Evidencia forense digital en equipos de cómputo, redes y computación en la nube*[1]

[Digital forensic evidence in computing, networking and cloud computing]

José Javier TRIANA FUENTES[2], Javier Antonio BALLESTEROS RICAURTE[3]

Recibo: 20.02.2014 – Aprobación: 04.11.2015

Resumen

La informática forense se encarga de investigar los antecedentes por los cuales se pudo haber realizado un crimen utilizando dispositivos electrónicos con el objeto de descubrir y analizar la información disponible para que pueda servir como evidencia en un asunto legal. Hoy en día, con la posibilidad de almacenar y procesar la información a nivel local, remoto y en la nube, las empresas necesitan cada día mayor seguridad. Por medio de la informática forense y diferentes técnicas que han sido desarrolladas, aplicables según la ubicación y manejo de los datos, se puede llegar a los procesos y eventos que hicieron que se presentará tal situación y así reconstruir los sucesos que la originaron. Las distintas metodologías forenses incluyen la captura de evidencias digitales, sin alterar la información de origen. Gracias a los avances tecnológicos, en el presente artículo se

* **Modelo para la citación de este artículo:**
TRIANA FUENTES, José Javier & BALLESTEROS RICAURTE, Javier Antonio (2016). Evidencia forense digital en equipos de cómputo, redes y computación en la nube. En: Ventana Informática No. 34 (ene-jun). Manizales (Colombia): Facultad de Ciencias e Ingeniería, Universidad de Manizales. p. 9-24. ISSN: 0123-9678

1 Artículo de revisión proveniente del proyecto *Desarrollo de una guía metodológica para la realización de un análisis forense en la nube, como referencia en la evaluación de propuestas para proyectos de desarrollo tecnológico*, ejecutado en el periodo 06/2013-09/2014, e inscrito en el grupo de investigación INFELCOM de la *Universidad Pedagógica y Tecnológica de Colombia*. [Trabajo para el título de Magíster en Tecnología Informática por el primer autor con dirección del segundo].

2 Ingeniero de Sistemas; Esp. en Diseño y construcción de soluciones telemáticas; Magister(c) en Tecnología Informática. Técnico operativo, Secretaría de Educación de Boyacá (Tunja, Boyacá, Colombia). Correo electrónico: josejavier.triana@uptc.edu.co

3 Ingeniero de Sistemas; Magíster en Ciencias Computacionales. Docente asociado, Escuela de Ingeniería de Sistemas, Universidad Pedagógica y Tecnológica de Colombia (Tunja, Boyacá, Colombia). Correo electrónico: javier.ballesteros@uptc.edu.co

pretende dar a conocer y analizar cómo se realiza la adquisición de las evidencias y herramientas que se utilizan para luego analizarla, haciendo énfasis en la captura forense computacional, en redes y en computación en la nube.

Palabras claves*: Computación en la nube, evidencia digital, Análisis Forense en la nube.*

Abstract

Computer forensics is responsible for investigating records by which a crime may have made using electronic devices, in order to discover and analysis available information so it can serve as evidence in a legal matter. Today, with the ability to store and process information at local, remote and cloud level, companies need a greater security level. Through computer forensics and different techniques that have been developed, applicable by location and data management, you can get to the processes and events that led to such a situation and thus reconstruct the events that led to it. Various forensic methods include capturing digital evidence without altering the source information. Thanks to technological advances, this article aims to present and analyze how to acquire evidence and the tools used to it, in order to made an analysis later on, emphasizing the computational forensic capture in networks and cloud computing.

Keywords*: Cloud computing, digital evidence, Cloud Forensic.*

Introducción

Para el estándar ISO/IEC 27001, la Seguridad de la Información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a una organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. Sin embargo, no puede considerarse la seguridad informática en términos absolutos, por lo que muchas empresas no se han concientizado sobre la necesidad de estar preparados para enfrentar un incidente de seguridad y considerar procesos para recolectar evidencia de dicho incidente de ser necesario, por lo tanto, es necesario establecer, junto con las buenas prácticas de seguridad, equipos de atención de incidentes y estrategias para la identificación y recolección de la evidencia digital del incidente, en caso de ser necesario efectuar un análisis forense digital, para lo cual, afirman Rodríguez & Doménech (2011, 3), debe realizarse un proceso metodológico para la recolección y análisis de los datos digitales de un

sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales.

El rol de la evidencia digital en casos legales y en investigaciones digitales ha tomado mucha relevancia. En los últimos años, el análisis forense digital ha desarrollado principios, métodos y mejores prácticas a menudo reguladas por leyes internacionales, pero desafortunadamente, la mayoría de esos resultados asumen que los dispositivos digitales están físicamente disponibles para los analistas, como en el caso de la computación forense.

Por el contrario, el análisis forense en la red (*Forensics Network*) y el análisis forense en la nube (*Cloud forensics*), todavía necesitan soluciones robustas y ampliamente adoptados para recopilar, preservar y exhibir la evidencia resultante. Según Gómez (2009, 150), la informática forense nace como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En el presente artículo se da a conocer cómo se realiza la adquisición de la evidencia digital para luego analizarla, los conceptos de informática forense y su terminología, cómo se realiza la manipulación y gestión de la evidencia digital, además de algunos modelos y guías para el desarrollo de un análisis forense digital y, por último, se analiza la adquisición de evidencia digital forense en equipos de cómputo, redes y la nube.

1. Una aproximación a la Informática Forense

Para RAE (2012), Informática es el «*conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*». Por otro lado, Universidad de Murcia (2014), señala que las ciencias forenses se trata de «*la aplicación de los métodos científicos a cuestiones legales, son un apasionante campo de estudio, complejo y multidisciplinar. En ellas se emplean principios científicos (químicos, físicos, biológicos,...) así como de ciencias sociales y jurídicas para la resolución de casos legales. Constituyen una disciplina en rápida evolución que adquiere una importancia cada vez mayor en los ámbitos científico y jurídico*». De acuerdo con Noblett & Pollitt (2000), la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional,

siendo sus principales objetivos, según López et al. (2002): - La compensación de los daños causados por los criminales o intrusos, - La persecución y procesamiento judicial de los criminales, y - La creación y aplicación de medidas para prevenir casos similares.

Dentro del campo de la informática forense se encuentran varias definiciones, dependiendo del escenario en el cual se esté trabajando: Computación Forense (*computer forensics)*, Informática Forense en redes (*Network forensics*) y análisis forense en la nube (*Cloud forensic, CF*). Cada una corresponde al escenario tecnológico que se presente, pero llevan en todos los casos hacia la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de evidencia digital para detallar, validar y sustentar las hipótesis que sobre un evento se haya formulado.

Entre los términos forenses de mayor uso, están:

- Incidente de seguridad. Shirey (2007, 94), lo define como un evento de seguridad importante para un sistema en el cual las políticas de seguridad han sido evadidas. En este caso, un incidente genera un desorden y confusión en la organización, para lo cual, es necesario estar preparado para su control, de lo contrario se compromete la seguridad de la organización, y la falta de estrategias para enfrentarlos.
- Evento de seguridad. Para Shirey (2007, 269), es una ocurrencia en un sistema que es relevante para la seguridad del mismo, el término comprende tanto a eventos que son incidentes de seguridad como a aquellos que no lo son.

Según Verizon (2013), la mayoría de incidentes de seguridad no presentan gran dificultad para los atacantes, y en comparación con los resultados de Verizon (2012), no hubo mejora en la eficiencia de controles de seguridad, lo cual demuestra que no se están mejorando los controles, aunque no se determinan las causas de tal situación. Por ello, dentro de la seguridad, la ciencia forense es la que más ha evolucionado en relación directa con el incremento de los incidentes de seguridad, en cantidad y maneras.

1.1 Evidencia Digital (ED)

Dávila (2008, 97), la define como cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal. Uno de los aspectos más importantes dentro de una investigación de informática forense, es la recopilación de evidencia digital, para que cobre valor legal y pueda ser admisible dentro de un proceso jurídico. A diferencia de las evidencias físicas, para Cano (2006, 67), la evidencia digital es anónima, frágil, fácilmente puede

ser corrompida y susceptible a cambios o ser copiada, lo que dificulta en ciertas ocasiones su ingreso dentro de procesos de investigación. Las evidencias electrónicas pueden recogerse en diferentes sitios y fuentes, encontrándose en cualquier elemento o sistema utilizado para transmitir o almacenar datos.

Afirma Dávila (2008, 96-98), que la ED se enfrenta a peligros como los *Malware* (software malicioso), el deterioro electromagnético o mecánico e incluso la presencia de trampas dejadas por los delincuentes con la finalidad de eliminar archivos tan pronto sean manipulados, por lo que la ED necesita un tratamiento muy especial para luego clasificarla en categorías que le permitan tener una mejor perspectiva. Al respecto, Ghosh (2004, 10) considera que la ED se divide en tres categorías (registros almacenados en un equipo de tecnología informática, generados por los equipos de tecnología informática, y parcialmente generados y almacenados en los equipos de tecnología informática), con base en si fueron generados por una persona o por un componente electrónico.

Mosquera, Certain & Cano (2005), consideran que por la importancia de la ED dentro de un proceso, se implementan procedimientos que garanticen la confiabilidad, la autenticidad, la suficiencia y la conformidad con las leyes y reglas de la administración de justicia, ya que dadas sus características, la colocan en un constante desafío para los investigadores.

1.2 Manipulación y Gestión de la evidencia digital

Standards Australia International (2003, 34), plantea que: los procedimientos a seguir deben ser idóneos, recolectar información de forma adecuada con perspectiva forense, procedimientos para la custodia y retención seguras de la información obtenida, manipulación de registros originales o copias de los mismos. Existen guías y buenas prácticas para efectuar la gestión de la evidencia digital y recuperar la mayor cantidad de fuentes digitales en la reconstrucción de eventos:

- Hay varios tipos de modelos dependiendo la investigación a hacer o el criterio del investigador, tales como: El Modelo de Lee y Casey (Ciardhuáin, 2004), Modelo de Reith, Carr y Gunsh (Cruz, 2007, 20) y el Modelo forense CICOM (Santos & Flórez, 2012). Dichos modelos se desarrollaron antes de la llegada de las tecnologías en la nube y en gran medida, se asume que el investigador tiene acceso físico y control sobre el sistema o dispositivo de destino, así, como sus medios de almacenamiento, supuestos que no hacen valedero investigar una actividad en un entorno de computación en la nube.

- Entre las guías más conocidas están la de ENFSI (2009, 1-30), que 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, y la *Electronic Crime Scene Investigation* (NIJ, 2008, 1-62), enfocada principalmente en identificación y recolección de evidencia. Además, existen otras como lo señalan ISFS (2009), ACPO (2011, 1-66), ACPO (2009a, 1-105), ACPO (2009b, 1-20), NIJ (2004) y Brezinski & Killalea (2002, 1-10), coincidentes en las fases de identificación, preservación, análisis y presentación de la evidencia digital, de acuerdo con Mckemmish (1999, 4).

2. Computación forense

Un aspecto importante a la hora de recolectar evidencia, afirman Casey (2004, 108) y Di Iorio (2013, 328), es la preservación de su integridad a través de métodos y herramientas, es decir, garantizar que los elementos volátiles se mantengan sin cambios. Lo primero a determinar es la cantidad de evidencia que se va a tomar, a sabiendas que el hardware puede serlo al tomarse como instrumento o producto del caso. Normalmente, es necesario recolectar computadores y elementos de almacenamiento que puedan contener evidencia, afirman Álvarez & Guamán (2008, 66). Otro punto importante es tomar una decisión crítica: apagar o dejar prendidos los equipos comprometidos, la respuesta la da el investigador, quien debe utilizar su buen juicio y sentido común para determinar las acciones a seguir. Cuando la evidencia está en formato digital, el objetivo de la investigación debe ser el contenido del computador y no el hardware, por lo que se puede copiar todo o solo la información necesaria.

A partir de los ‘90s, en procedimientos de *computación forense* se desarrollan herramientas con propósitos específicos, dependiendo de la investigación y el modelo a utilizar: Para Linux: *The Coroner’s Toolkit* (Yupanqui, 2009, 57-59), para Macintosh: *Macintosh Forensic Software* (Kubasiak, 2007, 63), y para Windows: *Autopsy* (Carrier, 2013, 1-40), y *EnCase* (Guidance Software, 2009). Ante la variedad de herramientas, como lo evidencia Álvarez & Guamán (2008, 98-106), la mejor opción depende de la pericia y práctica del investigador.

3. Informática forense en redes

Otra categoría de evidencia que puede ser recolectada en el caso de los crímenes informáticos, es la presente en las redes. El flujo de información a través de una red, sea interna o externa a una organización, incluyendo Internet, podría contener evidencia útil a la hora

de investigar crímenes, como la falsificación de correos electrónicos, intercambio de información ilegal a través de internet o cometidos con la utilización de redes. En este caso, la evidencia digital difiere de la almacenada en un solo computador, en que, por lo general, se encuentra en computadores remotos o no está almacenada, a no ser que se haga un esfuerzo explícito para capturarla mediante el uso de *sniffers*[4].

3.1 Captura de evidencia en una red

La capacidad de investigar un delito en la red representa un desafío para la organización afectada y el analista forense. Aunque muchos de los ataques internos y externos se producen en la red de una organización, Salinas (2005, 12-15) resalta la ausencia de Sistemas de Detección de Intrusos, IDS, en muchas de ellas.

3.1.1 Registros DHCP. Es importante que los registros de la organización conserven los registros DHCP[5] para el período de tiempo a examinar.

3.1.2 Utilización de un host para acceder tráfico que se puede ver. *Wireshark* es el más popular analizador de protocolos de red y ofrece características como disponibilidad para Windows y Linux, captura de paquete directo de la interfaz, muestra paquetes con información detallada del protocolo y filtra paquete en mucho criterio, manifiestan Lamping, Sharpe & Warnicke (2014, 1).

3.1.3 Tráfico de red de alguna ubicación útil. Para Bruschi, Mongui & Rosti (2005, 33-35), si se desea acceder al tráfico en algún punto de la red, sin interferir con el tráfico o ser detectado en una pequeña red enrutada, donde los desafíos no son muy altos, podría hacerse con un concentrador[6]. En una red que consta de *hubs* y *routers*, un *sniffer* conectado a un concentrador se vería todo el tráfico que pasa a través del dispositivo (Figura 1a), pero si el *hub* falla, todas las conexiones a través del *hub* quedarán rotas.

4 Sánchez (2002, 72-73), lo presenta como un dispositivo o una aplicación que permite capturar datos o información que pasan a través de una red.

5 *«El Protocolo de configuración dinámica de host (DHCP) es un estándar diseñado para reducir la complejidad de la administración de configuraciones de direcciones mediante el uso de un equipo servidor para administrar de forma centralizada las direcciones IP y otros detalles de configuración de la red. El servicio DHCP permite que el equipo servidor funcione como un servidor DHCP y configurar los equipos cliente habilitados para DHCP en la red. DHCP incluye el Protocolo de asignación dinámica de direcciones de multidifusión a clientes (MADCAP), el cual se usa para realizar asignaciones de direcciones de multidifusión. Si se asignan dinámicamente direcciones IP mediante MADCAP a los clientes registrados, éstos pueden participar de forma eficaz en el proceso de secuencia de datos (por ejemplo, transmisiones de red de vídeo o audio en tiempo real)»* (Microsoft, s.f.).

6 Concentradores baratos pueden no ser capaces de soportar el rendimiento de la red y, así, crear cuello de botella para el tráfico de la red.

En contraste, las conexiones conmutadas de red son punto a punto (Figura 1b). Un *sniffer* adjunto en una red conmutada solo verá el tráfico de difusión y el dirigido a ella misma. Puede utilizarse un *sniffer* de forma fiable en una red conmutada sin un puerto *Span* o un grifo de la red, solo si el *sniffer* se encuentra en el host de interés, todo el tráfico de interés implica que el huésped y el anfitrión no se vean comprometidos.

Lo anterior se debe a que los conmutadores crean de punto extremo a extremo de las conexiones en lugar de dejar todos los sistemas para ver todo el tráfico en la misma subred. Se tendrá que utilizar un puerto *Span* o un grifo de la red para ver el tráfico de otros dispositivos y asegurarse de que el anfitrión comprometido no interferirá con la colección de tráfico. La figura 1c ilustra el hecho de que otros dispositivos de la red no ven tráfico, pero el *sniffer* es capaz de ver el tráfico a través del puerto Span.

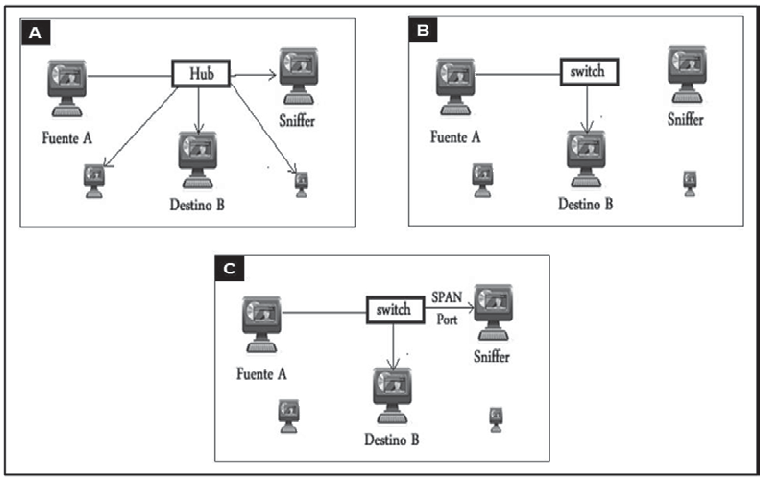

Figura 1. Redes con Hub, switch y Span

3.2 Herramientas para la Informática Forense en redes

3.2.1 Fiddler. Desarrollado por *Microsoft*, permite recolectar formatos http, https y tráfico web ftp y muestra los sitios web visitados en el camino hacia el sitio web destino, cualquier *malware* que se encuentre, el software descargado y las redirecciones se almacenan en un registro de la sesión.

3.2.2 Firewalls. Los registros de cortafuegos son una fuente primaria de muchas investigaciones, aunque no incluyen contenido, sino que recogen información acerca de las comunicaciones. Los *firewalls* empresariales suelen proporcionar información sobre dirección IP de

los puertos de origen y destino, interfaz, hora y fecha, y regla que causó el evento que desea grabar, además, se puede incluir la dirección IP de NAT y la acción que causó el servidor de seguridad.

Otras herramientas son: Colocación de sensores, *NetFlow* de Cisco y *Net Witness Investigator*.

4. Análisis forense en la nube

El software y los datos de aplicaciones en la nube se almacenan en servidores de terceros no locales para el usuario, que van más allá del control de un investigador al operar a través de diferentes jurisdicciones. Por tanto, la obtención de los datos suele ser ardua y costosa, ya que pueden ser borrados antes de lograr su disponibilidad. La posibilidad de realizar CF exige la disposición de la organización con el fin de posibilitar la evidencia digital potencial, por lo cual es conveniente crear un entorno propicio mediante acuerdos de nivel del servicio (SLAs) con los proveedores de servicios de nube (*Cloud Service Provider*, CSP). Ruan, et al. (2012, 209) y Podestá, et al.(2014), plantean recomendaciones para firmar el SLA: jurisdicción, propiedad de datos, cadena de custodia, notificación de eventos, cumplimiento de las normas y la capacidad de manejo de incidentes.

Según Colombini et al. (2013, 236-252), las tres principales amenazas en la nube, son: violaciones de datos, pérdida de datos y robo de cuentas. Lo anterior, va en contradicción con la capacidad clave del investigador en el análisis forense de computación y de red, quien tiene el control físico, o que puede tomar el control mediante la instalación de un software en el equipo para ser examinado. La falta de control hace que la recolección de evidencia sea un inconveniente para la realización de un análisis forense en la nube.

4.1 Antecedentes técnicos

De acuerdo con Jadeja & Modi (2012, 877), *Cloud Computing* (CC) es un modelo para permitir convenientemente la red por demanda, el acceso a un conjunto compartido de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de gestión o servicio interacción con el proveedor, con características como multialquiler, elasticidad, pago por uso y fiabilidad. Además, los sistemas de nubes son implementados en sistemas de archivos distribuidos que, de acuerdo con Martínez (2010, 175), presentan mejores características frente a sistemas no distribuidos, respecto a la fiabilidad y la escalabilidad del servicio.

Como lo señalan Grispos, Storer & Glisson (2012), un sistema de CC se compone de cliente y lo que está en la nube, relacionados y conectados entre sí. El servidor central vigila el tráfico, administra el sistema y las demandas de los clientes mediante el uso especial de un software, llamado *middleware*, que permite la comunicación entre los equipos conectados. También hay cuatro capas del CC que determinan su arquitectura: cliente, aplicación, plataforma, infraestructura y servidor, que establecen los modelos o servicios que ofrece la nube. A partir de las anteriores capas, considera Mell & Grance (2011), existen tres modelos que se utilizan en el contexto de CC:

- Infraestructura como Servicio (IaaS): El cliente utiliza la máquina virtual proporcionada por el CSP para instalar su propio sistema, mientras el sistema se puede utilizar como cualquier otro equipo físico con algunas limitaciones.
- Plataforma como servicio (PaaS): Proporcionan la capacidad de implementar los paquetes de aplicaciones creadas, usando el entorno de desarrollo virtual admitida por el CSP.
- Software como Servicio (SaaS): El cliente hace uso de un servicio gestionado por la CSP en una infraestructura de *cloud*. En la mayoría de los casos se accede a través de una API para una interfaz de cliente ligero como un navegador web.

4.2 Recolección de Evidencia en la Nube

La adquisición y el análisis de la evidencia digital desde la nube es complejo, debido a la naturaleza de la operación de los sistemas de CC, ya que podrían operar a través de diferentes jurisdicciones. En cuanto a los aspectos técnicos de las investigaciones forenses, la cantidad de evidencia disponible depende de los modelos de servicios y el despliegue de la nube.

4.2.1 Instancia Virtual en la Nube. La Máquina Virtual[7] (MV) dentro de la nube, en la mayoría de los casos, es el lugar donde ocurre un incidente y, por tanto proporciona un posible punto de partida para una investigación forense. La instancia de la máquina virtual se puede acceder a través del hipervisor, el Proveedor de Servicios en la nube (CSP) y el cliente que está ejecutando la instancia. Las instantáneas proporcionan una técnica para el cliente congelando los estados específicos de la máquina virtual. En los escenarios SaaS y PaaS, la posibilidad de acceder a la instancia virtual para la recopilación de información probatoria está altamente limitada.

7 Bem & Huebner (2007) lo señalan como donde los datos se almacenan o se manejan los procesos.

4.2.2 Capa de red. Según lo establecen Lillard et al. (2010, 282–288), las diferentes capas del modelo OSI proporcionan información sobre los protocolos de comunicación y entre instancias dentro de la nube, así como con instancias fuera de la nube. Desafortunadamente, una CSP actualmente no proporciona ningún dato de registro de los componentes de la red, lo que en caso de infección de *malware* de un VM IaaS, será difícil conseguir cualquier tipo de información de enrutamiento. Para Zawoad & Hasan (2013, 18), esta situación se complica en el caso de PaaS o SaaS.

4.2.3 Sistema Cliente. En la capa del sistema del cliente, que depende por completo del modelo utilizado (IaaS, PaaS, SaaS) y donde la evidencia potencial podría ser extraído, el navegador en el sistema cliente es la única aplicación que se comunica con el servicio en la nube, especialmente en las aplicaciones SaaS. Por lo tanto, en una investigación forense, los datos de las pruebas reunidas en el entorno del navegador no deben ser omitidos.

4.2.4. Entornos SaaS. En el modelo SaaS, el cliente no obtiene ningún tipo de control de la infraestructura operativa entregada, como redes, servidores, sistemas operativos, y aplicaciones que se utilice. Los cambios en la configuración de la aplicación específica del usuario se limitan únicamente a que pueden ser controlados, circunstancias que no permiten una investigación forense válida y sin que los clientes de modelos SaaS tengan oportunidad de analizar las incidencias potenciales.

4.2.5 Entornos PaaS. Una de las principales ventajas de este modelo es que la aplicación principal está bajo el control del cliente, permitiéndole dictar cómo la interactúa con otras dependencias (bases de datos, las entidades de almacenamiento, etc.), así como, dependiendo del tiempo de ejecución del medio ambiente, implementar mecanismos de registro, firmar automáticamente la información y transferir a una tercera parte de almacenamiento. Un ejemplo es la Plataforma de Microsoft Azure que, mediante *Diagnósticos de Windows Azure*, permite a los desarrolladores recopilar y almacenar datos de diagnóstico de manera altamente configurable.

4.2.6 Entornos IaaS. A diferencia de los otros modelos, proporciona mucha más información utilizable como pruebas forenses en el caso de un incidente, dependiendo de la capacidad del cliente para instalar y configurar la imagen con fines forenses. Por lo tanto, los datos de registro e información de pruebas podrían ser transferidos a otras máquinas frecuentemente, para proporcionarle capacidad de realizar una investigación si fuese necesario.

5. Conclusiones

La adquisición y el análisis de la evidencia digital en sistemas de computación en la nube más complejo que obtener pruebas digitales en equipos personales o sistemas basados en servidores tradicionales, debido a la complejidad de esta tecnología, por lo tanto la computación en la nube requiere una metodología diferente a las tradicionales.

Los investigadores comúnmente tienen la posibilidad de reconstruir el entorno correspondiente para recrear escenarios y la hipótesis de la prueba, lo que en el mundo de la computación ya no es posible, por lo tanto, los resultados preliminares de la comunidad informática forense tienen que ser revisados y adaptados al nuevo entorno de *cloud computing*.

Datos almacenados de manera distribuida y virtualizada, almacenamiento volátil, falta de servicios en la nube para almacenar pruebas, normas inter-jurisdiccionales, procedimientos y tecnología propia de la nube hace que la ciencia forense digital en la nube se dificulte. Sin embargo, se puede pedir al prestador de servicios que determine contractualmente una ubicación más específica para la información sobre el país, la región, o un determinado centro de datos, así como de asignación de adicional de recursos en relación con la capacidad de almacenamiento, procesamiento, memoria, ancho de banda de la red y de la disposición de máquinas virtuales.

Es importante que las empresas desarrollen buenas prácticas en seguridad que incluyan planes de respuesta a incidentes, que definan políticas y procedimientos que deben ser usados en caso de ocurrir un incidente para preservar la evidencia, que sirva de soporte en un proceso judicial y finalmente, Se deben unir fuerzas en la investigación y el desarrollo de nuevas técnicas forenses, tanto para desarrollar soluciones a los actuales problemas emergentes y encontrar soluciones que sean capaces de satisfacer las necesidades de un investigador forense.

Referencias bibliográficas

ACPO (2009a). Managers guide: Good Practice and Advice Guide for Managers of e-Crime investigation -. Official release v0.1.4. [online]. London (UK): Association of Chief Police Officers, ACPO. 105 p. + appendix <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf> [consult: 11/05/2014]

ACPO (2009b).e-Crime Strategy: version 1.0 [online]. London (UK): Association of Chief Police Officers, ACPO. 20 p. + appendix. <http://www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf> [consult: 20/05/2014]

ACPO (2011). Good practice guide for computer based evidence: Official release version 4.0 [online]. London (UK): Association of Chief Police Officers, ACPO – 7safe information security. 66 p. <http://7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf> [consult: 11/05/2014]

ÁLVAREZ GALARZA, M.D. & GUAMÁN REIBÁN, V.A. (2008). Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional. Tesis de pregrado (Ingeniero de Sistemas). Cuenca (Ecuador): Universidad Politécnica Salesiana, Facultad de Ingenierías. 122 p. + anexos. <http://dspace.ups.edu.ec/handle/123456789/546> [consulta: 09/04/2014].

BEM, D. & HUEBNER, E. (2007). Computer Forensic Analysis in a Virtual Environment [online]. In: International Journal of Digital Evidence, Vol. 6, No. 2. Utica (N.Y., USA): Utica College. p. 1-13 ISSN: 1938-0917. <http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf> [consult: 09/04/2014]

BREZINSKI, D. & KILLALEA, T. (2002). RFC 3227: Guidelines for Evidence Collection and Archiving [online]. Reston (VA, USA): Internet Engineering Task Force, IEFT Trust. 10 p. <https://www.ietf.org/rfc/rfc3227.txt> [consult: 16/09/2013].

BRUSCHI, D.; MONGA, M. & ROSTI, E. (2005).Trusted Internet Forensics: design of a network forensics appliance [online]. In: 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, SecureComm2005 (05-09/09/2005). Athens (Greece): IEEE - CreateNet. p. 33-35. <doi:10.1109/SECCMW.2005.1588292> [consult: 09/04/2014]

CANO, J.J. (2006). Introducción a la informática forense [en línea]. En: Revista de Sistemas ACIS. No 96 (abr-jun). Bogotá (Colombia): Asociación Colombiana de Ingeniería, ACIS. p. 64-73. ISSN: 0120-5919 <http://www.acis.org.co/fileadmin/Revista_96/dos.pdf> [consulta: 10/05/2013]

CARRIER, B. (2013). Autopsy 3.0: Extensible Desktop Digital Forensics, It's not your father's open source software [online]. Bethesda (MD, USA): The SNAS Institute. 40 p. <https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Autopsy-3-Extensible-Open-Source-Forensics-Brian-Carrier.pdf> [consult: 20/07/2014]

CASEY, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 2 ed. San Diego (CA, USA.): Elsevier-Academia Press. 690 p. ISBN: 0121631044

CIARDHUÁIN, S.Ó. (2004). An extended model of Cybercrime Investigations [online].In: International Journal of Digital Evidence, Vol. 3, No. 1 (Summer). Utica (N.Y., USA): Utica College. p. 1-22. ISSN: 1938-0917. <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf> [consult: 10/05/2013]

COLOMBINI, C.M.; COLELLA, A.; MATTIUCCI, M. & CASTIGLIONE, A. (2013). Cyber Threats Monitoring: Experimental Analysis of Malware Behavior in Cyberspace [online]. In: CD-ARES 2013 (02-06/09/2013). Regensburg (Germany): IFIP. CUZZOCREA, A.; KITTL, C.; SIMOS, D.E.; WEIPPL, E. & XU, L. (Eds.) (2013). Lecture Notes in Computer Science (LNCS), Berlin (Germany): Springer Berlin Heidelberg. p. 236-252 <http://link.springer.com/chapter/10.1007%2F978-3-642-40588-4_17#page-2> [consult: 15/11/2014]

CRUZ, J.A. (2007). Herramientas de apoyo para el análisis forense en Computadoras. Proyecto fin de carrera (Ingeniero en Informática). Jaén (España): Universidad de Jaén, Escuela Politécnica Superior de Jaén. 282 p. <http://collection.openlibra.com.s3.amazonaws.com/pdf/Herramienta-de-Apoyo-para-el-analisis-forense-de-computadoras.pdf?AWSAccessKeyId=AKIAIGY5Y2YOT7GYM5UQ&Signature=1%2BPaEA3wieulTl0rUkr%2BoRFzFVw%3D&Expires=1416098014> [consulta: 15/11/2014]

DÁVILA, J. (2008). La informática forense y el cuestionamiento de las evidencias digitales [en línea]. En: Revista SIC, No. 81. Madrid (España): Ediciones CODA. p. 96-98. ISSN: 1136-0623. <http://www.revistasic.com/revista81/pdf_81/sic81_enconstruccion.pdf.pdf> [consulta: 13/09/2013].

DI IORIO, A.H. (2013). La recuperación de la información y la informática forense: Una propuesta de proceso unificado [en línea]. En: Revista Democracia Digital e Governo Eletrônico, No. 8 Florianópolis (Santa Catarina, Brasil): Universidade e Federal de Santa Catarina p. 326-339. ISSN: 2175-9391 <http://buscalegis.ufsc.br/revistas/index.php/observatoriodoegov/article/view/34270/33136> [consulta: 15/1/2014]

EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES, ENFSI (2009).Guidelines for best practice in the forensic examination of digital technology – Version 6 [online].Warsaw (Poland): ENFSI Forensic IT Working Group. 30 p. <http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf> [consult: 07/01/2015]

GHOSH, A. (2004). Guidelines for the Management of IT Evidence [online]. In: 29th Meeting APEC Telecommunications and Information Working Group (21-26/03/2004). Hong Kong (China): APEC. Incidence Response and Forensics Workshop, Doc. No. telwg29/IRF/04a. 26 p. <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf> [consult: 23/11/2013]

GÓMEZ, L.A. (2009). La informática forense, una herramienta para combatir la ciberdelincuencia [en línea]. En: Cuadernos de seguridad, No 11 (feb.). Buenos Aires (Argentina): Presidencia de la Nación. p. 133-150 <http://www.minseg.gob.ar/download/file/fid/893> [consulta: 13/10/2013]

GRISPOS, G.; STORER, T. & GLISSON, W. (2012). Calm before the storm: The challenges of cloud computing in digital forensics [online]. In: International Journal of Digital Crime and Forensics, IJDCF, Vol. 3, No. 2 (apr-jun). Hersshey (PA, USA): IGI Global. p. 28-48. e-ISSN: 1941-6229 <http://www.igi-global.com/viewtitlesample.aspx?id=68408&ptid=59300&t=Calm%20Before%20the%20Storm:%20The%20Challenges%20of%20Cloud%20Computing%20in%20Digital%20Forensics> <DOI: 10.4018/jdcf.2012040103> [consult: 02/05/2015]

GUIDANCE SOFTWARE (2009). Características y funciones de EnCaseForensic: Toda investigación es importante [en línea]. Pasadena (CA, USA): Guidance Software <http://www.ondata.es/recuperar/encase/spanish_webready_encaseforensicfeaturesheet.pdf> [consulta: 21/07/2014]

INFORMATION SECURITY AND FORENSICS SOCIETY, ISFS (2009). Computer forensics. Part 2: Best Practices [online]. Information Security and Forensics Society. Hong Kong (China): ISFS, University of Hong Kong, Department of computer Science. 64 p. <http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf> [consult: 12/06/2014]

ISO27000.ES (2012). Serie 27000 [en línea]. Madrid (España): ISO27000.ES: El portal de ISO 27001 en español <http://www.iso27000.es/iso27000.html> [consulta: 20/09/2015]

JADEJA, Y. & MODI, K. (2012). Cloud Computing- Concepts, Architecture and Challenges. In: International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012 (21-22/03/2012). Kumaracoil (India): IEEE. p. 877-880. ISBN: 978-1-4673-0211-1.

KUBASIAK, R.R. (2007). Macintosh Forensics: A Guide for the Forensically Sound Examination of a Macintosh Computer [online]. Albany (NY, USA): New York State Police. 72 p. <http://www.appleexaminer.com/Downloads/MacForensics.pdf> [consult: 18/07/2014]

LAMPING, U.; SHARPE, R. & WARNICKE, E. (2014). Wireshark User's Guide for Wireshark 99 [online]. Manchester (NH, USA): Wireshark.org. 197 p. <https://www.wireshark.org/download/docs/user-guide-us.pdf> [consult: 20/01/2014].

LILLARD, T.V.; GARRISON, C.P.; SCHILLER, C.A. & STEELE, J. (2010). Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Burlington (MA, USA): Syngress Publishing. 368 p.. ISBN: 978-1-59749-537-0

LÓPEZ, Ó.; AMAYA, H.; LEÓN, R. & ACOSTA, B. (2002). Informática Forense: Generalidades, aspectos técnicos y herramientas [en línea]. En: Primer Congreso Iberoamericano de Seguridad Informática, CIBSI'02 (18-22/02/2002). Morelia (México): Universidad Nacional de México – Instituto Politécnico Nacional – Universidad Politécnica de Madrid. 22 p. <http://www.criptored.upm.es/guiateoria/gt_m180b.htm> [consulta: 23/11/2013].

MARTÍNEZ GOMÁRIZ., E. (2010). Diseño de Sistemas distribuidos [en línea]. Barcelona (España): Universidad de Cataluña, Departamento de Ingeniería de Servicios y Sistemas de Información,

ESSI. 238 p. <http://www.essi.upc.edu/~gomariz/index_archivos/IntroduccionSD-EnricMartinez.pdf> [consulta: 8/01/2014].

MCKEMMISH, R. (1999).What is forensic computing? [online]. In: Trends & Issues, No. 118 (jun). Camberra (Australia): Australian Institute of Criminology. p. 1-6. ISSN: 0817-8542. <http://www.aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf> [consult: 18/10/2013].

MELL, P. & GRANCE, T. (2011). The NIST Definition of Cloud Computing [online].. Gaithersburg (MD, USA): National Institute of Standards and Technology, Information Technology Laboratory. Special Publication 800-145. 7 p. <http://dx.doi.org/10.6028/NIST.SP.800-145> <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [consult: 03/06/2015].

MICROSOFT (s.f.). Protocolo de configuración dinámica de host (DHCP) [en línea]. Redmond (WA, EUA): Microsoft Corporation <https://technet.microsoft.com/es-es/library/cc755282.aspx> [consulta: 23/02/2016]

MOSQUERA GONZÁLEZ, J.A.; CERTAIN JARAMILLO, A.F. & CANO, J.J. (2005). Evidencia Digital: contexto, situación e implicaciones nacionales [en línea]. En: Revista de Derecho, Comunicaciones y Nuevas Tecnologías, No. 1 (abr). Bogotá (Colombia): Universidad de los Andes, Facultad de Derecho. .p. 175-205. ISSN: 1909-7786. https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics90.pdf [consulta: 10/11/2013].

NATIONAL INSTITUTE OF JUSTICE, NIJ (2004).Forensic examination of digital evidence. A guide for law enforcement. Special Report [online]. NIJ Special Report, NCJ 199408 (Apr). Washington DC (USA): U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. 88 p. <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf> [consult: 13/06/2014].

NATIONAL INSTITUTE OF JUSTICE, NIJ (2008). Electronic Crime Scene Investigation: A Guide for First Responders. 2 ed. [online]. NIJ Special Report, NCJ 219941 (Apr). Washington DC (USA): U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. 62 p. <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf> [consult: 15/11/2014].

NOBLETT, M.G. & POLLITT, M.M. (2000). Recovering and Examining Computer Forensic Evidence [online].In: Forensic Science Communications, Vol. 2, No. 4 (oct.). Washington DC (USA): The FBI, Federal Bureau of Investigation. ISSN: 1528-8005 <http://www.fbi.gov/about-us/lab/forensic-science communications/fsc/oct2000/computer.htm> [consult: 23/10/2014].

PODESTÁ, A.; CASTELLOTE, M.; CONSTANZO, B.; WAIMANN, J. & ITURRIAGA, J.I. (2014). Dificultades de Investigaciones Penales en Cloud Computing [en línea]. En: Tercer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática, CIIDDI 2014 (22-23/05/2014). Mar del Plata, (Argentina): Universidad FASTA. Trabajos seleccionados CIIDDI 2014. ISBN: 978-987-1312-59-7 <http://ciiddi.org/congreso2014/images/documentos/dificultades%20de%20investigaciones%20penales%20en%20cloud%20computing%20podest.pdf> [consulta: 18/04/2015].

REAL ACADEMIA DE LA LENGUA (2013). Diccionario de la lengua española (DRAE) [en línea]. Madrid (España): Real Academia Española. <http://buscon.rae.es/drae/?type=3&val=inform%C3%A1tica&val_aux=&origen=REDRAE.>http://lema.rae.es/drae/?val=informática[consulta: 13/10/2013].

RODRÍGUEZ MÁS, F. & DOMÉNECH ROSADO, A. (2011). La informática forense: el rastro digital del crimen [en línea]. En: Derecho y Cambio social, Vol. 8, No. 25. Lima (Perú), p. 1-9. ISSN 2224-4131. <http://www.derechoycambiosocial.com/revista025/informatica_forense.pdf> [consulta: 10/03/2014].

RUAN, K.; JAMES, J.; CARTHY, J. & KECHADI, T. (2012). Chapter 14: Key Terms for Service level agreements to support cloud forensics [online]. In: 8th IFIP WG 11.9 International Conference on Digital Forensics (03-05/01/2012). Pretoria (South Africa): Springer. PETERSON, G. & SHENOI, S. (Eds.). Advances in Digital Forensics VIII, p. 201-212. ISBN: 978-3-642-33962-2 <http://www.springer.com/la/book/9783642339615> [consult: 25/02/2015]

SALINAS, R. (2005). Sistemas de Detección de Intrusos. En: Actualidad TIC, No 6. Valencia (España): Instituto Tecnológico de Informática. p. 12-15. ISSN: 1696 - 5876

SÁNCHEZ BALLESTEROS, C. (2002). Sniffers. En: Sólo programadores, No. 89. Madrid (España): Revistas Profesionales, S.L. p. 72-73. ISSN 1134-4792.

SANTOS JAIMES, L.M. & FLÓREZ FUENTES, A.S. (2012). Metodología para el análisis forense en Linux [en línea]. En: Revista Colombiana de Tecnologías de Avanzada, Vol. 2, No. 20.

Pamplona (Colombia): Universidad de Pamplona, Facultad de Ingenierías y Arquitectura. p. 90-96. ISSN: 1692-7257<http://www.unipamplona.edu.co/unipamplona/portalIG/home_40/recursos/04_v19_24/revista_20/05112012/13.pdf> [consulta: 15/1172014].

SHIREY, R.W. (2007).Internet Security Glossary, Version 2 [online].Reston (VA, USA): Internet Engineering Task Force, IEFT Trust. 365 p. <http://www.rfc-editor.org/rfc/rfc4949.txt> [consult: 23/06/2013].

STANDARDS AUSTRALIA INTERNATIONAL (2003). HB 171-2003: Guidelines for the Management of IT Evidence [online]. Sydney (Australia): Standards Australia International. 34 p. ISBN: 0-7337-2795-6. <http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF>. [consult: 5/10/2013]

UNIVERSIDAD DE MURCIA (2014). Información general (Máster Universitario en Ciencias Forenses) [en línea]. Murcia (España): Universidad de Murcia, Facultad de Biología. <http://www.um.es/web/biologia/contenido/estudios/masteres/ciencias-forenses> [consulta: 15/11/2014]

VERIZON (2012). Data Breach Investigations Report 2012 [online]. New York (NY, USA): Verizon. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf> [consult: 13/10/2013].

VERIZON (2013). Data Breach Investigations Report 2013 [online]. New York (NY, USA): Verizon. <http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf>. [consult: 13/10/2013].

YUPANQUI CHIPANA, E. (2009). Análisis forense en sistemas operativos Linux utilizando The Coroner's Toolkit [en línea]. En: Revista de Información, Tecnología y Sociedad, RITS, No 3. La Paz (Bolivia): Universidad Mayor de San Andrés. p. 57-59. ISSN: 1997-4044.<http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200012&script=sci_arttext> [consulta: 15/11/2014]

ZAWOAD, S. & HASAN, R. (2013). Digital Forensics in the Cloud [online]. In: CrossTolk: The Journal of Defense Software Engineering, Vol. 25, No. 5 (sep-oct). Hill AFB (UT, USA): U.S. Air Force STSC - Lumin Publishing. p. 17-20. e-ISSN: 2160-1593 <http://secret.cis.uab.edu/media/secretlab-journal-2013-1.pdf> <http://static1.1.sqspcdn.com/static/f/702523/23526450/1379483025287/201309-0-Issue.pdf?token=cmUibJRO8K8m2q%2BXJUMUCk%2Bke0Q%3D> [consult: 02/02/2014].