Primer Congreso Estudiantil de Investigación del Sistema Incorporado 2013
"Para estimular la creatividad científica y humanística"
Ciclo escolar 2012-2013

IMPORTANCIA DE LA INFORMÁTICA FORENSE

Área de Conocimiento: Ciencias Fisicomatemáticas y de las Ingenierías.
Disciplina: Computación y Tecnologías de la Información.
Tipo de Investigación: Documental
Proyecto: CIN2012A20149

Institución: CENTRO UNIVERSITARIO MÉXICO AC (1009)

Autores: Colmenares Mendoza Alberto Yesid
Cruz Guzmán Diego

Asesor: M.A. Aarón Gordillo Ramírez

Febrero 2013.

RESUMEN

La informática forense se encarga de investigar los procesos mediante los cuales se pudieron haber cometido un crimen mediante dispositivos electrónicos con el fin de descubrir y analizar la información disponible, suprimida u ocultada y que ésta a su vez pueda servir como evidencia en un asunto legal. Se pueden reconstruir hechos en caso de que se haga un mal uso de ellos. Hoy en día las empresas necesitan cada día más seguridad para sí mismos y por medio de la informática forense, en cualquier intento de delito, se puede llegar a los procesos que se hicieron y recuperar los archivos que se tenían en un principio. Es por eso que se vuelve tan importante la protección de datos tanto en empresas como datos personales, en redes sociales o cualquier otro ámbito para no tener problemas con los llamados "hackers" o que puedan robar la identidad de una identidad por internet. Las distintas metodologías forenses incluyen la captura segura de datos de diferentes medios digitales y evidencias digitales, sin alterar la información de origen. Se han encontrado hallazgos en diferentes áreas dado que los eventos se dan en diferentes maneras como entrar a una pagina privada y gracias a un método llamado SMART y LINRes lograron detectar a los hackers y pudieron reforzar su programa a tiempo para algún otro incidente.

Palabras Clave:
Informática, Forense, Evidencias, Analizar, Métodos, Crimen, Empresas, Juzgados, Dispositivos Electrónicos, Red, Amenazas, Explorador, Herramientas.

ABSTRACT

Computer forensics has the commission to investigate the process where it might be commited a crime through electronic mechanisms to discover and analyze the available, abolished or hidden information and that can be an evidence in a legal matter. The incidents can be restored in case that it has a bad use of it. Nowadays, companies needs more security than they had ever had, through computer forensic, any type of crime, can get into the process which people used to do it and

restore the things that were damaged. That´s why data protection is becoming too important in companies as personal data or in social networks and do not have any problem with "hackers" or that someone could rob someone´s identity. Different forensic methodologies includes secure data capture from different digital media and digital evidence without modifying the source of the information. There have been sordid in different areas where people had hacked some pages and through methods as SMART and LINRes they have detected the people who were in that crime and also reinforce their program for another incidents.

Keywords:
Computing, Forensic Evidence, Analysis, Methods, Crime, Business, Courts, Electronic Devices, Network Threats, Explorer, Tools.

INTRODUCCIÓN

El valor de la información en nuestra sociedad, es cada vez más importante para el desarrollo de negocio de cualquier organización. Derivado de este aspecto, la importancia de la Informática forense adquiere cada vez mayor trascendencia. Desde que apareció Internet, uno de sus principales objetivos está relacionado con su uso en las empresas y otras instituciones no comerciales, pero tan importante como conocer sus beneficios es también entender los riesgos inherentes a la seguridad, cuando se implementa esta tecnología. Con el objetivo de reducir en porcentaje este problema, es que aparece una nueva modalidad llamada "Informática Forense", que permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos.(S/A, 2012)

Mediante los procedimientos de la informática forense se identifican, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal; y de la misma manera, mediante el uso de ésta, podemos reconstruir hechos por medio de dispositivos electrónicos en caso de un mal uso de la tecnología. (Pérez, 2013)

Las distintas metodologías forenses incluyen la captura segura de datos de diferentes medios digitales y evidencias digitales, sin alterar la información de origen.

Si utilizamos la informática forense, entonces podemos reconstruir hechos por medio de dispositivos electrónicos en caso de un mal uso de la tecnología. Al igual, por medio de la informática forense podemos rastrear cualquier intento de sobrepasar la protección de datos y llegar al responsable. La Informática Forense sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información y consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

¿QUÉ ES LA INFORMÁTICA FORENSE?

Empezamos por definir qué es informática y por otro lado qué es forense. Informática es el conjunto de conocimientos científicos y métodos que permiten analizar, mejorar e implementar actualizaciones a la comunicación, envío y recepción de información a través de los ordenadores. Por otro lado, tenemos que forense es la aplicación de prácticas científicas dentro del proceso legal, es decir, existen investigadores altamente especializados o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios.

Entendemos que ciencia forense es la aplicación de prácticas científicas dentro del proceso legal; es decir, es un conjunto de ciencias que la ley usa para atrapar a un criminal, ya sea físicamente, química, matemáticamente u otras más. (Beatriz, 2007)

La Informática Forense es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir y de analizar información disponible, suprimida, u ocultada que puede servir como evidencia en un asunto legal. (Miranda, 2008)

De acuerdo con el FBI, la informática forense se define como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Dentro del campo de la informática forense encontramos varias definiciones:

- Computación Forense: que se entiende como el proceso de aplicar técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal. Procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. (Gutiérrez, 2006)
- Forensia en redes: la forensia en redes se dedica a capturar, registrar, almacenar y analizar los eventos de la red, con el fin de determinar la fuente de uno o varios ataques a la red. O las posibles vulnerabilidades existentes en ella. (Camona, 2012)

PRINCIPIO DE INTERCAMBIO DE LOCARD

Dentro de los fundamentos de la informática forense nos encontramos con el principio de transferencia de Locard que dice que cualquiera o cualquier objeto que haya estado implicado en la escena del crimen, deja un rastro en la escena o en la víctima y viceversa, es decir, "cada contacto deja un rastro". En el mundo real significa que si una persona pisara la escena del crimen dejará algo suyo ahí, pelo, sudor, huellas, etc. Pero también se llevará algo conmigo cuando abandone la escena del crimen, ya sea un olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

Este principio establece en esencia, que cuando dos objetos llegan a tener contacto, el material de ambos es transferido entre ellos.

Los investigadores de la escena del crimen se refieren a posibles transferencias.

Esto ocurre por ejemplo, después que un carro golpea algo o cuando un investigador examina un cuerpo y localiza material que pareciera que está fuera de lugar.

Este mismo principio se puede aplicar a la realidad digital como por ejemplo cuando existen dos o más computadoras y éstas se transfieren datos o archivos vía red y así la información es intercambiaba y manipulada entre ellas. Halan Carvey (2009)

TIPOS DE EVIDENCIAS

Tenemos 4 tipos de evidencias:

- Evidencia transitoria: es un tipo que como su nombre lo indica, dura un tiempo determinado y no es para siempre, es temporal. Algunos ejemplos son que puede haber tierra, una temperatura diferente, un olor, etc.
- Evidencia condicional: éstas son causadas por un evento o una acción dentro de la escena del crimen. Como si pudiera estar dentro de la escena del crimen una ventana abierta, una bala, armas blancas, etc.
- Evidencia curso o patrón: son las cuales son producidas por un contacto como cuando una bala atraviesa el cuerpo, una ventana se encuentra rota, una televisión encendida, etc.
- Evidencia transferida: se refiere, como su nombre lo indica, a que son producidas por un contacto, se "transfieren" y puede ser entre personas u objetos. Existen dos tipos de evidencia transferida:
    a. Por rastro: puede haber sangre, pelo, semen, etc.
    b. Por huella: pueden ser huellas de zapato, una marca de una mano en alguna parte, etc.

EVIDENCIAS DIGITALES

Las evidencias digitales recabadas permiten elaborar un dictamen fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas. Gracias a este proceso, la informática forense aparece como una "disciplina auxiliar" de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad utilizando la "evidencia digital". La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada y al extenso uso de computadores por parte de las compañías de negocios tradicionales. Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

Las evidencias digitales son todos aquellos datos e información almacenados o transmitidos en formato electrónico que pueden tener valor probatorio en un procedimiento legal. Correos electrónicos, documentos, fotografías digitales, archivos de video o audio, blogs de eventos o históricos son algunos ejemplos de lo que podría ser evidencias digitales. (Andrés Velázquez, febrero 2012)

Es cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar un enlace entre un crimen y su víctima o un crimen y su autor. (Casey, 2006)

De acuerdo con el HB:171 2003 Guidelines for the Management of IT Evidence, 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.

CRITERIOS DE ADMISIBILIDAD

Los criterios de admisibilidad son los requisitos mínimos que deben cumplirse para que una candidatura sea considerada admisible. Los criterios de la admisibilidad deben ser conformes con los requisitos administrativos establecidos para cada convocatoria de proyectos, independientemente del contenido y de la calidad de los mismos. Deben ser contestados con un rotundo sí o no, que no permita ninguna posibilidad de interpretación.

Existen cuatro criterios que se deben tener en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia en las legislaciones modernas:

- Autenticidad: la autenticidad no es otra cosa más que obrar conforme al propio ser. Una evidencia digital será auténtica únicamente si dicha evidencia ha sido generada y registrada en el lugar de los hechos.
- Confiabilidad: se define como la capacidad que tiene un producto de realizar su función de la manera prevista sin incidentes por un período de tiempo determinado y bajo condiciones indicadas. Una prueba digital es confiable si el sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba.
- Completitud: es la propiedad que tiene un sistema lógico por la que cualquier expresión cerrada es derivable o refutable dentro del mismo sistema. Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa.
- Apego y respeto por las leyes: la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país.

(Zuccardi, 2006)

MANIPULACIÓN DE LA EVIDENCIA DIGITAL

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital:

1. Asegurarse de que los procedimientos a seguir son idóneos para dar certeza sobre la autenticidad y no alteración de la evidencia, sobre la confiabilidad de los programas de computadora que generaron tales registros de evidencia, sobre la fecha y hora de la creación de los mismos, sobre la identidad de su autor y por último sobre la fiabilidad del procedimiento para su custodia y manipulación. (Ajoy, G. 2004).
2. Recolectar información de forma adecuada desde una perspectiva forense.
3. Establecer procedimientos para la custodia y retención seguras de la información obtenida. Esto podría lograrse llevando registros de acceso y manipulación realizada a la información que se pretende usar como prueba (Ajoy, G. 2004).
4. Determinar si se está manipulando registros originales o copias de los mismos. Así mismo, sería pertinente documentar apropiadamente cualquier tipo de acción tomada sobre los registros de evidencia. En este aspecto.
5. Por último, se hace hincapié en que el personal comprometido en los procesos de producción, recolección, análisis y exposición de la evidencia debe tener un entrenamiento apropiado, experiencia y calificaciones para cumplir sus roles.

GESTIÓN DE LA EVIDENCIA DIGITAL

Existen gran cantidad de guías y buenas prácticas que nos muestran como llevar acabo la gestión de la evidencia digital

Las guías que se utilizan tienen como objetivo identificar evidencia digital con el fin de que pueda ser usada dentro de una investigación. Estas guías se basan en el método científico para concluir o deducir algo acerca de la información. Presentan una serie de etapas para recuperar la mayor

cantidad de fuentes digitales con el fin de asistir en la reconstrucción posterior de eventos. (Zuccardi, 2006)

PROCEDIMIENTOS DE INFORMÁTICA FORENSE

Siendo especialista en informática forense, se es necesario precisar las medidas de seguridad y control que se deben tener a la hora de hacer sus labores.

Algunos elementos que se deben considerar para el procedimiento forense son:

1. Esterilidad de los medios informáticos de trabajo.
   Esta es una condición fundamental para el inicio de un procedimiento forense en informática ya que si existe un instrumental contaminado, puede ser causa de una interpretación o análisis erróneo.
2. Verificación de las copias de los medios informáticos.
   Las copias que fueron efectuadas en los medios previos, deben ser idénticas al original. La verificación debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia y es preciso que el software o la aplicación soporte de la operación ya haya sido probado y analizado por la comunidad científica para que sea válido en un procedimiento ante una diligencia legal.
3. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.
   La persona que hace la investigación debe ser la misma que sea responsable del proceso. Debe conocer cada uno de los pasos realizados, herramientas utilizadas, resultados de análisis, y todo claramente documentado para que cualquier persona diferente pueda revisar dichos datos.
4. Mantenimiento de cadena de custodia de las evidencias digitales.

Va ligado al tercer punto. Se debe documentar cada uno de los eventos que se hayan realizado con la evidencia en su poder como quién la entregó, cuándo se entregó, entre otras cosas.

5. Informe y presentación de los análisis de los medios informáticos.

   Pueden presentarse falsas expectativas cuando existe una inadecuada presentación de los resultados. Los elementos críticos a la hora de defender un informe de las investigaciones son: la claridad del uso del lenguaje, una buena redacción sin juicios de valor, y una ilustración pedagógica de los hechos y resultados.

   Existen dos tipos de informes: técnicos, con los detalles de una inspección realizada; y ejecutivos, para la gerencia y sus dependencias.

6. Administración del caso realizado.

   Mantener un sistema automatizado de documentación de expedientes con una cuota de seguridad y control, es necesario para salvaguardar los resultados con el debido cuidado y los investigadores deben prepararse para declarar ante un jurado.

7. Auditoría de los procedimientos realizados en la investigación.

8. El profesional debe mantener un ejercicio de autoevaluación de sus procedimientos y así contar con la evidencia de una buena práctica de investigaciones forenses y hacer el ciclo de calidad: PHVA

   Planear, Hacer, Verificar y Actuar. (García, 2013)

FINES Y OBJETIVOS

La informática forense tiene 1 Objetivo General y 4 Objetivos Particulares de acuerdo a (Arias Chaves, Michael, 2006)

Objetivo General:

Protección de Datos tanto en empresas como datos personales o en redes sociales y cualquier otro ámbito.

Objetivo particular:

La compensación de los daños causados por los criminales o intrusos: esto llega a ser demasiado peligroso ya que los criminales cuando dañan a las personas llegan a perder el control y suelen dejar marcas que ayuden a la informática forense a averiguar los daños y llegar más rápido al que lo hizo.
La persecución y procesamiento judicial de los criminales: La Informática Forense se encarga de determinar las evidencias para poderles imputar cargos.

La creación y aplicación de medidas para prevenir casos similares: Aquí se encarga de generar programas, para que el mismo programa que este dañado se pueda arreglar y tenga mucho más seguridad.

La utilización de la informática forense con una finalidad preventiva: Esto se hace con el fin de que los intrusos o bromistas quieran llegar a meterse a una cuenta privada o algún programa de seguridad nacional y los quiera hachear y el informático forense los detecte a tiempo y pueda atacarlos o la vez componer el programa para que no sea tan sencillo meterse.

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

LAS EVIDENCIAS FORENSES

Según (Lic. Zajaczkowski Enrique, 2005) cuando se ha cometido un crimen, el delincuente deja con frecuencia señales sobre sus vestidos, sus zapatos o su cuerpo. Los indicios de esta clase son valiosos y, normalmente, el criminal no percibe su significado por esta razón le es difícil defenderse contra ellos. Algunas veces no tiene idea de que los lleva sobre sí.

Es de la mayor importancia que el investigador considere siempre las posibilidades de prueba ofrecidas por tales indicios, y los busque y conserve con el mayor cuidado.

El valor del indicio depende con frecuencia de la naturaleza del lugar del crimen, así como del tipo de este crimen. Vamos a dar una idea de estas pruebas según las diferentes circunstancias.
En ellas se incluyen:

1. Polvo característico del escenario del crimen o de sus alrededores.
2. Porciones de materia vegetal del exterior del lugar del crimen.
3. Trozos de cristal, vidrio, astillas de madera, manchas de pintura, etc.
4. Marcas de explosión o de relleno de cajas fuertes, (Fracturas de cajas fuertes).
5. Partículas de virutas metálicas, gotas de metal fundido o lana de vidrio (apertura de cajas fuertes, con soplete oxiacetilénico).
6. Marcas de tierra, pintura, grasa, polvo de ladrillo, yeso, lápiz de labios, polvos faciales, etcétera.
7. Manchas de sangre que puede estar en fragmentos casi invisibles a la vista, así como semen.
8. Partículas de tejidos, pelo y plumas.
9. Fibras textiles (en zapatos) de alfombras y esteras.

Por otra parte hay recolección de evidencia forense

Los equipos envasados en cajas de SIRCHIE vienen sellados de fábrica para garantizar su integridad. SIRCHIE envuelve en plástico termo-retráctil cada equipo envasado en caja para reforzar su integridad y protección durante el envío, desde la fábrica hasta llegar a sus manos. Esta doble integridad significa que se asegura doblemente que su equipo no ha sido adulterado antes de utilizarlo. Ofrece una amplia gama de Equipos de Recolección de Evidencia Forense para satisfacer las necesidades de agencias encargadas del cumplimiento de la ley, instalaciones médicas y laboratorios privados. Los equipos están diseñados y fabricados para ofrecer:

- Alta calidad
- Funcionalidad
- Variedad
- Valor

Nuestros equipos están diseñados para estandarizar la recolección y la identificación de muestras para análisis de laboratorio. Los procedimientos de unidad limpia de nuestras instalaciones garantizan la integridad y precisión de cada equipo que producimos. Ofrece Equipos de Recolección de Evidencia Forense para los siguientes tipos de muestras de evidencia:

- Evidencia de asalto sexual
- Evidencia de ADN
- Recolección de muestras de sangre
- Recolección de evidencia de alcohol en la sangre

Indague con el laboratorio que realiza los análisis para su compañía para decidir cuál equipo se adapta mejor a sus necesidades. se especializa en producir Equipos de Recolección de Evidencia Forense personalizados. Sugerimos a las agencias que envíen sus requerimientos para ofrecerles una cotización.

EL PROCESO DE LA INFORMÁTICA FORENSE

Según Cano Martínez. (2006) la investigación forense tenga validez es necesario que cumpla con ciertas normas y leyes, ya sea a nivel legal o corporativo. En este sentido la ciencia forense provee de ciertas metodologías básicas que contemplan el correcto manejo de la investigación y de la información.

La IOCE, publicó "Guía para las mejores prácticas en el examen forense de tecnología digital" (Guidelines for the best practices in the forensic examination of digital technology). El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Su estructura es:

a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b) Determinación de los requisitos de examen del caso.
c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d) Prácticas aplicables al examen de la evidencia de digital.
e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia

y empaquetado, etiquetado y documentación.

f) Priorización de la evidencia.

g) Examinar la evidencia: protocolos de análisis y expedientes de caso.

h) Evaluación e interpretación de la evidencia

i) Presentación de resultados (informe escrito).

j) Revisión del archivo del caso: Revisión técnica y revisión administrativa.

k) Presentación oral de la evidencia.

l) Procedimientos de seguridad y quejas.

De toda esta estructura se puede rescatar en general 4 fases principales:

1) Recolección de la evidencia sin alterarla o dañarla.

2) Autenticación de la evidencia recolectada para asegurar que es idéntica a la original.

3) Análisis de los datos sin modificarlos.

4) Reporte final.

Ya que con estas fases damos finalización al proceso forense y es en las 4 que se pueden rescatar más información de lo que se haya hecho, gracias a esto se han podido rescatar o salvar cualquier tipo de situaciones en la vida que intenten hacer mal uso de ellas o hacer algún daño a la sociedad.

MODELOS

Hay tipos de modelos según Arquillo Cruz, (2007) dependendiendo la investigación que vayas a hacer o cual escoja el investigador.

Estos son algunos modelos que propone:

MODELO DE CASEY (2000)

Eoghan Casey, en el año 2000 presenta un modelo para procesar y examinar evidencias digitales. Este modelo ha ido evolucionando en las siguientes Tiene los siguientes pasos principales: 18 Herramienta de apoyo para el análisis forense de computadoras.

1. La Identificación
2. La Conservación, la Adquisición, y la documentación
3. La clasificación, la comparación, y la individualización
4. La reconstrucción

En los últimos dos pasos es cuando la prueba es analizada. Casey señala que éste es un ciclo de procesamiento de prueba, porque al hacer la reconstrucción pueden hallarse pruebas adicionales que provoquen que el ciclo comience. El modelo se replantea primero en términos de sistemas de cómputo sin tener en cuenta la red, y luego ejercido para las distintas capas de red (desde la capa física hasta la capa de aplicación, e incluyendo la infraestructura de la red) para describir investigaciones en redes de computadoras. El modelo de Casey es muy general y se aplica exitosamente para ambos sistemas, las computadoras aisladas y con entornos de red.

MODELO PUBLICADO POR EL U.S. DEP. OF JUSTICE (2001)

Este modelo se publicó en el año 2001 y quizás sea el más sencillo.
Básicamente existen cuatro elementos clave en un análisis forense de computadoras, que son:

1. Identificación
2. Conservación

3. Análisis
4. Presentación

Este modelo supuso una de las grandes bases en este campo ya que a partir de estos conceptos clave, varios autores han desarrollado sus modelos para englobar todos los pasos de una investigación forense de computadoras.

MODELO DE LEE (2001)

Lee propone la investigación como un proceso. Este modelo se ocupa sólo de investigación de la escena de delito, y no del proceso investigador completo. Identifica cuatro pasos dentro del proceso:

- Reconocimiento
- Identificación
- Individualización
- Reconstrucción

El reconocimiento es el primer paso, en el cual se buscan ítems o patrones como pruebas potenciales.

La identificación de los tipos diversos de prueba es el siguiente paso. Esto implica la clasificación de la prueba, y una subactividad, la comparación. Físicas, biológicas, químicas, y otras propiedades de los artículos de prueba son comparadas según los estándares conocidos.

La individualización se refiere a determinar si los ítems de prueba posible son únicos a fin de que puedan ser conectados con un acontecimiento o individuo particular.

La reconstrucción implica unificar el significado de las salidas de las anteriores partes del proceso, y cualquier otra información pertinente que los investigadores pudieron haber obtenido, para proveer una detallada relación de los acontecimientos y las acciones en la escena de delito.

MODELO DEL DFRWS (2001)

El primer Forensics Digital Research Workshop (Palmer, 2001) produjo un modelo que muestra los pasos para el análisis forense digital en un proceso lineal. Los pasos
son los siguientes: 20 Herramienta de apoyo para el análisis forense de computadoras

1. La identificación
2. La preservación
3. La colección
4. El examen
5. El análisis
6. La presentación
7. La decisión

El modelo no pretende ser el definitivo, sino más bien como una base para el trabajo futuro que definirá un modelo completo, y también como una armazón para la investigación de futuro. El modelo DFRWS se replantea como lineal, pero la posibilidad de retroalimentación de un paso para los previos es mencionada. El informe DFRWS no discute los pasos del modelo con todo lujo de detalles sino por cada paso se listan un número de asuntos pendientes.

MODELO DE REITH, CARR Y GUNSCH (2002)

Reith, Carr y Gunsch (2002) describen un modelo que hasta cierto punto deriva del modelo DFRWS. Los pasos en su modelo son:
1. La identificación 2. La preparación 3. La estrategia de acercamiento
4. La preservación 5. La colección 6. El examen 7. El análisis
8. La presentación 9. Devolviendo la evidencia
Este modelo es notable en cuanto a que explícitamente pretende ser un modelo abstracto aplicable para cualquier tecnología o cualquier tipo de ciberdelito. Se pretende que el modelo pueda ser utilizado como base otros métodos más detallados para cada tipo específico de investigación.

MODELO INTEGRADO DE BRIAN CARRIER Y EUGENE SPAFFORD (2003)

Brian Carrier y Eugene Spafford han propuesto otro modelo que organiza el proceso en cinco grupos, cada uno dividido en 17 fases.

Fases de Preparación

El objetivo de esta fase es asegurar que las operaciones e infraestructuras están preparadas para soportar una investigación completa. Incluye dos fases:

• Fase de preparación de operaciones: que asegura que los investigadores están adiestrados y equipados para tratar con un incidente cuando este ocurre. 22 Herramienta de apoyo para el análisis forense de computadoras
• Fase de preparación de infraestructuras: que asegura que la infraestructura subyacente es suficiente para tratar con incidentes. Por ejemplo, cámaras fotográficas, material de conservación y transporte de hardware, etc.

Fases de Despliegue

El propósito es proporcionar un mecanismo para que un incidente sea detectado y confirmado. Incluye dos fases:

1. Fase de Detección y Notificación: donde el incidente es detectado y y notificado a las personas apropiadas.
2. Fase de Confirmación y Autorización: en la cual se confirma el incidente y se obtiene la aprovación legal para llevar a cabo la búsqueda.

Fases de Investigación Física de la escena del crimen

La meta de estas fases es recopilar y analizar las evidencias físicas y reconstruir las acciones que ocurrieron durante el incidente. Incluye seis fases:

1. Fase de Conservación: que busca conservar la escena del crimen de modo que la evidencia pueda ser identificada más tarde y recolectada por personal adiestrado en identificación de evidencias digitales.
2. Fase de Inspección: que requiere que un investigador recorre la escena física del delitto e identifique elementos de evidencia física.
3. Fase de Documentación: que incluye tomar fotografías y videos de la escena del delito y de la evidencia física.
4. Fase de búsqueda y recolección: que entraña una búsqueda y recolección en profundidad de la escena de modo que se identifican evidencias físicas adicionales y se establecen vías para comenzar la investigación digital.
5. Fase de Reconstrucción: que incluye organizar los resultados del análisis hecho usándolos para desarrollar una teoría del incidente.
6. Fase de Presentación: que presenta la evidencia digital y física en un juicio o ante la dirección de una empresa.

Fases de Investigación de la Escena Digital del Delito

El objetivo es recolectar y analizar la evidencia digital que se obtuvo de la fase de investigación física y a través de otras fuentes. Incluye fases similares a las de la investigación física, aunque en este caso el objetivo principal es la evidencia digital. Las seis fases son:

1. Fase de conservación: que conserva la escena digital del delito de modo que la evidencia pueda ser después analizada.
2. Fase de Inspección: por la que el investigador transfiere los datos relevantes de una jurisdicción que está fuera del control físico o administrativo del investigador, a una posición controlada.
3. Fase de Documentación: que incluye documentar la evidencia digital cuando es encontrada. Esta información es útil en la fase de presentación.
4. Fase de Búsqueda y Recolección: se realiza un análisis en profundidad de la evidencia digital.
5. Fase de reconstrucción: que incluye ubicar las piezas del puzle y desarrollar una hipótesis investigativa.
6. Fase de Presentación: que consiste en presentar la evidencia encontrada y unirla a la evidencia física encontrada.

Fase de revisión

Esto conlleva una revisión de la investigación entera e identifica áreas de mejora.

MODELO MEJORADO PROPUESTO POR VENANSIUS BARYAMUREEBA Y FLORENCE TUSHABE (2004)

Este modelo se basa en el anterior e intenta mejorar algunos aspectos, aunque básicamente son muy similares. Este modelo consiste en cinco fases principales:

Fases de Preparación Las mismas que para el modelo anterior.

MODELO EXTENDIDO DE SÉAMUS Ó CIARDHUÁIN (2004)

En el año 2004, el IJCE (International Journal of Digital Evidence) publica un modelo extendido para investigaciones de ciberdelitos, cuyo autor fue Séamus Ó Ciardhuáin.

Las actividades en una investigación se mencionan a continuación:

1. La conciencia 2. Autorización 3. Planificación 4. La notificación 5. Buscar e identificar pruebas 6. La colección de prueba 7. Transporte de prueba 8. El almacenamiento de prueba 9. El examen de prueba 10. La hipótesis 11. La presentación de hipótesis 12. La prueba /defensa de hipótesis 13. La diseminación de información.

Este modelo tiene forma de cascada y las actividades se suceden unas a otras. Los flujos de información de una actividad a la siguiente pasan hasta el final del proceso de investigación. Por ejemplo, la cadena de custodia se forma por la lista de aquellos que han manipulado una evidencia digital y debe pasar de una etapa a la siguiente agregando los nombres en cada paso.

Estos son algunos de los modelos para cualquier investigación forense y sus pasos a seguir.

HERRAMIENTAS

Hay tipos de Herramientas según Arquillo Cruz, (2007) dependendiendo la investigación y modelo que vaya a utilizar el investigador.

Herramientas basadas en Linux

LINReS, de NII Consulting Pvt. Ltd.

LINReS es una herramienta de Primera Respuesta diseñada para ejecutarse en sistemas Linux sospechosos/comprometidos, con un mínimo impacto en el mismo para

satisfacer varios requerimientos estándar forenses. Esta herramienta ha sido probada con éxito en sistemas RedHat Linux.

Características principales:

Recoge información volátil y no volátil del sistema sospechoso
Recoge meta-datos de los ficheros del sistema sospechoso
Calcula los hashes de todos los ficheros del sistema sospechoso
Transfiere datos a través de la red usando conexiones de Netcat persistentes

SMART, BY ASR DATA

SMART es una herramienta software que ha sido diseñada y optimizada para dar soporte a los investigadores forenses y al personal de seguridad informática en la consecución de sus respectivas tareas y metas. SMART es más que un simple programa forense.
Las características de SMART le permiten ser usado en multitud de escenarios, incluyendo:
• Investigaciones de "Knock-and-talk" • Vista previa remota o in-situ de un sistema objetivo • Análisis post mortem • Testing y verificación de otros programas forenses
• Conversión de ficheros entre distintos formatos forenses
SMART es usado actualmente por: • Agentes de la ley Federales, estatales y locales en U.S.A. • Organizaciones militares y de inteligencia en U.S.A. • Empresas de contabilidad
• Investigadores forenses • Especialistas en recuperación de datos • Profesionales en recuperación de desastres • Profesionales de la seguridad informática • Profesionales de la privacidad en la asistencia sanitaria • Auditores internos • Administradores de sistemas

HERRAMIENTAS BASADAS EN MACINTOSH

MACINTOSH FORENSIC SOFTWARE, DE BLACKBAG TECHNOLOGIES, INC.

The BlackBag Macintosh Forensic Software (BlackBag MFS) es un conjunto de herramientas independientes que dan al examinador el nivel más alto de flexibilidad permitido en el campo forense.

- Adquisición de imágenes
- BlackBag MFS soporta varios métodos de adquisición de imagen. Se recomienda usar "dd" dada su flexibilidad y fiabilidad. Los métodos soportados son: dd, iLook, Disk Copy y SafeBack.
- Analizar la imagen
- Un análisis se realiza mejor usando la misma plataforma en la que se encuentra la evidencia original.
- BlackBag Macintosh Forensic Software
- La siguiente lista representa las características principales dentro del conjunto de herramientas independientes de BlackBag MFS.
- Breakup simplifica la gestión de los directorios que contienen miles de imágenes, reduciendo un gran directorio a tamaños más pequeños y manejables.
- CommentHunter proporciona una rápida instantánea de la actividad de un sospechoso, introduciendo todos los comentarios sobre ficheros conocidos en un fichero fácil de leer.
- DirectoryScan muestra un listado de directorio de un volumen o directorio seleccionado.
- FileSearcher permite al examinador la búsqueda en el sistema de ficheros completo de una variedad de características diferentes, incluyendo nombres de fichero (extensiones), tipos de fichero, y codificación del creador.

MACFORENSICLAB, DE SUBROSASOFT

MacForensicsLab es un conjunto completo de herramientas forenses y de análisis en un paquete consistente.

• La seguridad lo primero - MacForensicsLab tiene mucho cuidado a la hora de asegurar la integridad de la evidencia.

• Logs detallados – Cada acción tomada mientras que se usa el software es almacenada en logs altamente detallados para proporcionar al investigador la mayor cantidad posible de información.

• Informes del caso en HTML – Una combinación de datos del gestor del caso y de los ficheros logs (cronología, recuperaciones, análisis, adquisición, catálogos, favoritos, notas) puede ser exportada en un informe HTML para su visionado en cualquier navegador Web.

• Hashing flexible – Los procesos de adquisición de datos incluyen la utilización de hashes MD5, SHA1 y SHA256.

• Recuperar evidencias después de que un disco o dispositivo ha sido formateado - MacForensicsLab recuperará ficheros, hará búsquedas de cadenas y permitirá el análisis de las unidades formateadas recientemente.

• Recupera evidencias de medios corruptos – Se procesará cualquier dato intacto en el disco, y recuperará cadenas y ficheros enteros o parciales donde quiera que se encuentren.

• Trabaja con datos de otros sistemas operativos - MacForensicsLab está preparado para realizar adquisición de datos y análisis de unidades con Windows, Linux, y otros sistemas operativos.

• Proporciona métodos muy rápidos y fáciles para encontrar y marcar evidencias – con la herramienta "Browse", MacForensicsLab permite al investigador el visionado de ficheros en vista nativa a la vez que se recorre una estructura completa de directorios.

HERRAMIENTAS BASADAS EN WINDOWS

BRINGBACK DE TECH ASSIST, INC.

BringBack proporciona recuperación de
datos de sistemas operativos Windows ™ & Linux
(ext2), además de imágenes digitales almacenadas en tarjetas de memoria, etc.
Características:

• Disk Viewer – está diseñado para asistir a una persona experta en la valoración de las condiciones de un volumen. Proporciona búsqueda, navegación y visionado de los formatos más comunes.

• Los sistemas de ficheros soportados son FAT16, FAT32 y NTFS (todas las versiones)

• Proporciona soporte limitado para ext2 (sistema de ficheros Linux)

• Recupera hardware RAID0 y RAID5

• Motor de validación – comprueba ficheros en disco antes de recuperarlos para ver los que estar rotos y los que no.

La siguiente es la lista de formatos de fichero conocidos por la versión actual del motor de validación de datos (BringBackTM 2.1), en ningún orden en particular:

-Almacenamiento con estructura OLE :
Microsoft Word .doc
Microsoft Excel .xls José Arquillo Cruz 127
Microsoft Power Point .ppt
Windows Installer package .msi
o .exe, .dll, .cpl Módulo ejecutable Windows (Win32/PE format) o .ace archivo comprimido o .arj archivo comprimido o .asf video o .dbf formato de base de datos o.gif imagen o .gz archivo

comprimido gzip o .ico fichero icono Windows o .inf fichero INF Windows o .jpg, .jpeg imagen JPEG o .mid sonido MIDI entre otros.

• Recuperación de ficheros de imagen digital desde cámaras digitales

• Funciona sobre Windows NT/2000/XP/2003

• Puede ejecutarse desde un CD, por ejemplo, y no necesita escribir en el disco excepto por dos cosas:

1. Ficheros log opcionales (configurable)
2. Ficheros recuperados

ENCASE, BY GUIDANCE SOFTWARE

EnCase, desarrollada por Guidance Software Inc., permite asistir al especialista forense durante el análisis de un crimen digital.

Se trata 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: 128 Herramienta de apoyo para el análisis forense de computadoras

- Copiado Comprimido de Discos Fuente. Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen.
- Búsqueda y Análisis de Múltiples partes de archivos adquiridos. EnCase permite al examinador buscar y analizar múltiples partes de la evidencia.
- Diferente capacidad de Almacenamiento. Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz.
- 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 libre.
- Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de EMail. 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.
- 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.
- 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 DVDR.
- Vista de archivos y otros datos en el espacio Libre. 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 Libre.
- Integración de Reportes. EnCase genera el reporte del proceso de la investigación forense como un estimado.
- 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.

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

CONCLUSIONES

En la elaboración de este proyecto, aprendimos en cómo se hace una investigación con calidad y no como otras de las que mucha gente hace la mayoría de veces que dicen hacer un proyecto cuando en realidad sólo copian y pegan lo que encuentran y se tiene que hacer investigando cada tema a profundidad, comparando definiciones, buscando teorías, hechos pero no cualquiera, sino los que más llaman la atención o los más extravagantes dónde se diera a conocer el papel importante que ha jugado la informática forense en la historia.

Por lo tanto también concluimos que la elaboración de un proyecto no es solamente buscar y poner cosas sin saber de qué son, para empezar, se tuvo que tener conciencia acerca de qué es lo que significa cada palabra del proyecto y así empezamos a hacernos una amplia idea de los resultados que teníamos que obtener. De mejorar las cosas que aprendimos fue a cómo documentar un trabajo y en especial a trabajar en equipo, en investigar juntos y después ponernos de acuerdo en cómo tenía que ir quedando nuestro proyecto en cuanto a orden.

En este trabajo pudimos concluir en que la informática forense tiene un buen uso en la sociedad ya que cualquiera está expuesto a un fraude en línea o algun hacker de algun programa o documento personal que tengas en cualquier aparato electrónico o correos, y el informático forense puede ocupar un modelo y herramientas que le faciliten a encontrar al usuario que está tratando de afectar el documento.

Por último esta investigación nos llevó a la exploración de varios temas y noticias y tener una base más de conocimientos básicos de si algun dia nos pudiera llegar a pasar, al igual que pudimos aprender más sobre informatica forense que hasta ahorita no es muy conocida y se puede dar a conocer con el paso del tiempo a la sociedad.

REFERENCIAS

Pérez Gómez E. (S/F) ¿Qué es la informática forense o forensics?
Recuperado de: http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=121

Carvey Harlan (2009) Principio de intercambio de Locard
Recuperado de: http://www.nobosti.com/spip.php?article557

Sin autor (2008) Qué es la informática forense?
Recuperado de: http://www.informaticaforense.com/criminalistica/categoryblog/69-que-es-la-informatica-forense

Sin Autor (2012) Forensia en Redes
Recuperado de: http://forensiaredes.blogspot.mx/

Zuccardi G., Gutiérrez D. (2006) Informática Forense
Recuperado de:
http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Sin Autor (2013) Procedimientos de la informática Forense
Recuperado de: http://seguridadinformaticagarcia-s.wikispaces.com/Procedimientos+de+Informatica+Forense

Jeimy J. Cano M, (2006),Introducción a la informática forense,
Recuperado de: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

Panorama General De La Informática Forense Y De Los Delitos Informáticos, Vol. VII, Núm.12, 2006, pp. 141-154, Recuperado de: http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=66612867010.

Jose Arquillo Cruz, (Septiembre, 2007),"Herramientas de apoyo para el analisis forense de computadores", Recuperado de http://www.portantier.com/biblioteca/seguridad/analisis-forense.pdf