva.

9. Dificultad para hacer correctamente una entrevista con las personas involucradas.
10. Reglamentación que puede causar problemas legales a la persona.

Es por esto que, antes de lanzarse a ser un investigador forense, se necesita bastante estudio y experiencia, entre otras cosas, y si no se cumple con los requisitos, en caso de un accidente es aconsejable llamar a uno o varios expertos.

Capítulo III EnCase Forensic

Capítulo III EnCase Forensic

3.1. Que es Encasé Forensic

EnCase Forensic es el estándar de la industria en tecnología de investigación forense informática. Con una interfaz gráfica del usuario (GUI) intuitiva, análisis superior, soporte mejorado de correo electrónico/Internet y motor potente de scripting, EnCase proporciona a los investigadores una herramienta única, capaz de realizar investigaciones complejas y a gran escala de principio a fin.

Funcionarios encargados del cumplimiento de la ley, investigadores gubernamentales/corporativos y consultores en todo el mundo se benefician de la potencia de EnCase Forensic en una manera que supera ampliamente a cualquier otra solución forense.

- Adquiera datos en una manera sólida desde el punto de vista forense, con software que posee un registro sin igual en los tribunales de justicia de todo el mundo.
- Investigue y analice plataformas múltiples (Windows, Linux, AIX, OS X, Solaris y más) con una sola herramienta.
- Ahorre días, si no semanas, en tiempo de análisis al automatizar tareas complejas y rutinarias con módulos EnScript® precreados, como el análisis de registros de eventos y casos inicializados.
- Encuentre información a pesar de los esfuerzos de ocultarla, encubrirla o eliminarla.
- Maneje fácilmente grandes volúmenes de evidencia informática al visualizar todos los archivos relevantes, incluidos los archivos "eliminados", los espacios muertos de los archivos y los espacios no designados.
- Transfiera archivos de evidencia directamente a los representantes legales o encargados del cumplimiento de la ley, según sea necesario.
- Las opciones de revisión permiten que las personas que no son investigadores, como los abogados, revisen la evidencia con facilidad.

- Las opciones de generación de informes permiten la preparación rápida de informes.

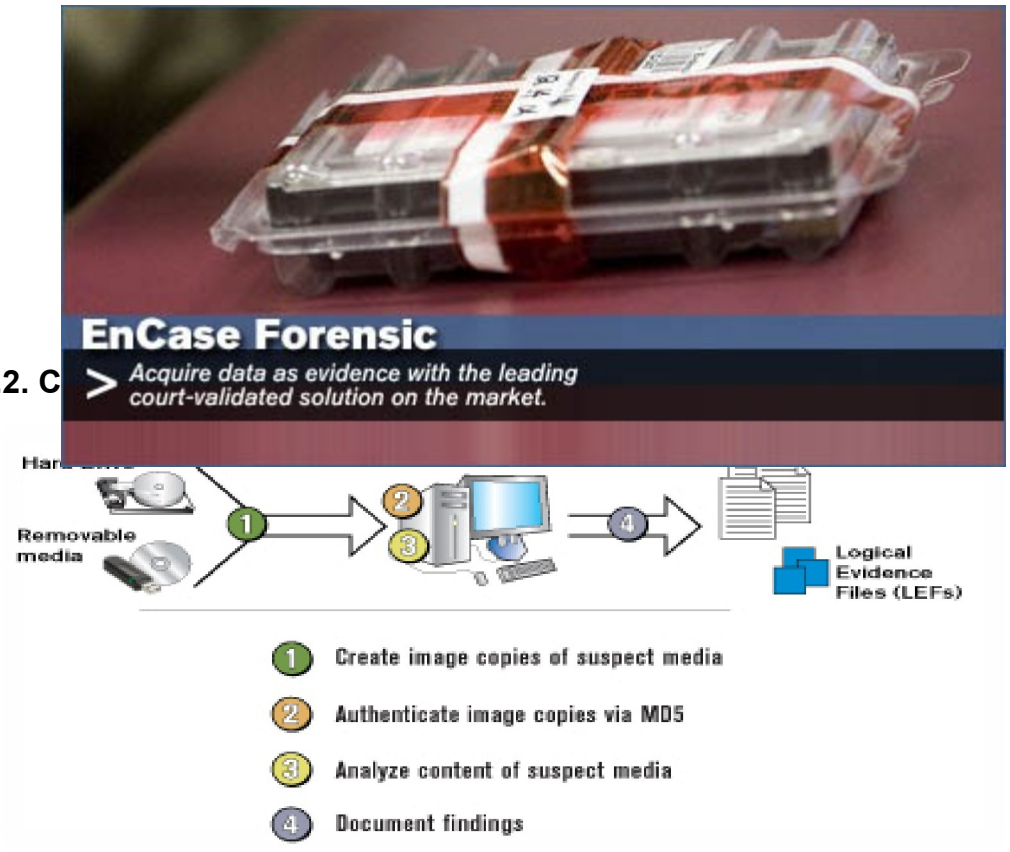


Figura 3.2. Cómo funciona EnCase® Forensic

*Sistemas de archivos admitidos por el software EnCase: FAT12/16/32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), Sistema de archivos transaccional de AIX (JFS y jfs) LVM8, FFS (OpenBSD, NetBSD y FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD, sistemas de archivos ad TiVo® 1 y TiVo 2.

3.3. Requisitos del sistema para EnCase® Forensic

Guidance Software recomienda los siguientes requisitos mínimos de hardware para EnCase Forensic:

• Windows 2000, XP ó 2003 Server

• Procesador Intel o AMD de 3 GHz o superior recomendado

• 1 GB de RAM (se recomienda 2 GB o más)

• 1 puerto USB

• Se recomienda un amplio espacio de almacenamiento de datos para admitir la adquisición de archivos de evidencia

3.4. El Estándar en Computación Forense

El estándar a nivel mundial en computación forense: Utilizado por más de 12.000 investigadores y profesionales de la seguridad.
La policía, el gobierno, los militares y los investigadores corporativos confían en EnCase Edición Forense para ejecutar exámenes informáticos delicados y conclusivos. Guiados por nuestras relaciones con investigadores en el mundo entero, El programa EnCase ha sido optimizado para manejar la complejidad cada vez mayor de las configuraciones y capacidades informáticas. El programa EnCase soporta un amplio rango de sistemas operativos, archivos y periféricos que son el desafío de los investigadores forenses diariamente.
Como una herramienta seleccionada por la policía, el programa EnCase ha soportado numerosos desafíos en las cortes de justicia, demostrando su confiabilidad y exactitud. Recientemente, el Instituto Nacional para Estándares y Tecnología (NIST) concluyó que EnCase Imaging Engine (motor de creación de imágenes de discos) opera con mínimos defectos. Ninguna otra solución de computación forense tiene este record de credibilidad, otorgado por sus usuarios, agencias independientes y cortes de justicia. EnCase software fue premiado con el prestigioso premio eWEEK por la excelencia y un grado de 5 estrellas en SC Magazine.

3.5. Alto rendimiento de procesamiento y confiabilidad

La clave para computación forense es la capacidad de adquirir y analizar datos rápidamente. EnCase Edición Forense V4 le permite a los investigadores manejar fácilmente largos volúmenes de evidencia computacional, la visualización de todos archivos relevantes, incluyendo aquellos eliminados y el espacio no utilizado. La incomparable funcionalidad del programa de EnCase permite a los investigadores llevar satisfactoriamente el proceso completo de investigación computacional, incluyendo reportes personalizados de búsquedas y sus ubicaciones.

3.6. Adquisiciones forenses confiables

El programa EnCase ejecuta adquisiciones de medios produciendo un duplicado binario exacto de los datos del medio original. EnCase verifica este duplicado generando valores de hash MD5 en ambos medios (el original y el archivo imagen o "archivo de evidencia"). Adicionalmente, a cada 64 sectores de la evidencia se le asigna un valor CRC. Estos valores CRC son verificados cada vez que la evidencia es accesada.

3.7. Flexibilidad extrema: EnScript

EnScript es un macro lenguaje de programación incluido en el programa EnCase. Emulando características de Java y C++, EnScript le permite al investigador construir scripts personalizados para necesidades específicas de la investigación y/o automatización de tareas rutinarias complejas. Mediante la automatización de cualquier tarea investigativa, EnScript no solamente puede salvar días de investigación, si no semanas del tiempo de análisis.

3.8. Características de EnCase Edición Forense

3.8.1. Múltiple administración de casos

La característica de múltiple administración de casos del programa EnCase, permite a los investigadores ejecutar simultáneamente múltiples casos hacia diferentes objetivos con diversos medios.

3.9. Soporte Unicode

Cuando un usuario visualiza un documento creado en un lenguaje diferente, el programa EnCase puede desplegar los caracteres correctamente. Esta es una característica que le permite al programa EnCase buscar palabras claves y desplegar los resultados en cualquier lenguaje.

3.10. Configuración dinámica de discos

El programa EnCase soporta las siguientes configuraciones dinámicas de discos: Spanned, Mirrored, Striped, RAID 5 y básico. Con el ingreso de un mínimo de información, por parte del investigador, el programa EnCase puede detectar automáticamente la configuración de los discos y conectar todas las particiones, mientras que se conservan intactas las áreas libres y de arranque para futuras búsquedas.

3.11. Búsqueda y análisis: palabras claves, búsqueda de hash y firmas, y filtros

EnCase Edición Forense V4 le permite a los investigadores analizar y pre visualizar simultáneamente múltiples bloques de datos adquiridos. Los investigadores pueden utilizar búsquedas globales de palabras claves, análisis de hash, análisis de firmas de archivos y filtros específicos de archivos para analizar rápidamente la evidencia.

3.12. Opciones de adquisición múltiple

Al igual que existen muchas formas de medios digitales, existen muchas otras formas de adquisición de medios. EnCase incluye cables para puertos paralelos y cable de red cruzado para Windows y DOS. Ambos métodos permiten al programa "escribir bloques" para ser colocados en el medio sospechoso, asegurando que el medio original no sea alterado.

3.13. Sistemas de archivos (file systems) interpretados por EnCase

Los siguientes sistemas de archivos son actualmente soportados por EnCase Edición Forense Versión 4: FAT12 (disco flexible), FAT16, FAT32, NTFS, HFS, HFS+, Sun Solaris UFS, EXT2/3, Reiser, BSD FFS, Palm, CDFS, Joliet, UDF e ISO 9660.

3.14. Soporte para correo electrónico PST

El programa EnCase soporta archivos PST que tengan cifrado compresible y cifrado completo, obviando el archivo de contraseñas PST.

3.14.1. Visor de galería

El visor de galería provee un método simple para visualizar rápidamente todas las imágenes en el archivo de evidencia. La galería despliega imágenes BMP, JPGs, GIFs y TIFFs.

3.14.2. Visor de escala de tiempo

El visor de escala de tiempo le permite a los investigadores visualizar gráficamente toda la actividad de en un estilo de calendario, ilustrando los atributos del archivo, por ejemplo: cuándo el archivo fue creado, última vez accesado o escrito. El visor de escala de tiempo puede mostrar escalas desde días hasta años, sirviendo como una herramienta invaluable para mirar todos los patrones de actividad de archivos.

3.14.3. Visor de reportes

Los reportes pueden ser generados sobre cualquier archivo, carpeta, volumen, disco físico o el caso completo. Los reportes incluyen información referente a la adquisición de datos, geometría del disco, estructuras de carpetas, marcadores de archivos e imágenes. Los investigadores pueden exportar los reportes a formato RTF o HTML.

3.15. EnCase módulo del sistema de archivos de cifrado (Encrypting File System. EFS)

El módulo de EFS de EnCase provee la capacidad de descifrar carpetas y archivos del sistema de archivos cifrados (EFS), para usuarios locales autenticados.

3.15.1. EnCase módulo del sistema de archivos virtuales (Virtual File System . VFS)

El módulo de VFS de EnCase permite a los examinadores montar la evidencia de un computador en modo de lectura únicamente y fuera de la red,

permitiendo la examinación adicional de la evidencia usando el explorador de Windows y herramientas de terceros.

3.15.2. Módulo del servidor de autenticación en red (Network Authentication Server . NAS)

El servidor de autenticación en red provee una completa flexibilidad en el licenciamiento del programa EnCase. NAS permite licenciar el programa EnCase de tres formas: Local en el computador del examinador, remotamente con servicios de terminal y a través de red usando el administrador de licencias (License Manager).

3.16. Acerca de Guidance Software

Guidance Software es el líder en computación forense y soluciones de respuesta a incidentes. Fundado en 1997 y ubicado en Pasadena, CA. Guidance Software tiene oficinas y centros de capacitación en California, Virginia y el Reino Unido.

Más de 12.000 investigadores corporativos y del gobierno confían en el programa EnCase, mientras que más de 3.500 investigadores atienden a las capacitaciones anuales sobre metodología en forenses. Aceptado por numerosas cortes judiciales y honrado con el premio a la excelencia de eWEEK y el premio anual de SC Magazine, el programa EnCase es considerado como la herramienta estándar en computación forense.

3.17. Acerca de Internet Solutions

Internet Solutions es una compañía de servicios e integración de soluciones de prevención, detección y reacción en Seguridad Informática, proporcionando confidencialidad, integridad, disponibilidad, autenticación y no repudio en la información.

La clave para computación forense es la capacidad de adquirir y analizar datos rápidamente.

3.18. Capturas de Pantalla

3.18.1. EnCase® Forensic Screenshots

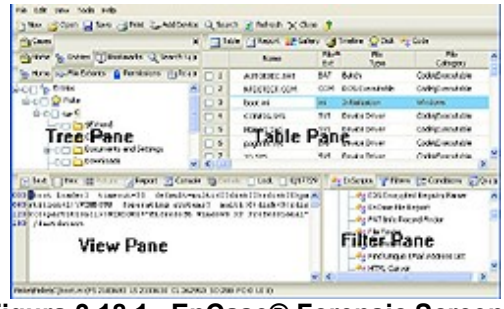
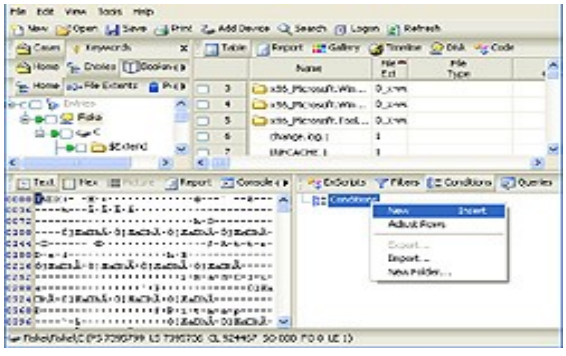
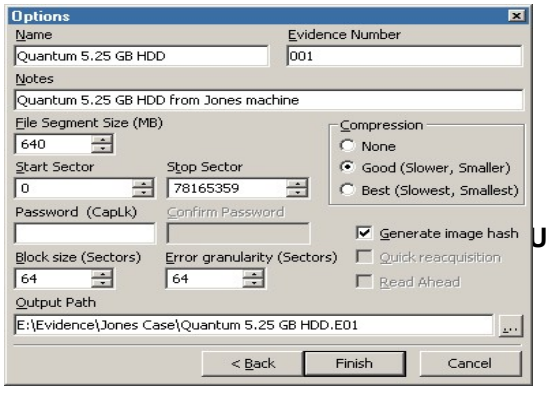


Figura 3.18.1. EnCase® Forensic Screenshots

3.18.2.The EnCase Forensic GUI.



Usuarios con permiso de las condiciones para crear rápidamente los filtros complejos, polifacéticos, sin cualquier conocimiento del lenguaje de programación de EnScript®.



UI.

Los ajustes de la granulosidad del tamaño y del error de bloque interconectan.

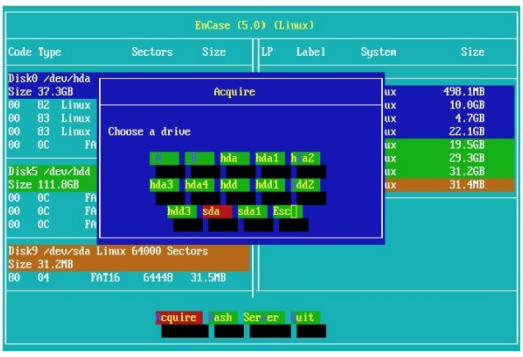
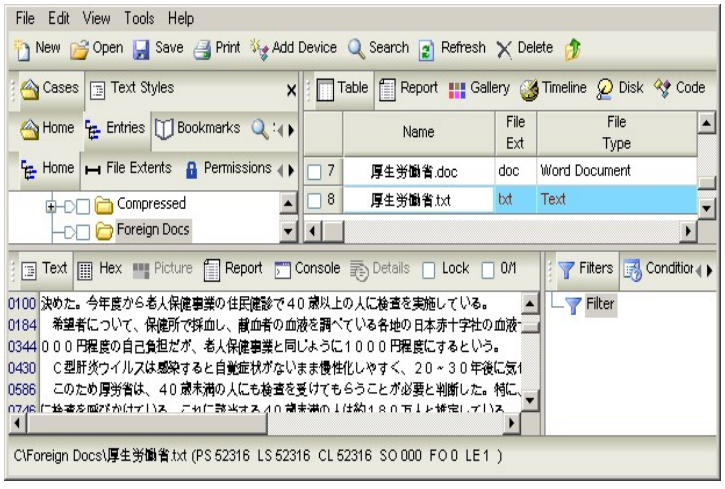
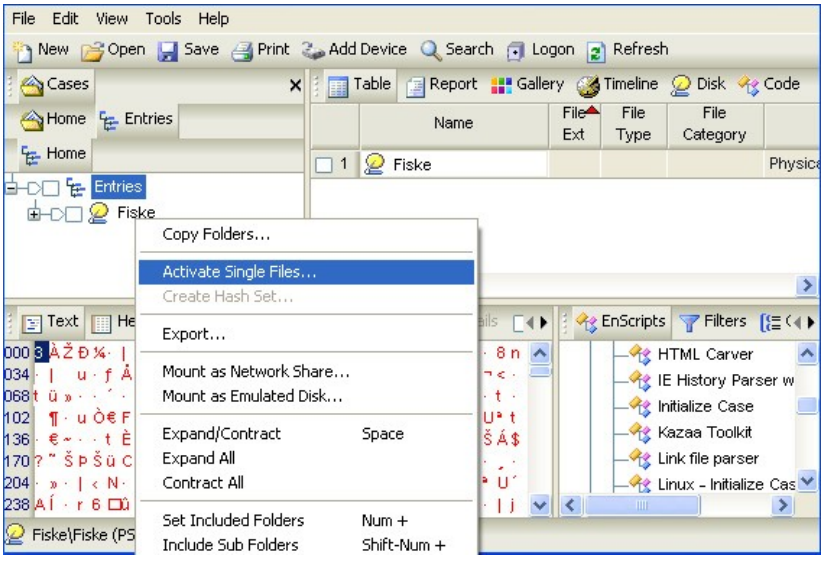


Figura 3.18.2.2. The EnCase Forensic GUI.

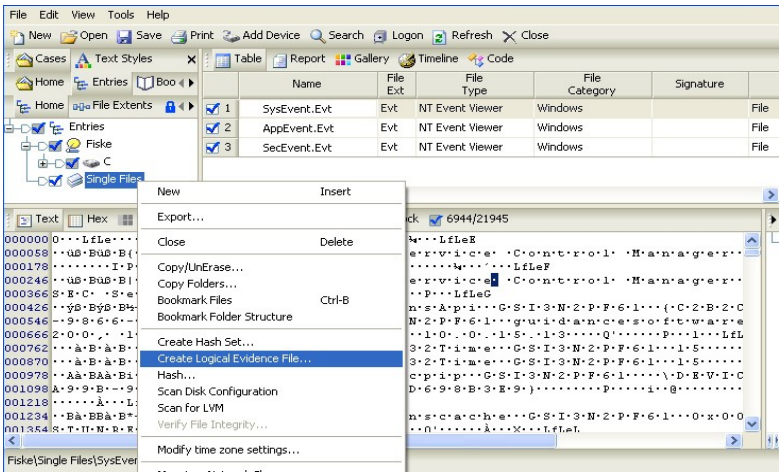
La herramienta de lino de la adquisición puede ser agregada fácilmente a cualquier disco blando forense de la computadora del linux o patear el CD.



Ayuda de Unicode teniendo en cuenta la exhibición de idiomas carácter-basadas.



Los solos archivos permiten que un examinador arrastre - y - caen archivos particulares del interés en encajonan para el análisis.



Los archivos lógicos de la evidencia se pueden crear y trabar de " Solos archivos, " así como de archivos específicos del interés de una inspección previo del embalaje de medios sujetos.

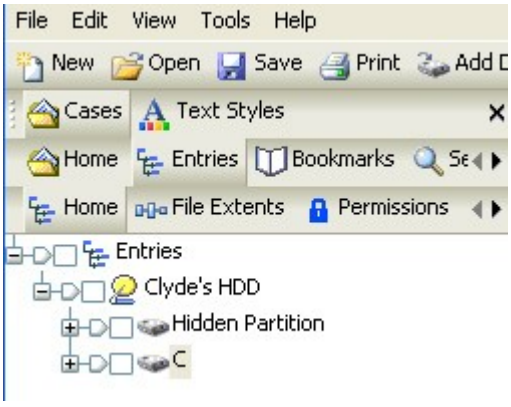
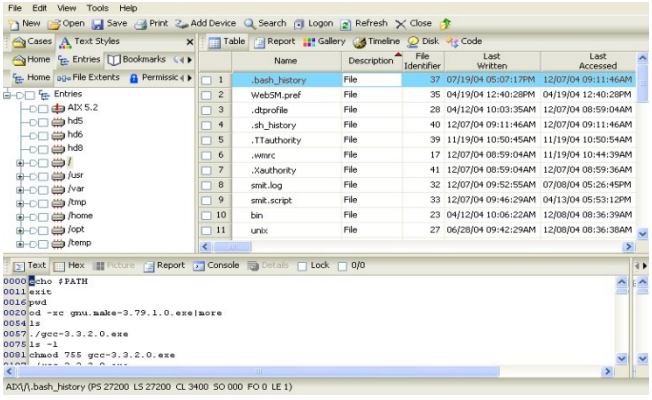
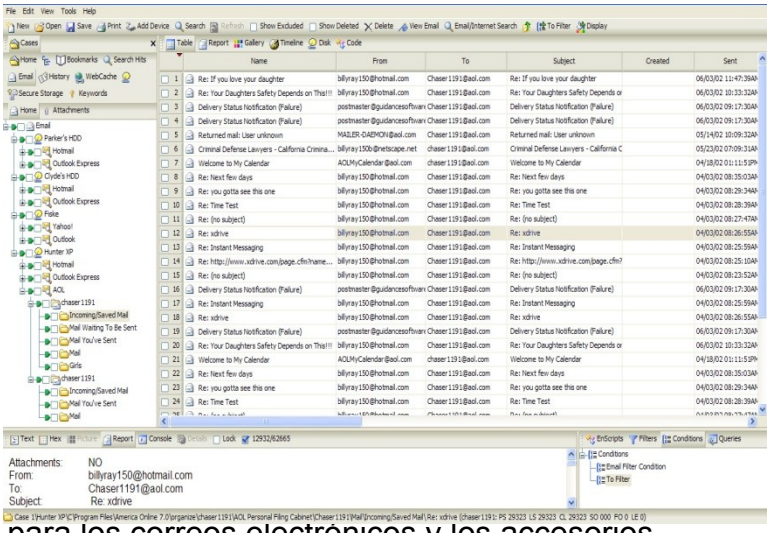


Figura 3.18.2.6. The EnCase Forensic GUI.

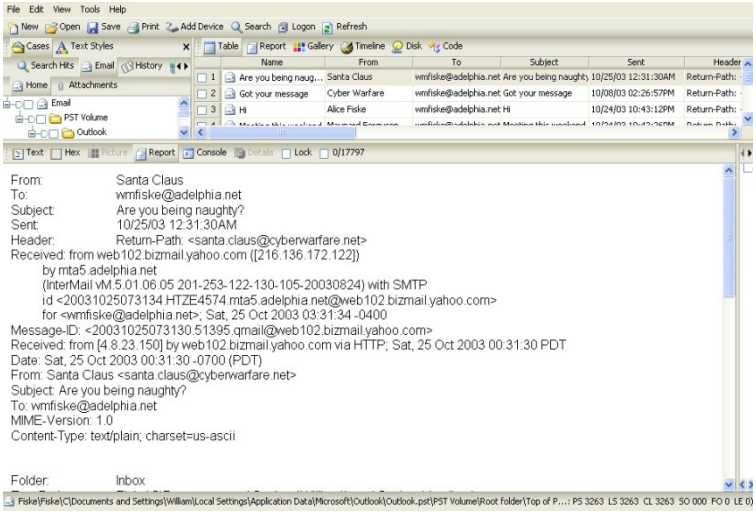
Las particiones lógicas se pueden retitular para etiquetar correctamente particiones de diagnóstico u ocultadas.



Encase Forense proporciona la ayuda para la exhibición de los sistemas de ficheros de los jfs y de JFS para el AIX.



Exhibición para los correos electrónicos y los accesorios.



La información de jefe del email se puede exhibir o no, con el jefe de la demostración.

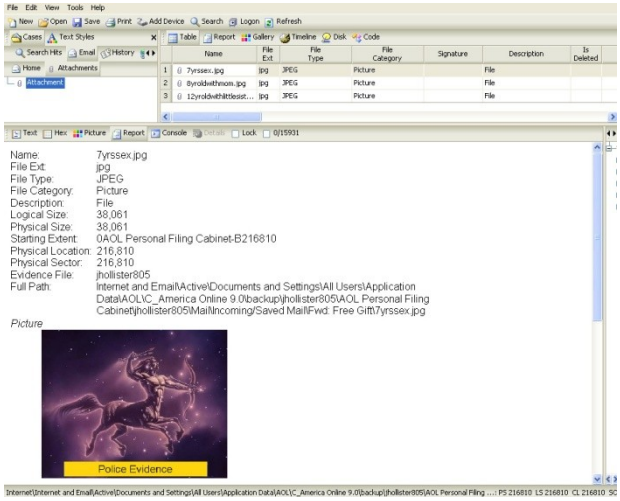


Figura 3.18.2.10. The EnCase Forensic GUI.

Los accesorios del email son fáciles de ver.

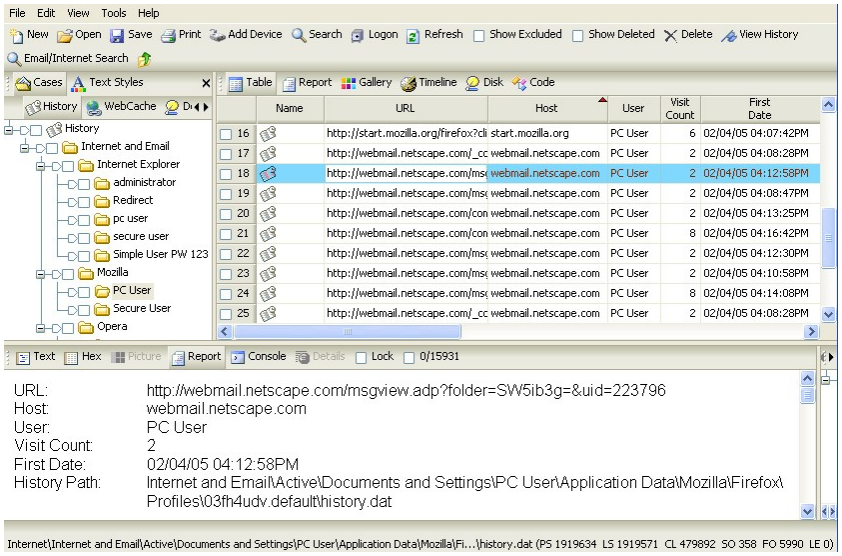


Figura 3.18.2.11. The EnCase Forensic GUI.

Ayuda con Internet Explorer, Mozilla, la ópera y el safari de Macintosh.

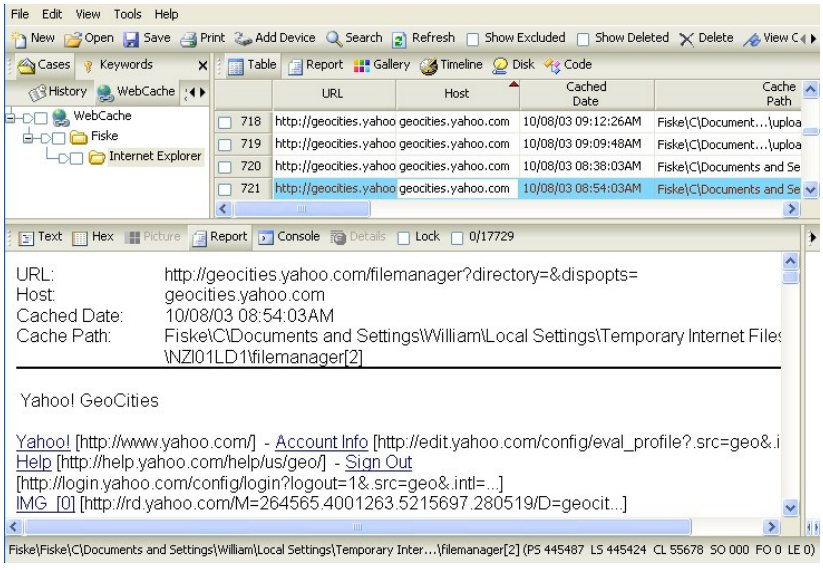
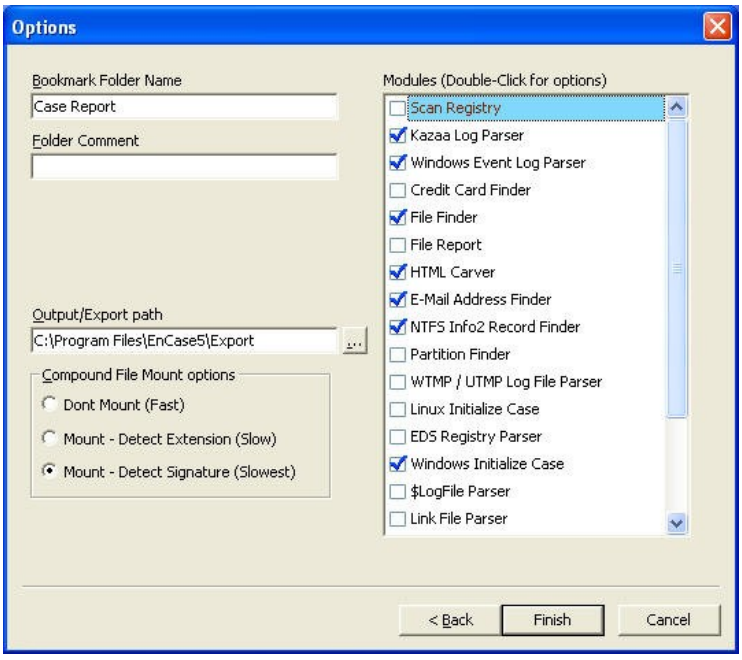


Figura 3.18.2.12. The EnCase Forensic GUI.

Ayuda del análisis del escondrijo de Web para Internet Explorer, Mozilla, la ópera, y el safari de Macintosh.

Figura 3.18.2.13. The EnCase Forensic GUI.



El caso EnScript del barrido automatiza investigaciones permitiendo que el otro EnScripts sea llamado y funcionó.

Glosario

Glosario

Clúster: Conjunto de empresas, agentes u organizaciones que inciden en la elaboración de un producto o en la presentación de un servicio y que están geográficamente próximas.

Coercividad: Cantidad de fuerza eléctrica requerida para reducir la fuerza magnética grabada a cero.

Computación forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Concernientes: Diccionario de la lengua española. Que concierne o corresponde:

Confiabilidad: Método de medición cualitativa que sugiere que los mismos datos deben ser observados cada vez que se realiza una observación del mismo fenómeno. Grado en que una prueba proporciona resultados consistentes.

Criminalística: La definición más común entre la mayoría de los autores es la que concibe la Criminalística como "la disciplina auxiliar del Derecho Penal que se ocupa del descubrimiento y verificación científica del delito y del delincuente".
Aparte algunos otros puntos discutibles, consideremos que la anterior definición adolece de imprecisión en su última parte, al hablar de delito y delincuente.

Deterioro: Daño. Poner en mal estado o en inferioridad de condiciones algo.

Diligencia: Es la precaución o cuidado con que una persona desempeñan sus funciones o se comporta en su vida a fin de no causar daño o lesión a terceros

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.

Discrepancia: Aquella información o información faltante, de los documentos presentados en virtud de un crédito documentario, que: - no concuerda con sus términos y condiciones. - no concuerda con los demás documentos presentados. - no cumple con los requisitos de las RRUU Si los documentos revelan discrepancias, el banco emisor no estará obligado a pagar y, en el caso de un crédito documentario confirmado tampoco lo estará el banco confirmador. (Principio del estricto cumplimiento documentario).

EnCase Forensic: Es el estándar de la industria en tecnología de investigación forense informática. Con una interfaz gráfica del usuario (GUI) intuitiva, análisis superior, soporte mejorado de correo electrónico/Internet y motor potente de scripting.

Esterilidad: Es una cualidad atribuible a aquellas personas u otros organismos biológicos que no se pueden reproducir.

Fraudulentos: es la intervención deliberada en un proceso electoral con el propósito de impedir, anular o modificar los resultados reales.

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.
Idoneidad: Las normas o requisitos que determinan si una persona tiene las características necesarias para participar en un estudio de investigación.

Incidentes: Es un litigio accesorio con ocasión de un juicio, que normalmente versa sobre circunstancias de orden procesal.

Inherente: Que es necesario e inseparable de lo que está unido

Interdisciplinario: Estudios u otras actividades (juegos) que se realizan mediante la cooperación de varias disciplinas.

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

Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.
Perjuicio: Ganancia o utilidad que con razón era esperada y que por la acción de alguien ha dejado de obtenerse.

Peritaje: (expert testimony). El dictamen que se encomienda a un perito, en materia de su competencia, para ser presentado ante las autoridades judiciales o administrativas.

Previsibilidad: Debe de realizarse tomándose en cuenta no hay certeza completa por la cantidad de factores y la intervención de decisiones humanas, por lo siempre existirá en la empresa un riesgo.

Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

Salvaguardar: Mecanismo físico o lógico capaz de reducir el riesgo y, también, acción fruto de una decisión para reducir un riesgo.

Salvaguarda preventiva: acción sobre la vulnerabilidad que neutralizando otra acción, materializada por la amenaza, antes de que actúe ésta.

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

Vulnerabilidad: Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar.

Bibliografía

Bibliografía

CANO, J. (2006) Estado del arte del peritaje informático en Latinoamérica. Alfa- REDI. Disponible en: http://www.alfa-redi.org/ar-dnt-documento. shtml?x=728

Cashin, James A.; Newirth, Paul D.; Levy John S. **Enciclopedia de Auditoria.** España: Editora Océano Centrum, 2000.

Cepeda Alfonso, Gustavo. **Auditoría y Control Interno.** Santo Domingo, Editora Corripio C. Por A. 1997.

BRUNGS, A y JAMIESON, R. (2003) Legal issues for computer forensics. Proceedings for 14th Australasian Conference on Information Systems.

Hernández Sampieri, Roberto.; Fernández Collado, Carlos y Baptista Lucio, Pilar. **Metodología de la Investigación.** México: 2da. Edición Macgraw−Hill Interamericana Editores, S.A. 1998.

Instituto Mexicano de Contadores Públicos**. Normas Internacionales de Auditoría (NIA's).** México: 4ta. Edición 1997.

Instituto Mexicano de Contadores Públicos. **Normas Internacionales de Contabilidad (NIC's)**. México: 4ta. Edición 199.7

KSHETRI, N. (2006) The simple economics of cybercrime. IEEE Security & Privacy. January/February.

MCKEMMISH, R. (1999) What is forensic computing?. Australian Institute of Criminology. Issues and Trends in crime and criminal justice. No. 118.

Méndez A. Carlos E. **Metodología .** Colombia, Bogota: 2da Edición: Magraw−Hill Internacional, S.A., 1995.

Perth, Western Australia. November. WHITE, D., REA, A., MCKENZIE, B y GLORFLED, L. (2004) A model and guide for an introductory computer security forensic course. Proceedings of the Tenth Américas Conference on Information Systems, New York, New York, August.

República Dominicana, Contraloría General de la República Dominicana. **Sistema de Contabilidad Gubernamental**, Santo Domingo: Edición Alfa & Omega, 1997. 5−7p.

República Dominicana, Contraloría General de la República Dominicana, **Normas Internas de Auditoría Gubernamental,** Santo Domingo: Edición Alfa & Omega, 1997, 4p.

República Dominicana, Contraloría General de la República Dominicana, **VI Seminario Latinoamericano de Contadores y Auditores (SELACA),** Santo Domingo: Editora Corripio C. por A. 2001, 221p.

República Dominicana, Contraloría General de la República. **Aspectos Básicos de la Contabilidad y Auditoría Municipal,** Santo Domingo: Editora de Luxes, S.A. 2000. 13−17 p.

República Dominicana, Instituto de Contadores Público Autorizados de la República Dominicana (ICPARD)**. La Corrupción Gubernamental**. Santo Domingo: Editora Servicios Gráficos Integrados, 1987. 195p.

República Dominicana, Dirección General de Impuestos Internos. **Código Tributario de la República Dominicana.** Santo Domingo: Editora Corripio C. por A. 2000 4−7p.

Silei Gaton, Jose A. **Instituciones de Derecho Público.** Santo Domingo: Editora Centenario.1999 565.p

Soriano Guzmán, Genaro. Control Gubernamental **Contaduría** (Santo Domingo): 19 (2000), 6p.

SUNDT, C. (2006) Information security and the law. Information Security Technical Report. Vol.2 No.9

TAYLOR, R., CAETI, T., KALL LOPER, D., FRITSCH, E y LIEDERBACH, J. (2006) Digital crime and digital terrorism. Pearson Prentice Hall. Cap. 11 y 12.

Waldis Taveras. **Legislación Municipal de la República Dominicana**. Santo Domingo: Editora Corripio, C. Por A. 1997.

Whittington, Ray y Pany Kart, **Auditoría Un Enfoque Integral.** Colombia, Bogota: Edición: Magraw−Hill Internacional, S.A., 1999. 9p.

WILSON, A. (2003) Investigation by computer. Digital evidence - data in the box!. Association of Certified Fraud Examiners. Proceedings of 14th Annual Fraud Conference. Chicago, IL. August.

Paginas Consultadas

http://pdf.rincondelvago.com/auditoria-forense_1.html

http://www.forensics-intl.com/art12.html
http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm
http://www.ioce.org/ioceprinc.shtml
http://www.forensics-intl.com/def6.html
http://www.forensics-intl.com/def7.html
http://www.forensics-intl.com/def8.html
http://www.forensics-intl.com/def3.html
http://www.encase.com/html/how_encase_works.html
http://www.keylogger.com/
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm
Janet Reno, U.S. Attorney General, Oct 28, 1996
http://www.cert.org/stats/cert_stats.html
http://www.softmart.com/connected/Spring2001/forensics.htm
http://www.itl.nist.gov/div897/docs/computer_forensics_tools_verification.html
http://www.softmart.com/connected/Spring2001/forensics2.htm
http://www.softmart.com/connected/Spring2001/forensics.htm
http://www.computer-forensics.com/products/welcome.html?peru.html
http://www.compukirk.com/kk00010.html
http://www.usdoj.gov/criminal/cybercrime/search_docs/sect3.htm
http://www.cdrfaq.org/faq07.html#S7-8
http://www.itworld.com/Career/1969/ITW0302weinstein/
http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm
http://www.auscert.org.au/Information/Auscert_info/Papers/win-UNIX-system_compromise.html
http://www.terra.com.co/
http://www.khaleejtimes.com/uae.htm#story1
http://www.readrite.com/html/magbasic.html
http://www.dss.mil/isec/nispom.htm
http://www.dss.mil/infoas/magnetic_tape_degaussing.doc
http://www.dss.mil/infoas/clearing_and_sanitization_matrix.doc
http://rs121.rapidshare.com/files/29699844/EnCase.zip
http://www.internet-solutions.com.co/encase.php
http://www.criptored.upm.es/guiateoria/gt_m142y.htm
http://www.contraloria.gov.do/
http://www.respondanet.com/spanish/admin.financiera/auditoría/smithp1/repdomin/do05.pdt
http://www.respondanet.com/RD/actuales/gobierno/plan_nacional.pdf
www.google.com
www.yahoo.com
http://es.wikipedia.org/wiki/C%C3%B3mputo_forense
http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:idoneidad&ei=ewOgS5uCH5CcsgPh4YmLCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE
http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:Esterilidad&ei=7wOgS52AKoXcsgOwmtHnCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE
http://www.iuriscivilis.com/2008/12/letra-d.html
http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:salvaguarda&ei=WwWgS7KaM5HQtAOC5eSKCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE

http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:previsibilidad&ei=FwagS8CBNJDkswOf4eTkCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE
http://www.monografias.com/trabajos74/conceptos-terminos-admin-empresas/conceptos-terminos-admin-empresas2.shtml
http://diccionarios.astalaweb.com/Local/Diccionario%20de%20deporte.asp
http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:inherente&ei=AwmgS7rIAorWsQOy3amvCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE
http://www.seguridadinformatica.dcyc.ipn.mx/glosario.html
http://www.cnbv.gob.mx/recursos/Glosario1P.htm
http://www.iuriscivilis.com/2009/06/diccionario-juridico-letra-p.html
http://es.wikipedia.org/wiki/Incidente
http://es.wikipedia.org/wiki/Fraudulento
http://www.google.com.mx/search?hl=es&lr=lang_es&defl=es&q=define:deterioro&ei=7A2gS7GhC43wsgOxyvnWCw&sa=X&oi=glossary_definition&ct=title&ved=0CAYQkAE
http://www.wordreference.com/definicion/concerniente
http://www.emprendedoresucu.com/diccionario.htm
http://www.leyes.com.py/documentaciones/diccionarios/terminos%20aduaneros/index.php?ver=d

Anexos

Anexos

Es una página que constituye un tipo de información de soporte enciclopédico, que aporta información relacionada con artículos, pero que no es un artículo en sí mismo.

Son secciones relativamente independientes de una obra que ayudan a su mejor comprensión y que permiten conocer más a fondo aspectos específicos que por su longitud o su naturaleza no conviene tratar dentro del cuerpo principal. Son elementos accesorios que pueden interesar tal vez a algunos lectores, o que conviene incluir para dar una información más completa sobre los temas tratados pero que, en definitiva, resultan de algún modo prescindibles. Esto último no implica que deban ser desdeñados como agregados sin importancia; por el contrario ellos son, muchas veces, un elemento enriquecedor del discurso principal que hace que éste cobre mayor relieve, sea comprendido más a fondo o pueda ser objeto de subsiguientes investigaciones.

Cuestionario

Este formato es el que se pretende aplicar a la población seleccionada, pero es tentativo ya que se agregaran mas preguntas.

1.- ¿Considera usted que la adquisición de la evidencia electrónica se debe hacer siempre de forma que el sistema examinado se vea modificado en lo más mínimo?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

2.- ¿La aplicación de este proceso puede ser utilizado como evidencia en un proceso legal?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

3.- ¿El desconocimiento de este proceso puede ocasionar perjuicios innecesarios a la persona/entidad investigada?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

4.- ¿Consideraría como una opción la adquisición de software para evitar la pérdida o alteración de información?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

5.- ¿Se debe contar con personal capacitado y con cierto grado de conocimientos en el tema para un adecuado manejo de la evidencia y evitar la pérdida de datos?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

6.- ¿Estaría dispuesto a implementar programas de recolección de evidencia para prevenir posibles ataques?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

7.- ¿La utilización de este proceso nos ayudaría a obtener los datos claves para la investigación y para un posible juicio?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

8.- ¿Considera que al utilizar estas técnicas en una red podríamos saber donde se localiza la computadora y si el archivo fue enviado desde ahí?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

9.- ¿Al implementar estas técnicas se podrá encontrar evidencias de fraudes, como hojas financieras, e-mail o alguna evidencia de una naturaleza particular?

(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

10.- ¿Consideraría como una opción la implementación de la informática forense para evitar posibles fraudes?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no

11.- ¿Se pude considerar piratas informáticos nada más a las personas externas a la empresa o también empleados de ésta que usan Internet para robar o dañar?
(5)Definitivamente sí (4) Probablemente sí (3) Indeciso
(2) Probablemente no (1) Definitivamente no