INFORMÁTICA FORENSE: CUANDO EL DELITO HACE USO DE LA TECNOLOGÍA

Carlos Edgardo López Grande
Ingeniero en Sistemas y Computación. Docente de Escuela de Ingeniería Eléctrica y Electrónica. ITCA-FEPADE Sede Central. E-mail: carlos.lopez@itca.edu.sv
Ricardo Salvador Guadron Gutiérrez
Ingeniero Electricista. Director de Escuela de Ingeniería Eléctrica y Electrónica. ITCA-FEPADE Sede Central. E-mail: rguadron@itca.edu.sv

Resumen

El crimen ha evolucionado a la misma velocidad que la tecnología. El fraude, el engaño e incluso la violación y el asesinato pueden ser cometidos usando la tecnología. Es necesario que la evidencia digital considerada en los procedimientos judiciales para resolver muchos de estos casos considerados insolubles.

Palabras clave

Protección de datos, inteligencia artificial, aplicación informática, legislación de las comunicaciones, derecho a la privacidad, derecho de la informática, cibernética.

Abstract

Crime has evolved at the same speed as technology. Fraud, deception and even rape and murder can be committed using technology. It is necessary that digital evidence can be considered in court proceedings to resolve many of these cases considered unsolvable.

Keywords

Data protection, artificial intelligence, computing application, communications legislation, right to privacy, computer law, cybernetics.

Introducción

El 10 de enero de 2007 en un apartamento de la calle Güemes 2280 en Florida, ciudad de Buenos Aires, encontraron el cuerpo sin vida de Solange Grabenheimer, con cuatro puñaladas en su cuello y con señales de estrangulamiento. La principal sospechosa del asesinato: su amiga y compañera de cuarto Lucila Frend. [1]

Figura 1 – Lucila Frend (a la izquierda) junto a Solange Grabenheimer

En la autopsia que se le hizo al cuerpo de Solange en la escena del crimen se le extrajo el "humor vítreo", un líquido que se encuentra en el globo ocular y el que, al realizarle un análisis de potasio, permite obtener datos certeros sobre el tiempo de la muerte.

Uno de los forenses del caso mencionó que **el líquido extraído de la víctima se contaminó** porque dio como resultado 77 horas de muerta, es decir, dio que Solange estaba muerta cuando todavía estaba viva. Otros resultados arrojaron que el asesinato sucedió entre las 5 a.m. (cuando Lucila estaba en casa) y las 5 p.m. (cuando Lucila no estaba en casa) y otro estudio realizado dio como resultado que la víctima falleció entre las 7 am y 1 pm. Nunca se tuvo intervalo de tiempo certero para la muerte de Solange.

¿Por qué se contaminó el humor vítreo? Porque la aguja tocó otros tejidos del ojo debido a la **inexperiencia de quien tomó la muestra;** además, **no tomaron la temperatura del cuerpo** porque al levantar las evidencias se fijaron que **no llevaban consigo el termómetro indicado. La coartada de Lucila comenzó a tomar más fuerza** y casi 7 años después, en noviembre de 2013, **fue absuelta definitivamente de los cargos** y **el caso quedó sin resolver.**

Como este, existen muchos casos que no logran ser resueltos por malos procedimientos al momento de levantar evidencias de una escena del crimen. La falta de experiencia, el no contar con las herramientas adecuadas o incluso

Recibido: 27/03/2017 - Aceptado: 11/06/2017

hasta el desconocimiento pueden llevar a que el análisis forense tenga vacíos y se puedan perder casos como el de Solange y que los culpables queden libres o que los inocentes cumplan condenas que no merecen.

El mundo digital no está exento de este tipo de escenarios delictivos, entre ellos el uso de informática para realizar una estafa, obtener credenciales de cuentas bancarias, enviar amenazas (intentando quedar en el anonimato), robo de datos a una empresa o persona, acceso indebido a la información de la compañía, daños a sitios web, violaciones a la confidencialidad y secretos de una organización. Así como en el mundo real existe un procedimiento forense para esclarecer los hechos y encontrar a los responsables, en la informática también podemos hacer uso de la Informática Forense.

Según el Buró Federal de Investigaciones (FBI, por sus siglas en inglés), la Informática Forense es la ciencia que se encarga de adquirir, preservar, analizar y presentar los datos que han sido procesados electrónicamente y almacenados en medios electrónicos aplicando técnicas científicas y analíticas utilizando hardware y software especializado para realizar la tarea. [2]

La aplicación de estas técnicas a través de procesos técnicos y científicos, permite presentar datos válidos dentro de un proceso legal a partir de la reconstrucción de un bien informático, el examen de datos residuales, la autenticación de datos y la recuperación de información, entre otras actividades relacionadas puntualmente a cada delito informático, con el objetivo de alcanzar:

- La compensación de los daños causados por el delito.
- La persecución y procesamiento judicial de los criminales, en base a las leyes de cada país en el que se haya realizado el delito informático.
- La creación y aplicación de medidas para prevenir más casos similares. Es necesario aclarar en este punto que la Informática Forense no es una ciencia de prevención;
  se aplica una vez el delito ha sido cometido, pero puede ofrecer insumos que permitan evitar delitos similares en el futuro.

Principios de la Informática Forense

A principio de los años 90, el FBI observó que, así como la identificación del ADN es un elemento de prueba poderoso en el combate contra el crimen, las pruebas o evidencias digitales también podrían serlo, creando así la unidad CART (Análisis Computacional y Equipo de Respuesta, por sus siglas en inglés) encargada de dar soporte al FBI en las investigaciones y exámenes forenses de las evidencias digitales.

A finales de los 90, se creó la IOCE (Organización Internacional de Evidencia Computacional, por sus siglas en inglés) con el objetivo de compartir información sobre las prácticas de Informática Forense en todo el mundo.
En marzo de 1998, se le encargó a la IOCE el desarrollo de una serie de principios aplicables a los procedimientos para actuaciones relacionadas a las pruebas digitales, la armonización de métodos y procedimientos entre las naciones que garantizas en la fiabilidad en el uso de las pruebas digitales recogidas por un estado para que fueran utilizadas en los tribunales de justicia de otro estado.
Después de dos años, el G8 aprobó un conjunto de principios básicos aplicables a las evidencias digitales [3]:

- Al manipular evidencias digitales deben aplicarse todos los procedimientos generales y técnicas forenses con el objetivo de proteger los intereses de todas las partes.

- Las acciones que se realicen sobre las evidencias digitales no deben alterar por ningún motivo la evidencia digital. Si se requiere realizar una prueba que altere la evidencia, debe documentarse el procedimiento.

- Toda persona que manipule una evidencia digital debe ser formada para ese propósito. Aunque se realice una copia de la evidencia para actuar sobre dicha copia, algunos casos requerirán que se actúe sobre la evidencia original y deberá hacerlo una persona preparada para ello.

- Toda actividad relacionada a la evidencia digital: recogida, acceso, almacenamiento o transferencia, debe ser completamente documentada, conservada y estar disponible para su estudio.

- Mientras una persona esté a cargo de una evidencia digital, es la única responsable de todas las acciones tomadas sobre ella.

Las instituciones autorizadas para recoger y manipular pruebas digitales deben velar por el cumplimiento de estos principios, que servirán como marco de referencia y apoyarán los procedimientos de actuación que se desarrollen en dichas instituciones.

Todas las técnicas que se utilicen en la recolección y análisis de las evidencias digitales deben respaldarse en una buena metodología científica y documentarse bajo un protocolo de actuación que permita recoger los aspectos técnicos informáticos y legales de la peculiaridad forense.

Una premisa fundamental en la Ciencia Forense, que puede aplicar también a la Informática Forense, es el Principio de Transferencia de Locard [4], que permite relacionar a un criminal con el delito que ha cometido. Suele expresarse de la siguiente manera: "Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"; por ejemplo, si en el mundo físico se rompe un cristal con la mano, entonces en la mano pueden quedar residuos del cristal y en el cristal pueden quedar rastros de sangre. Si se pisa el césped, puede quedar césped en el zapato y puede quedar una huella en el césped. Si aplicamos este principio al mundo digital, una conexión SSH indebida puede dejar logs que pueden ser visualizados posteriormente; un ataque con exploits podría dejar un MD5 único de un "único" atacante.

Fases de la Informática Forense

Basado en el concepto de Informática Forense del FBI, existen 4 fases principales en el proceso; sin embargo, se puede agregar una fase previa, tal como se observa en la Figura 2.

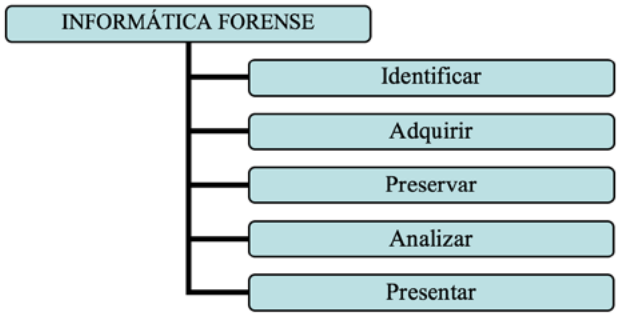

Figura 2 – Fases de la Informática Forense

A. Identificar

Una vez que el delito ha sido cometido, debe iniciarse una identificación que consiste en el conocimiento y la comprobación del hecho delictivo; por lo general se realiza con una evaluación de los recursos, alcances y objetivos para realizar la investigación, que debe ser hecha por un equipo de trabajo idóneo al que se le definirán sus límites, funciones y responsabilidades. Además, debe hacerse una investigación preliminar que permita describir la situación actual, los hechos, las partes afectadas, los posibles sospechosos, la infraestructura que ha sido afectada o vulnerada para lograr una mayor comprensión de la situación y definir un curso de acción de acuerdo a ella.

Por otra parte, deben reconocerse los elementos informáticos involucrados en el delito, tales como servidores, computadoras de escritorio, dispositivos móviles, switches, routers, firewalls. También deben identificarse dispositivos de almacenamiento que se consideren comprometidos y que puedan servir como evidencia, por ejemplo discos duros internos y externos, memorias flash extraíbles, entre otros.

Es importante asegurar la escena del hecho delictivo, tanto física como digitalmente. Al igual como se asegura la escena para que el ADN y las huellas digitales no se contaminen, así deben asegurarse los elementos electrónicos. La contaminación física puede alterar una evidencia digital, por ejemplo: la electricidad estática del cuerpo humano podría inhabilitar un circuito; los golpes en un disco duro podrían dejarlo inaccesible; un imán cerca de un dispositivo electrónico puede alterar los datos almacenados en el mismo, entre otros.

En todo procedimiento forense informático es necesaria la aplicación de la Cadena de Custodia, que no es más que un conjunto de pasos o procedimientos que ayudan a preservar la prueba digital para que posteriormente pueda ser utilizada como evidencia digital en un proceso judicial. No existe un estándar reconocido mundialmente para la Cadena de Custodia, pero existen algunos procedimientos que pueden utilizarse para manipular las pruebas digitales.

La Cadena de Custodia [5] debe reducir lo más que se pueda la cantidad de agentes implicados en el tratamiento de las evidencias. Además debe mantener la identidad de las personas implicadas desde que se obtienen hasta que se presentan las evidencias; debe garantizar la integridad de las evidencias en los traspasos entre agentes involucrados en el proceso. Para ello, se deben firmar los registros de tiempos de traspaso de evidencias y, en cada uno de ellos, el agente que corresponde es responsable de la evidencia. La Cadena de Custodia permitirá observar quién obtuvo la evidencia; dónde y cuándo la evidencia fue obtenida; quién protegió la evidencia y quién ha tenido acceso a la evidencia en todo el proceso de investigación.

Esta fase debe entregar como resultado un documento que permita definir un punto de partida para realizar la adquisición de datos, así como el aseguramiento de los dispositivos que se van a peritar.

B. Adquirir

El grupo IETF (Grupo de Trabajo en Ingeniería de Internet, por sus siglas en inglés), conformado por gente que viene de proveedoras de servicios, fabricantes de equipos, investigadores, profesores, estudiantes, entre otros, desarrolló en el año 2002 el documento RFC 3227 [6] con los lineamientos necesarios para la recolección y archivamiento de las

evidencias digitales. Si bien es cierto, esta RFC no es de cumplimiento obligatorio, la mayoría de lineamientos son aplicables a los procedimientos de Informática Forense, y pueden servir para reforzar otros procedimientos que los propios forenses sigan. Aún, considerando que en el año 2002 la tecnología no estaba tan avanzada como hoy, el RFC 3227 sigue teniendo la misma vigencia para esos casos.

Entre los lineamientos cubiertos por la RFC tenemos los siguientes:

- Minimizar los cambios de los datos que se están recolectando; de existir cambios, estos deben ser registrados debidamente.
- Verificar la diferencia entre la hora local y la de los sistemas comprometidos.
- Cuando en la escena del crimen se tenga que decidir entre recolectar la evidencia o analizarla, se debe recolectar primero y analizar después.
- Proceder en el orden de volatilidad. Del elemento más volátil al menos volátil. El siguiente es un ejemplo del orden que debería seguirse según la volatilidad:
    - Registros y memorias caché.
    - Tablas de ruteo, caché del ARP, tabla de procesos, estadísticas del kernel, memoria.
    - Archivos temporales del sistema.
    - Disco físico.
    - Inicios de sesión remotos y monitoreo de información relevante al caso.
    - Configuración física, topología de red.
    - Almacenar el medio.

Considerando que la destrucción de las evidencias digitales es realmente fácil, el RFC 3227 [6], contiene las siguientes recomendaciones:

- No apagar el equipo hasta que se haya terminado de recolectar toda la evidencia. Puede perderse mucha evidencia y el atacante pudo haber alterado el inicio o apagado del sistema para destruir la evidencia.

- No utilizar los programas del sistema para recolectar evidencias, debido a que no son confiables al haber sido comprometidos. Debe utilizar sus propias herramientas de software para recolectarla.

- No utilizar programas que modifiquen las fechas y horas de acceso a los archivos del sistema.

- No desconectar los equipos de la red hasta recolectar toda la evidencia, ya que la simple desconexión del equipo podría activar un proceso que identifique la desconexión y borre automáticamente la información del equipo.

Por otra parte, el RFC 3227 [6] tiene consideraciones de privacidad con respecto al levantamiento de evidencias digitales:

- Respetar los lineamientos y reglas de privacidad dictadas por la organización y por las leyes del país o ciudad donde se realizó el delito. Considerando que debe asegurarse que nadie que no esté autorizado tenga acceso a información que pueda ser recogida como evidencia, como por ejemplo archivos de logs; en ellos puede encontrarse los patrones del ataque realizado.

- No hacer intrusión en la privacidad de las personas sin tener una justificación de peso que lo respalde. Particularmente, no recolectar información de áreas en las que normalmente no se tiene una razón para accederlos, como, por ejemplo, los archivos personales del usuario, a menos que se tengan indicios suficientes y comprobables que sugieran que allí hay información relacionada al delito cometido.

- Asegurarse de tener el respaldo de los procedimientos de la organización correspondientes a la recolección de evidencias digitales de un incidente o delito.

Estas medidas, adicionando otras que el forense o la organización estimen convenientes en el proceso, permitirán que la evidencia cumpla con las siguientes características para que sea tomada en cuenta como evidencia válida:

- ***Admisible:*** debe estar conforme a las leyes (de cada país o ciudad) para que sea aceptada en una corte.

- ***Auténtica:*** esto permitirá relacionar la evidencia digital con el incidente o delito cometido.

- ***Completa:*** la evidencia debe respaldar la historia detrás del delito y no solamente una perspectiva del mismo.

- ***Confiable:*** no debe existir nada que haga dudar de la autenticidad y veracidad de la evidencia.

- ***Creíble:*** debe ser evidencia creíble y entendible para el juez de la corte en la que se utilizará.

Al momento de recoger las evidencias en la escena de delito, es necesario empaquetarlas adecuadamente para poder así garantizar su integridad sin dejar de poner atención a la Cadena de Custodia. Estas acciones son fundamentales debido a la gran cantidad de

situaciones y evidencias digitales que pueden encontrarse.

C. Preservar

Una vez que se ha recogido la evidencia se recomienda fotografiar el equipo sin desmontar con el número de serie visible; fotografiar el equipo ya desmontado siempre mostrando el número de serie para que coincidan al momento de realizar una comparación. Debe fotografiarse además la configuración de conexiones internas del equipo, dejando constancia de todo esto en el respectivo informe y respetando los principios de la Cadena de Custodia.

Si la principal evidencia es el disco duro del equipo, es necesario que no sea alterada, tal y como se ha mencionado anteriormente. Por lo tanto, debe hacerse una o varias copias del elemento incautado para evitar que la evidencia original sea modificada. La copia es íntegra del dispositivo, es decir, bit a bit. Una vez la copia se ha realizado exitosamente, debe asegurarse la evidencia original con algún dispositivo que no permita la escritura en el disco.

La copia realizada deberá firmarse con un hash de MD5 o SHA1 generando así un segundo original a partir del cual se realizarán las demás copias que irán siendo analizadas en el proceso; a estas copias debe generársele un MD5 para comprobar que no han sido alteradas y son iguales al original. Es necesario documentar toda la evidencia incluyendo un documento para su embalaje, en donde se describan todas las características, como, por ejemplo: el fabricante, el número de serie, el estado físico, la capacidad de almacenamiento, entre otros.

Se recomienda fotografiar el disco duro original más los medios en los que se realizó la copia y documentarse con fecha y hora para hacer constar la entrega del original y las copias. Deben resguardarse en un lugar seguro y libre de ondas electromagnéticas que afecten la evidencia.
A partir de este momento, es recomendable que cada vez que se vaya a hacer uso de alguna evidencia recolectada, sea con la supervisión de un testigo de confianza que haga constar que se han utilizado las copias y que no han sido alteradas. Es opcional y recomendable también, que todo el proceso descrito anteriormente esté acompañado de un testigo que pueda dar fe de que al momento de recolectar la evidencia, hacer las copias y resguardarlas, no se hizo nada que afecte o corrompa el proceso de análisis.

D. Análisis

Al tener completa la recolección de la evidencia digital necesaria para la solución del caso, el análisis de éstas debe realizarse en una red aislada con equipos que estén preparados para tal fin. Existen diferentes soluciones de hardware y software que permitirán realizar el análisis forense, tanto de paga como de código abierto. Dependerá del forense y el entorno de trabajo para decidir las herramientas a utilizar para el análisis de las evidencias.

Dependiendo del tipo de escenario, así sería la aplicación de la Informática Forense; cuando está implicado el uso de un sistema informático o una evidencia digital, pero, que el crimen que se haya cometido pueda ser de distinta índole, como el robo de información, el fraude, delitos de propiedad intelectual, entre otros, entonces se aplica **Computer Forensics**. Si en cambio, la investigación está destinada a ataques o comportamientos sospechosos directamente a sistemas informáticos tales como intrusiones, ataques de DoS, entre otros, entonces la Informática Forense se aplica como **Intrusion Forensics.** [7]

El análisis de las evidencias digitales puede realizarse en dos modos:

Análisis Post-mortem: cuando la evidencia se analiza con un equipo dedicado especialmente a la Informática Forense. Se encuentra generalmente en un laboratorio y cuenta con las características de hardware y las herramientas de software necesarias para el análisis.

Análisis en Caliente: no es recomendable, pero si no existe otra opción, el análisis se realiza en el equipo que se presume fue violentado o que ha sufrido algún incidente de seguridad. Para este caso se recomienda utilizar un medio de almacenamiento que contenga diferentes herramientas de análisis forense compiladas de tal forma que no modifiquen en ninguna manera el sistema comprometido. Luego de terminar el análisis en caliente, debe realizarse el análisis post-mortem.

Una de las primeras cosas que un forense informático debe plantearse a la hora de hacer el análisis de las evidencias, es el arsenal de herramientas con las que cuenta en el laboratorio. Como anteriormente se mencionó, existen diferentes soluciones de pago y gratuitas para este fin. A continuación, se detallarán 3 distribuciones gratuitas de Linux que contienen sets de herramientas útiles al momento de realizar el **Análisis Forense**:

Kali Linux 2016.1 [8]: distribución más reciente de Linux conocida por ser utilizada en la mayoría de los casos por la cantidad de herramientas de hacking que contiene.

Bajo ese mismo sentido, esta distribución posee una caja de herramientas relativamente pequeña para realizar análisis forense de evidencias digitales. Incluso, puede ser utilizada para un Análisis en Caliente, debido a que tiene una opción de arranque en "Modo Forense", tal y como vemos en la Figura 3. Este modo permite iniciar el equipo comprometido sin montar automáticamente las unidades de almacenamiento internas y externas que puedan modificar en alguna medida la información contenida en ellos.

Figura 3 – Opciones de arranque de Kali Linux 2016.1

CAINE 7 (Computer Aided Investigative Enviroment) [9]**:** Como se muestra en la Figura 4, CAINE es una distribución de Linux creada por desarrolladores italianos basada en Ubuntu 14.04 y liberada en el 2015 para arquitecturas de 64 bits. Permite bloquear los dispositivos de almacenamiento y ponerlos como en modo lectura haciendo uso de una de las herramientas que posee la distribución. Posee un entorno de trabajo amigable que acompaña al forense desde el momento en el que se adquiere la evidencia hasta que se entrega el reporte a las autoridades. Posee una aplicación llamada Systemback que permite volver atrás como cuando se hace un punto de restauración. Además de poder ser utilizado como LiveCD. Posee herramientas especializadas en la copia de imágenes íntegras de dispositivos de almacenamiento, para recuperar ficheros y carpetas borrados previamente y otras como para recuperar imágenes o fotos que han sido eliminadas del sistema.

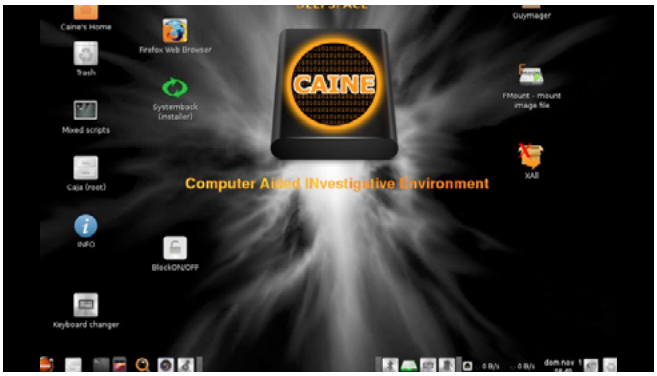

Figura 4 – Interfaz de usuario de CAINE 7

SIFT (SANS Investigative Forensic Toolkit) [10]**:** basado en Ubuntu, es una plataforma que ofrece al investigador una serie de herramientas para realizar una investigación detallada de la evidencia digital. Soporta los diferentes sistemas de archivos de los sistemas operativos actuales, además de contener aplicaciones que ayudan a crear imágenes íntegras de los dispositivos de almacenamiento, recuperación de archivos, documentos e imágenes, herramientas para examinar logs de diferentes dispositivos, entre otros. Una de las ventajas de SIFT es que a partir de cualquier distribución de Linux puede generarse este set de herramientas forense haciendo la instalación de los paquetes necesarios para el mismo. Además, cuenta con una gran cantidad de manuales y guías que ayudarán a los que se encuentran comenzando en el ámbito de la Informática Forense para que sepan utilizar las distintas herramientas, tal como se ve en la Figura 5.

Figura 5 – Entorno de trabajo de SIFT

El objetivo de éstas y otras distribuciones o herramientas de software es la de poder acompañar a cada parte del proceso de Informática Forense. La flexibilidad y personalización que permiten estas distribuciones hará que el investigador pueda agregar o eliminar las herramientas que considere necesarias en su metodología de investigación. Pudiendo generar así, resultados que podrán ser presentados en un proceso judicial.

E. Presentar

A lo largo del proceso de la aplicación de la Informática Forense se ha mencionado muchas veces la documentación que es una parte importante del proceso porque al final, permitirá presentar por escrito de forma exacta, comprensible, clara y completa, los pasos que se llevaron a cabo en el análisis, los hallazgos realizados y la interpretación de los mismos para poder ofrecer una conclusión para cada uno de ellos. Debido a que, en la mayoría de los casos, el documento se presenta a instancias que no tienen los conocimientos técnicos suficientes sobre la materia, éste debe ser escrito en una forma fácil y entendible sin dejar vacíos.

Por lo general se recomienda la presentación de dos

documentos: un **Informe Ejecutivo** que muestre los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos. Este informe debe ser muy claro, certero y conciso, dejando afuera cualquier cuestión que genere algún tipo de duda. El segundo documento, un **Informe Técnico**, es una exposición que nos detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales.

Conclusiones

Después de conocer un poco sobre la Informática Forense, es necesario reconocer que existen varias dificultades para su correcta aplicación, que van desde la preparación académica y técnica de los especialistas, hasta las legislaciones de cada país y la forma en la que se manejan y aportan las evidencias digitales a cada uno de los casos. Pero, además de dificultades, se convierten en un reto para todos los involucrados en el proceso: legisladores, jueces, investigadores, especialistas informáticos.

Todas las disciplinas forenses evolucionan con el paso del tiempo a partir de nuevos hallazgos, se desarrollan nuevas metodologías científicas y se mejoran las técnicas de aplicación con el objetivo de favorecer el trabajo del investigador y al análisis que los especialistas forenses realizan día con día. El ámbito informático no se queda atrás, debido a que este campo sufre cambios a diario, lo que implica mayor preparación.

Muchos casos que en la actualidad aparentan no tener solución, posiblemente la tengan, porque ahora el crimen hace uso de la tecnología dejando evidencias que la Informática Forense será capaz de rastrear.

Referencias

[1] S. Amaya, "Caso Solange: qué podría llegar a condenar o absolver a Lucila Frend", La Nación, 4 July 2011, [En línea]. Disponible en: http://www.lanacion.com.ar/1386331-caso-solange-que-podria-llegar-a-condenar-o-absolver-a-lucila-frend [Accedido: 10 -feb- 2016]

[2] M. G. Noblett y M. M. Pollit, «FBI,» FBI, October 2000. [Online]. Available: https://www.fbi.gov/about-us/lab/forensic-science- communications/fsc/oct2000/index.htm/computer.htm [Accessed: 10 Feb. 2016]

[3] "Digital Evidence: standards and principles", Forensic Science Communications, FBI, apr. 2000. [Online]. Avalilable: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm. [Accessed: 10 -Feb-2016]

[4] L. F. Hombreiro Noriega, "El ADN de Locard, genética forense y criminalista", Madrid: Reus, 2013, pp. 13-17.

[5]. Argentina. Sistema Argentino de Información Jurídica, Infojus. Ministerio de Justicia y Derechos Humanos. Presidencia de la Nación. "Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen : Programa Nacional de Criminalística", [En línea]. Argentina : Ministerio de Justicia y Derechos Humanos: Presidencia de la Nación, 2015. Disponible en: http://www.mpf.gob.ar/capacitacion/files/2015/07/Manual-Criminalistica.pdf. [Accedido: 10 -feb- 2016]

[6] D. Brezinski y T. Killalea, "Guidelines for Evidence Collection and Archiving", Feb. 2002. [Online]. Available: https://www.ietf.org/rfc/rfc3227.txt. [Accessed: 4 -Mar- 2016]

[7] G. Mohay [et al.] "Computer and Intrusion Forensics.pdf", George Mohay… [et al.]. Artech House, 2001. [Online]. Available: https://doc.lagout.org/network/1_Security/Computer%20and%20Intrusion%20Forensics.pdf. [Accessed: 5 -Mar- 2016]

[8] Muts. "Kali Linux, Rolling Edition Released - 2016", Article, 21 January 2016. [Online] Available: https://www.kali.org/news/kali-linux-rolling-edition-2016-1/. [Accessed: 6 -Mar- 2016]

[9] "CAINE Live USB/DVD : computer forensics digital forensics", 2015. [Online]. Available: http://www.caine-live.net/. [Accessed: 5 –Jun- 2016]

10] Digital Forensics and Incident Response, DFIR - SANS, "Investigative Forensic Toolkit (SIFT)" : Workstation Versión 3", 2015. [Online]. Available: https://digital-forensics.sans.org/community/downloads [Accessed: 12 -Mar- 2016]