UN MIRADA A LA INFORMATICA FORENSE

Lozano González, Sol Verónica
Universidad Piloto de Colombia, Bogotá, Colombia
Sol.lozano@hotmail.com

I. Abstract

Thepresentarticle has as objectgive a briefintroductionontheforensic IT worldforitthefollowingtopicsweretreatingeachother: beginning, types of evidences, applications and hischallenges.

II. Resumen

El presente artículo tiene como objeto dar una breve introducción sobre el mundo de la informática forense para ellose trataran los siguientes temas: principios, tipos de evidencias, aplicaciones y sus desafíos.

Índice de Términos- delito informáticolos actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, hora UTC tiempo universal coordinado, línea de tiempo secuencia cronológica en la cual se demuestra la ocurrencia de los hechos, evidencia digital es la información en formato digital que pueda establecer una relación entre un delito y su autor.

III. Introducción

Los objetivos de la informática forense son: la identificación de las posibles fuentes, recolección de los diferentes tipos de evidencias, analizar las evidencias encontradas y la confirmación de los hechos a través de pruebas cruzadas.
La informática forense se ha convertido para los ingenieros en un campo de acción muy amplio con gran demanda de conocimientos, a la vez se ha convertido en un retopor los nuevos desarrollos de herramientas que permiten analizar las tecnologías existentes; cada nueva aplicación, sistema operativo o sistemas para analizar, es nuevo conocimiento que enriquece a los ingenieros que realizan los análisis forense.
Es una de las ramas que más demanda interacciones con las diferentes ramas de la ingeniería debido a la especialidad de conocimientos que requieren algunos casos.
La informática forense se ha convertido en una de las ramas auxiliares de la justicia Colombia brindando soporte en los casos que involucre delitos informáticos.

IV. Que 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. [1]

Complementado la definición anterior es una disciplina criminalista que tiene como objetivo lainvestigación en sistemas informáticos de hechos con relevancia jurídica o para la investigación privada. [2]

V. Principios de la informática forense

La IETF determinó que los principios rectores para la recolección de la evidencia digital son:

A. Respetar las leyes y aplicar las políticas de seguridad:

Dependiendo del país donde se desarrolle la investigación hay que cumplir normas o políticas de seguridad, las normas legales que se deben cumplir en Colombia en investigación forense son:

1) Código de procedimiento Civil

En la sección tercera Titulo XIII: Las decisiones judiciales deben fundarse únicamente en las pruebas que sean oportunamente allegadas a un proceso.
Deberán ceñir al asunto materia del mismo y que, el juez rechazará aquellas que sean legalmente prohibidas o ineficaces, impertinentes y/o superfluas: Certeza y convencimiento que debe otorgar al juez.[3]
Numeral 6 del artículo 237 hace referencia a las características que debe tener el informe de un perito "el dictamen debe ser claro, preciso y detallado; en él se explican los exámenes, experimentos e investigaciones efectuadas. Lo mismo que los fundamentos técnico, científicos o artísticos de las conclusiones". [4]

Artículo 175:Medios de prueba, **S**irven como pruebas, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez.[5]
El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio.

2) LEY 527

La cual define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [6]
ART. 10. Admisibilidad y fuerza probatoria de los mensajes de datos. [7]
ART. 11. Criterio para valorar probatoriamente un mensaje de datos. [8]
La Corte Constitucional en la Sentencia No. C-662 de Junio 8 de 2000 consideró: "El proyecto de ley establece que los

mensajes de datos se deben considerar como medios de prueba. [9]

3) Ley 1273

Esta ley crea un nuevo bien jurídico denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones; en esta ley se define que es el acceso abusivo a un sistema de informático, interceptación de datos informáticos; obstaculización ilegítima de un sistema informático o una red de telecomunicaciones, suplantación de sitios web para captura de datos y violación de datos personales. *[10]*

4) Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene como objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.[11]

5) Ley 1266 de 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [12]

6) Ley 599de 2000 Acceso abusivo a un sistema de informático

Articulo 195 el que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurra en multa.[13]

7) Ley 1288de 2009

Articulo 25 Modificación de penas para los delitos de divulgación y empleo de documentos reservados y acceso abusivo a un sistema informático. [14]

Articulo 195 Articulo 195 el que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurra en pena de prisión de 5 a 8 años. [15]

B. La toma de imagen de un sistema debe ser lo más exacta posible

En el mercado existe una gran variedad herramientas para la recolección de evidencia digital y depende del nivel de experiencia del investigador el seleccionar aquellas que se ajusten a la investigación en curso. Basado en la experiencia del ingeniero Jeymy Cano y la ingeniera ÁngelaMaríaRodríguez en su libro peritaje informático y la evidencia digital en Colombia,se recomiendan los software ENCASE, FORENSIC TOOLKIT Y WINEX (forense edición) como los máseficaces ya que permiten realizar análisis de la imagen teniendo control de la integridad y son las herramientas que gozan de un gran reconocimiento en el medio.

C. Detallar fechas y horas

Para poder establecer la línea de de tiempo sobre los hechos que son materia de investigación es importante anotar las diferencias entre la hora del sistema y la de la hora UTC. Se debe tener en cuenta si los sistemas están sincronizados y utilizan hora local o utilizan la hora UTC, estas diferencias afectan la línea de tiempo en una investigación.

D. Estar preparados para testificar

Hace referencia al perito forense, persona experta que tiene la facultad de rendir un concepto en el tema de su conocimiento para ayudar al juez en su tarea de forjarse un criterio sobre el tema que se está analizando en el juicio. [16]

E. Minimizar los cambios a los datos que se van a recolectar

En lo posible se debe trabajar sobre las copias de las imágenes minizando el trabajo sobre la imagen original.

F. Entre la recolección y el análisis, prevalece primero la recolección

Teniendo en cuenta que la evidencia puede ser volátil se debe recolectar de lo más volátil a lo menos volátil.

G. Por cada dispositivo se debe adoptar un criterio que debe ser aprobado

Seleccionar las herramientas apropiadas para cada dispositivo o software a analizar. Bloqueadores de escritura (TableauultimateForensicWrite Protection Kit II-ES), Estaciones Forenses, Conectores para los diferentes tipos de discos duros (IDE/SATA, SCSI), Discos Duros Externos, Dongles (Para la ejecución de aplicaciones forenses), Cables USB, Cables cruzados.

H. Principio deLocard

Este principio creado por EdmonLocard hace referencia a: siempre que dos objetos entran en contacto, transfieren parte del material que incorpora entre ellos**.**

Cualquier objeto que entra en la escena del crimen deja un rastro, los indicios o evidencias físicas proceden de principalmente del sitio o lugar de los hechos, del presunto responsable o autor.[17]

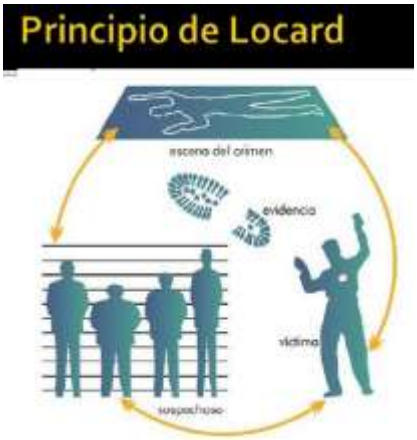

Fig. 1 principio de Locard

VI. Tipo de evidencias

Existen tres tipos de evidencias:

A. Evidencia condicional

Estas son causadas por un evento o una acción dentro de la escena del crimen. Dentro de la escena del crimen un computador, memorias USB y teléfonos celulares etc.

B. Evidencia curso o patrón

Son producidas por un contacto con sistema por ejemplo las trazas de ingreso a los sistemas, las conexiones de red entre los equipos, la transferencia de información entre los sistemas.

C. Evidencia transferida

Se basa en el principio de Locard se refiere, como su nombre lo indica, a que son producidas por un contacto, se"transfieren" y puede ser entre personas u objetos.

VII. APLICACIONES DE LA INFORMATICA FORENSE

A. Temas corporativos

Ayuda a la recolección de información de acoso sexual, robo, mal uso o apropiación de la información confidencial propietaria, o de espionaje industrial; la industria de los seguros se apoya en la informática forense para la recolección y presentación de evidencias ante reclamaciones por accidentes.

B. Prosecución criminal

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

C. *Delitos informáticos*:

Ayuda a la comprobación de suplantación de identidad, denegación de servicios, ataques a redes informáticas y corporativas, SQL inyección, intrusión a un sistema por un hacker.

VIII. Desafíos de la informática forense

El ingeniero Jeymi Cano en su libro de computación forense describe la informática forense como un desafío interdisciplinario que demanda un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimientos formal, científico y legal para el ejercicio de una disciplina que apoye directamente a la administración de justicia.[18]

Debido al alto costo que tienen las herramientas para el ejercicio de la informática forense la acreditación laboratorios informático forenses es uno de los retos que enfrentan la informática forense.

En mí opino la informática forense tiene 6 principales retos los cuales se describen a continuación:

A. Ausencia de talento y expertos factor humano

Se requiere una formación experta para mejorar la efectividad de los procesos de recolección, análisis, elaboración de informe técnico y la presentación ante el juez de los resultados; para ello se requiere tener experiencia como investigador forense.

B. Marco legal

Nuevos delitos informáticos y su tipificación en el sistema penal acusatorio, el sistema penal acusatorio no van de la mano a las modalidades de delitos informáticos.

C. Infraestructura y tecnología

La tecnología existente en el mercado para el análisis forense tiene falencias en casos como daño del equipo, teléfonos chinos de marca no comerciales, el desarrollo de nuevas tecnologías sin un estándar previamente definido por los organismos reguladores del marcado.

D. La preparación de la rama judicial en Colombia

La rama judicial en Colombia tiene como reto mejorar las habilidades y aptitudes de los jueces con el propósito de obtener los conceptos básicos que son abordados en los juicios contra delitos informáticos.

E. La computación forense en la nube

Es uno de los análisis más complejos a realizar inicia desde entender la relación del usuarios con las redes sociales, luego la red social con los medios inalámbricos, los programas utilizados hasta llegar a la prestación de servicios por terceros.

De acuerdo a lo anterior la computación forense es un complejo mundo tecnológico que demanda una elaborada estrategia de análisis y entendimiento, que reta los modelos actuales de investigación empleados por la informática forense.

F. Disco en estado solido

Los discos en estado sólido son discos de nueva tecnología que se basan en memoria flash;el reto radica en que la información borrada de un disco en estado solido no es recuperable, la empresa recupera data es la empresa pionera en este proceso en la primera empresa que ha reportado que ha logrado la recuperación de información en esta clase de discos.

IX. Conclusiones

La informática forense permite a las organizaciones la creación de políticas sobre el uso y manejo de los sistemas de información facilitando a los empleados y la organización el cumplimiento de las normas legales.

Permite a las organizaciones auditar la tecnología y los recursos informáticos de forma más profunda; producto de este análisis se detectan las vulnerabilidades que van asociadas a cada tecnología utilizada en la organización.

Ayuda a la creación de medidas preventivas que permiten a las organizaciones y la personas a mejorar sus estándares de seguridad.

En caso de un incidente de seguridad que implique que los sistemas de la compañía han sido vulnerados; la informática forense permite la recolección de datos probatorios que siguiendo las evidencias nos lleven al origen del ataque;

Determinando las posibles alteraciones, manipulaciones, fugas o destrucción de datos.

Los delitos informáticos siempre irán adelante de las leyes.

La informática forense busca responder preguntas ¿Cómo?, ¿Dónde?, ¿Para què? Y ¿por què?.

La línea tiempo juega un papel muy importante en la demostración de la comprobación de los hechos de no estar correctamente elaborada el juez la puede considerar como prueba no valida y podía ocasionar el cierre o pérdida del caso.

Dentro de la escena de un posible delito informático es muy importante que la persona tiene el primer contacto con la escena del delito y con los medios implicados, tenga conocimiento de cómo atender el primer nivel de incidente, documente todo lo realizado en la atención de esta primera parte de la atención del incidente, de la correcta atención depende el éxito del análisis realizado por examinador forense; actualmente la gran mayoría de personas que atienden incidente a primer nivel no cuentas con este capacitación, lo que dificulta de demostración de los delitos informáticos.

Dentro de las principales causas de anulación de la evidencia encontramos la falta de conocimiento de las leyes colombianas, ruptura de la cadena de evidencia, experiencia no demostrable por el perito informático ante el juez.

El desarrollo de la tecnología contribuye con la variedad de los delitos informáticos, la investigación de estos delitos permite el desarrollo de nuevas herramientas forense que contribuyen al fortalecimiento de la informática forense.

X. REFERENCIAS

[1] Sitio web EcuReddisponible en: http://www.ecured.cu/index.php/Inform%C3%A1tica_Forense#Definici.C3.B3n

[2] Sitio web Criptoreddisponibleen: http://www.criptored.upm.es/descarga/ConferenciaJavierPagesTASSI2013.pdf

[3] Sitio web alcaldía de Montería disponible en: http://alcaldiademonteria.tripod.com/codigos/civil/tblcndo.htm

[4], [13],[14],[13], [14],[15],[16],[18]JeimyJosé Cano Martínez, El peritaje informático y la evidencia digital en Colombia.

[5] Sitio web de la cancillería disponible en:http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/codigo_procedimiento_civil.pdf

[6], [7], [8] [9] sitio web de la alcaldía disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[10] Sitio web slideshare.net disponible en: http://es.slideshare.net/scarchivistas/ley-no-1273-de-2009-proteccin-de-la-informacin-y-de-los-datos

[11] sitio web secretaria del senado disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[12] Sitio web de la alcaldía de Bogotá disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

[16] sitio web es.scribd.com disponible en: http://es.scribd.com/doc/181782097/Principio-de-Locard-o-de-Intercambio-de-Indicios

[17] Sitio web es.slideshare.net disponible en: http://es.slideshare.net/joseber/computacin-forense