INFORMÁTICA FORENSE: UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA

Autor:

Marco Espinoza Mina[1]

Dirección para correspondencia: mespinoza@ecotec.edu.ec

Fecha de recepción: 25 de marzo del 2019

Fecha de aceptación: 22 de abril del 2019

Fecha de publicación: 4 de mayo del 2019

Citación/como citar este artículo: Espinoza, M. (2019). Informática forense: una revisión sistemática de la literatura. *Rehuso, 4*(2), 112-128. Recuperado de: https://revistas.utm.edu.ec/index.php/Rehuso/article/view/1641

RESUMEN

La ciencia informática forense estudia y analiza una amplia gama de evidencias de delitos, es así que el forense informático requiere de un profundo conocimiento técnico y manejo de herramientas especializadas. El actual trabajo presenta una revisión sistemática cuyo objetivo fue conocer los sistemas informáticos que se usan en esta ciencia y los componentes tecnológicos que más se analizan. Se exponen las soluciones forenses evaluadas científicamente, utilizadas para exámenes en hardware y software, ya sea a través de desarrollos propios o comerciales, aplicados específicamente a las computadoras, redes, dispositivos digitales y la información en la nube; adicionalmente, se despliegan las propuestas de modelos de confiabilidad de evidencias analizadas, con el fin de que el forense informático pueda dar opiniones y emitir informes técnicos, cumpliendo con una correcta metodología forense. Los software comerciales de apoyo a la labor del forense informático, tienen como limitante que van solo dirigidos a un trabajo específico; por lo cual se evidencia que hay mucho por desarrollar en aplicaciones para esta actividad. Otros resultados encontrados señalan que el área legal y la de informática son las que tienen predominio de aplicabilidad de esta ciencia.

Palabras clave: Software forense digital; forense informático; forense digital; evidencia digital.

COMPUTER FORENSICS: A SYSTEMATIC REVIEW OF THE LITERATURE

Abstract

Forensic computer science studies and analyzes a wide range of evidence of crimes, so the IT forensic scientist requires a deep technical knowledge and management of specialized tools. The current work presents a systematic review whose objective was to know the computer systems used in this science and the technological components that are most analyzed. Scientifically evaluated forensic solutions are exposed, used for examinations in hardware and software, either through own or commercial developments, applied specifically to computers, networks, digital devices and information in the cloud; In addition, proposals for models of reliability of analyzed evidence are deployed, so that the computer forensic expert can give opinions and issue technical reports, complying with a correct forensic methodology. Commercial software that supports the work of computer forensics has the limitation that they are only directed to a specific job; therefore it is evident that there is much to

[1] Universidad Ecotec, Ecuador.

develop in applications for this activity. Other results found that the legal area and computer science are those that have predominance of applicability of this science.
Keywords: impact; virtual environment; context; teaching; pedagogical model.

Introducción

En los últimos años se ha presentado un interés creciente sobre la informática forense y el forense informático. Los forenses informáticos tienen a su cargo el descubrimiento y la descripción de la información contenida en un medio digital. Los medios digitales incluyen sistemas informáticos, discos duros, DVDs y otros dispositivos de almacenamiento magnéticos, ópticos y sólidos, así como documentos y archivos digitales, como son los correos electrónicos e imágenes. El campo, de rápido crecimiento, de la informática forense, incluye varias ramas relacionadas con redes de computadoras, bases de datos, dispositivos móviles, entre otros.

Un examen forense puede revelar cuándo fue creado por primera vez un documento en una computadora, cuándo fue editado por última vez, cuándo fue guardado o impreso por última vez y qué usuario llevó a cabo estas acciones. Muchas organizaciones comerciales han utilizado a la informática forense en una variedad de casos tales como: robo de propiedad intelectual, espionaje industrial, disputas de empleo, investigaciones de fraude, falsificaciones, investigaciones de bancarrota, uso inadecuado de correo electrónico y servicios de la internet en el lugar de trabajo.

La informática forense se la identifica como una actividad crítica en muchos procesos judiciales, ya que se puede encontrar evidencia digital que lleva a declarar a alguien inocente o culpable, al analizar el hardware y software reconstruyendo hechos cuando se ha dado un mal uso de ellos.

En el desarrollo del presente trabajo de investigación se determinan las soluciones informáticas usadas por el forense informático en mayor proporción, los dispositivos electrónicos que se analizan dentro de una evaluación forense informática y las áreas en las que más interviene el forense informático.

Una característica positiva de los resultados del análisis comparativo del software forense digital publicado en la literatura científica es la exhaustividad y la base científica, mientras que un aspecto negativo es que a menudo no están actualizados debido al desarrollo de nuevas versiones de software (Stanivukovic y Randjelovic, 2016:2). El propósito de este trabajo es presentar información actualizada sobre las herramientas informáticas disponibles utilizadas en la informática forense, ya que estas herramientas son la base técnica para el forense informático.

Este documento está organizado de la siguiente manera: La sección siguiente presenta el desarrollo de la metodología que incluye la extracción de la información; posteriormente se presenta el resumen de resultados; le sigue su discusión, y finalmente se muestra las conclusiones de este trabajo.

Metodología

En este artículo se presenta una revisión sistemática (RS) de la literatura acerca del tópico de forense informático, siguiendo los lineamientos de Kitchenham (2004), para obtener y evaluar la evidencia disponible perteneciente al tema específico de investigación. Esta revisión sistemática de la literatura permitió identificar, evaluar e interpretar toda la documentación disponible relevante de la pregunta de investigación. Se realizó de acuerdo a una estrategia de selección de fuentes con criterios de inclusión y exclusión, y una búsqueda predefinida, con lo cual se identificó y procesó todas aquellas investigaciones que respaldan el presente resultado sistemático sintetizado.

Definición de la pregunta de investigación

Para conocer las aplicaciones informáticas, las características y las áreas en las que más se desarrolla la labor del forense informático, se definió la siguiente pregunta: ¿Cuáles son las aplicaciones (programas) disponibles en informática forense y qué componentes tecnológicos son los que más analizan?

Como palabras claves se utilizaron: software forense digital, forense informático, forense digital y evidencia digital.

La pregunta de investigación planteada se subdividió en las siguientes, con el objeto de concretarla un poco más:

• ¿Las aplicaciones tecnológicas forenses están dirigidas a analizar tanto el hardware como el software de los equipos?

• ¿Las soluciones encontradas son desarrollos a medida, aplicaciones abiertas o software comerciales?

• ¿Cuáles son las áreas o sectores en los que más han sido aplicadas las habilidades y destrezas del forense informático?

Selección de fuentes

Se realizaron búsquedas en las siguientes bibliotecas electrónicas: EBSCOhost (EBS), IEEE Xplore (IEEEX), Springer y ERIC, esta lista de fuentes bibliográficas fue elegida por la experiencia de uso de los autores en el área de la revisión sistemática, las cuales son comúnmente utilizadas para investigaciones en el ámbito de la computación e informática y con la posibilidad de consultar documentos libres en formato digital. Adicionalmente, las fuentes bibliográficas seleccionadas tenían que contar con un motor de búsqueda que permita ejecutar consultas de búsqueda avanzada.

Estrategias de búsqueda

- Se seleccionaron una serie de términos y palabras claves para responder a la pregunta ¿Cuáles son las aplicaciones disponibles para realizar informática forense y qué componentes tecnológicos son los que más analizan? y así, obtener los resultados esperados.
- La estrategia de búsqueda se basó en las palabras "computer forensics" y "digital forensics".
- La cadena de búsqueda estructurada fue: “computer forensics” OR “digital forensics”.
- Se aplicó la cadena de búsqueda solo al título de los artículos, en cada una de las bibliotecas electrónicas y cuando contenía las palabras definidas, se obtenía y revisaba el artículo.
- La temporalidad de las publicaciones fue desde el año 2014.
- Los tipos de publicaciones fueron conferencias, conferencias internacionales, workshops internacionales y artículos de revistas.
- Los artículos debían ser escritos en idioma inglés.

Criterios de inclusión y exclusión

Criterios de inclusión:

- Artículos publicados entre los años 2014 y 2018.
- Artículos cuyos títulos tuvieran la expresión “computer forensics” o su sinónimo “digital forensics”.
- Contenidos específicos sobre “computer forensics”.
- Artículos de conferencias, revistas y “workshops” internacionales.

Criterios de exclusión:

- Trabajos en diapositivas y libros.
- Literatura gris, que corresponde a artículos no publicados.
- De los artículos repetidos en varias bibliotecas digitales, solo se seleccionó uno de ellos.

Extracción de información y revisión de trabajos

Para el proceso de extracción y revisión de los trabajos de investigación se asumió que la calidad de los mismos estaría garantizada por la evaluación que realizan las propias fuentes bibliográficas de donde se los tomó, ya que las plataformas generan sus resultados de búsqueda por orden de relevancia. Para la recopilación se tomaron solo aquellos que estuvieron relacionados a la pregunta de investigación.

Con respecto al procedimiento para seleccionar los estudios, se aplicó la cadena de búsqueda exclusivamente en el título de la publicación. En la mayoría de artículos se requirió revisar el contenido completo, después de haber aplicado todos los criterios de búsqueda.

En la selección inicial de estudios se realizó la ejecución de las búsquedas, con la cadena: "computer forensics" OR "digital forensics", lo cual arrojó una gran cantidad de documentos, por lo cual procedió a aumentar los criterios de búsqueda para reducir los resultados.

La segunda búsqueda fue basada en aplicar la cadena de búsqueda en el campo por "título", esto permitió eliminar algunos resultados no útiles, pero todavía no resultaba suficiente para satisfacer la limitante de investigación. Finalmente, para obtener la lista definitiva de estudios primarios, se añadió un filtro de solo los artículos académicos y con texto completo.

La búsqueda en las bases arrojó 5.415 entradas de publicación. EBSCOhost devolvió 455 estudios, Springer con 2.512, ERIC con 103 e IEEE Xplore con 2.345 estudios. Los títulos de los estudios fueron inspeccionados para encontrar duplicados entre los motores de búsqueda. Después de eso estaban listos para ser filtrados por los criterios de exclusión explicados anteriormente, arrojando un total de 32 artículos para realizar la revisión. Los resultados se resumen en la tabla 1.

Tabla 1. Número de estudios de la revisión sistemática, con cadena de búsqueda entre el año 2014 y 2018

Criterio de búsqueda	Número de artículos
Sin filtros	5.415
Con cadena de búsqueda en el "título"	276
Con filtro texto completo y publicaciones académicas	32

Fuente: Elaboración propia.

Al revisar los artículos filtrados según los criterios de exclusión, se encontró que algunos fueron conferencias que se excluyen porque no están escritas como trabajos científicos. Después de leer el resumen de los estudios, algunos no estaban relacionados con el objetivo de esta revisión sistemática y se decidió excluirlos. Además, no se tuvo acceso a algunos estudios, debido a que eran artículos por los cuales se debía pagar, incluso después de pedir ayuda a otros profesionales del área con diferentes accesos y visitar otras bibliotecas, estos estudios no fueron inspeccionados en esta revisión sistemática. Al final, 21 estudios fueron revisados y analizados en su totalidad.

Resultados

El proceso de lectura se centró en encontrar respuesta a la pregunta planteada, con lo cual se encontraron tres tipos de resultados: uno que indica que las soluciones encontradas son en su mayoría desarrollos propios, luego siguen los son software comerciales y resto hace uso de código abierto;

otro que indica que las aplicaciones tecnológicas están dirigidas a analizar tanto el hardware como el software en semejantes proporciones, y el último resultado corresponde a las áreas de aplicación de la informática forense en las que se centran los estudios científicos, siendo estás el área legal, comercial e informática.

Se leyeron los resúmenes y las introducciones de cada artículo, cuando no era suficientemente claro el resultado, se leía parte o la totalidad de la descripción o formulación del estudio realizado. En muchos casos no era necesario leer el artículo completo. En la sección de conclusiones se buscaba también la descripción de trabajos futuros con el fin de conocer nuevos problemas abiertos o nuevas direcciones de investigación. Después de leer todos los estudios, se organizaron para facilitar nuevamente su lectura y análisis.

En la tabla 2 se presenta el listado de los artículos seleccionados para realizar la revisión, el año de publicación, si se trata de un desarrollo propio y los medios y herramientas de software analizados.

Tabla 2. Listado de artículos seleccionados con sus años de elaboración, en el que se indica si es desarrollo propio y los medios analizados junto con las herramientas propuestas.

Trabajo	Año	Desarrollo propio Si/No	Medio analizado y herramienta	
			Hardware	Software
A fast source-oriented image clustering method for digital forensics	2017	Si	Dispositivos con cámara	Algoritmo
Special Issue on Mobile Systems, Mobile Networks, and Mobile Cloud: Security, Privacy, and Digital Forensics	2017	No	Celulares, redes públicas	
An Ontology-Based Transformation Model for the Digital Forensics Domain	2017	Si	Computadoras	Algoritmo para transformación de documentos a XML
Application of multiple criteria decision making in the selection of digital forensics software	2016	Si		Expert Choice computer program para realizar la selección de software de apoyo
Scenario-Based Digital Forensics Challenges in Cloud Computing	2016	No	Red, nube	
METRICS-BASED Risk Assessment and Management of DIGITAL FORENSICS	2016	Si	Computadoras, nube	Algoritmos de modelos de análisis digital
Challenges in digital forensics	2016	Si	Computadoras	Encase y Forensic Toolkit (FTK) para análisis
Museums Go High-Tech with Digital Forensics	2014	Si	Computadora tomográfica, Escaneo CT	Sistema de Tomografía Computarizada

General Evaluation and Requirement of Computer Forensics Education	2016	No	Computadoras	Computer Forensic
Computer forensics: an overview	2016	No	Computadoras	Capacitaciones para Digital forense
Digital Forensics Capabilities in an Open Source Framework	2015	Si	Computadoras	Software premium, DDF - Digital Forensics Framework es un código abierto
On the Digital Forensics of Heavy Truck Electronic Control Modules	2014	Si	Computadoras de camiones pesados	Software electronic control modules (ECMs), Archivos XTR
Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics	2014	Si	Computadoras	Software para recuperación de evidencia TSI
Cybercrime and digital forensics – technologies and approaches	2014	No aplica	No aplica	No aplica
Review of Evidence Collection and Protection Phases in Digital Forensics Process	2017	Si	Computadoras	Proceso digital forense para control de información
The Application of Peer Teaching in Digital Forensics Education	2014	No aplica	No aplica	No aplica
The Future of Digital Forensics: Challenges and the Road Ahead Digital Forensics	2017	No	Teléfonos inteligentes y dispositivos portátiles	Sistema de parámetros multidisciplinario para reunir evidencia
Digital Forensics of Microsoft Office 2007–2013 Documents to Prevent Covert Communication	2015	Si	Computadoras, Teléfonos inteligente, Internet	Software para llevar a información a documentos en formato OOXML.
Trustworthy Digital Forensics in the Cloud	2016	No	Computadoras, máquinas virtuales	Método de análisis de información
A study on memory dump analysis based on digital forensic tools	2015	Si	Disco duro, memoria flash	Sistema para analizar la memoria física, Sistema operativo Windows 7, xp, Linux
A granular approach for user-centric network analysis to identify digital evidence	2015	No	Teléfonos celulares, computadoras	'Vizster' y 'Prefuse' , SNIMforensically, Redes sociales, Google Talk, mensajes de texto

Fuente: elaboración propia

Soluciones de informática forense aplicadas a estudios de hardware y software

A la hora de realizar un estudio, el forense informático debe contar con una serie de herramientas para realizar su actividad. Se debe considerar: complejidad, tiempo de análisis a invertir, riesgo de pérdida o destrucción de evidencias y lo que se conoce como "forensically sound" que representa la fiabilidad; esto es solo un énfasis adicional, ya que todas las herramientas y técnicas deben tener una fiabilidad contrastada, tanto para el hardware como para el software.

Del total de artículos científicos revisados se encontró que los 21 artículos dirigen sus soluciones propuestas al software; de los cuales 12 tanto a hardware como a software; en 7 artículos las soluciones están enfocadas en buscar modelos de procesos para la confiabilidad de evidencia, ver tabla 3.

En el artículo de Li y Lin (2017:8), se evidencia el desarrollo de algoritmos propios, ya que indican lo siguiente: Se llevó a cabo los experimentos en la base de datos de imágenes de Dresde. 7400 imágenes adquiridas en formato JPEG por 74 cámaras (cada una responsable de 100 imágenes), que abarca 27 modelos de cámara y 14 fabricantes; por lo que, para probar su algoritmo desarrollado recurrieron a esta información.

"El análisis forense digital requiere la capacidad de manejar varias entidades de hardware y software, desde memoria RAM hasta almacenamiento masivo USB y archivos. Por lo tanto, la comunidad de investigación ha intentado acordar formatos, esquemas y ontologías estándares" (Caviglione, Wendzel, y Mazurczyk, 2017, p.14).

Las investigaciones sobre delitos informáticos buscan el procesamiento de la información de manera colaborativa y adecuada entre el hardware y el software, es por esto que los investigadores muestran además modelos que se pueden aplicar en el momento de realizar la revisión de la evidencia.

Tabla 3. Soluciones propuestas para hardware y software

Clasificación	Número de artículos	Artículos
Hardware y software	12	(Li y Lin, 2017), (Chen, Li, y Haddad, 2017), (Stanivukovic y Randjelovic, 2016), (Subbaraman, 2014), (Rajesh y Ramesh, 2016), (Johnson, Daily y Kongs, 2014), (Syambas y El Farisi, 2014), (Cisar, Cisar, y Bosnjak, 2014), (Varol, 2017), (Fu, Sun, y Xi, 2015), (Seo, Lee y Shon, 2015), (Yasin, Qureshi, Kausar, Kim, y Seo, 2015)
Modelos para confiabilidad de evidencia	7	(Govan, 2014), (Zawoad y Hasan, 2016), (Grigaliunas, Toldinas, y Venckauskas, 2017), (Miranda, Moon, y Park, 2016), (Vincze, 2016), (Merve, İbrahim, y Hüseyin, 2016), (Bubulan, 2015)

Fuente: elaboración propia

Desarrollos propios

Los desarrollos propios encontrados, en la mayoría de las ocasiones se trata de un software a medida que ha sido diseñado para un usuario específico, sea este una empresa o un profesional como el forense informático, que le sirve de apoyo al solicitante adaptado específicamente a su forma de trabajar y necesidad. Siempre, busca complacer todos los requerimientos y adaptarse lo mejor posible a lo que una empresa o persona necesita. Entre las ventajas se encuentran: reducción de los gastos, ahorro de tiempo, garantía de calidad, facilidad de mantenimiento.

En la revisión sistemática se encontró que en doce artículos se plantean desarrollos propios, donde se muestran los algoritmos que buscan aligerar las actividades del forense informático.

Grigaliunas, Toldinas, y Venckauskas (2017), proponen en su artículo, crear un modelo de transformación basado en la ontología para el dominio de la investigación forense y desarrollar un sistema para expertos en informática forense en sus respectivos dominios, para el uso de herramientas en investigaciones de pruebas digitales con la trasformación de documentos XML.

La herramienta del medidor de riesgo proporciona los medios para identificar áreas donde el riesgo puede ser minimizado, así como brindar el asesoramiento de mitigación objetivo basado en dólares. Se generará un índice numérico prototipo que facilitará los protocolos y procedimientos adecuados para garantizar que se cumplan los estándares legales de prueba y admisibilidad (Sahinoglu, Stockton, Barclay y Morton, 2016, p. 154).

Con los rápidos cambios que se presentan en los equipos tecnológicos también deben mejorar y cambiarse los estándares forenses, las prácticas, herramientas y técnicas, además de los software desarrollados.
A continuación, se presenta la nómina de los autores de los doce artículos que muestran desarrollos propios: Li y Lin (2017), Grigaliunas, Toldinas y Venckauskas (2017), Stanivukovic y Randjelovic (2016), Sahinoglu, Stockton, Barclay, y Morton (2016), Subbaraman (2014), Bubulan (2015), Johnson, Daily y Kongs (2014), Syambas y El Farisi (2014), Varol (2017), Govan (2014), Fu, Sun y Xi (2015), Zawoad y Hasan (2016).

Soluciones de código abierto y comerciales evaluadas
En las investigaciones forenses digitales se presentan regularmente situaciones muy particulares y complejas, debido a este hecho, es necesario elegir y usar un software forense digital óptimo para cada etapa de la investigación, con el fin de cumplir con un análisis formal y adecuado, para llegar a la correcta presentación y posterior interpretación de la evidencia encontrada.

En los artículos se encontró que los autores mencionan y revisan los aplicativos siguientes:
EnCase Enterprise v4: realiza soporte de encriptación, de Apple File System y capacidades de copia instantánea de volumen, son características diseñadas para ayudar a recopilar y analizar la evidencia que necesita el forense informático, de manera eficiente y precisa.

FTK imager 3.1.1: es una herramienta de obtención de imágenes y vista previa de datos utilizada para adquirir evidencia de manera forense mediante la creación de copias de datos sin realizar cambios en la evidencia original.

WinHex 18.5: es una herramienta avanzada para inspeccionar y editar todo tipo de archivos, recuperar archivos eliminados o datos perdidos de discos duros con sistemas de archivos corruptos o de tarjetas de cámaras digitales.

Stanivukovic y Randjelovic (2016), indican en su artículo que de estos tres programas para realizar su evaluación y aplicando los criterios de optimización pudieron elegir el mejor software para la actividad que realizan. Siendo EnCase Enterprise v4 el mejor y más óptimo, de acuerdo al método del proceso de jerarquía analítica, que ellos aplicaron para llegar a esta conclusión.

DFF – Digital Forensic Framework: es un software de código abierto informático forense, utilizado por profesionales y no expertos para recopilar, preservar y revelar evidencia digital sin comprometer los sistemas y datos. En el artículo de Bubulan (2015), se indica que usan esta solución de código abierto porque tienen un rápido desarrollo y al tener la comunidad de desarrolladores que las respalda constituye una gran ventaja; muestra grandes capacidades que cumplen con excelentes funciones de investigación.

Open Cloud Forensics (OCF), modelo y arquitectura FECloud: solución propuesta por Zawoad y Hasan (2016:80), contiene el módulo editor de pruebas, que propaga de forma periódica y pública, las pruebas de registros, posesión de datos, verificación de marca de tiempo y procedencia en la Web. Las pruebas verifican todo el sistema de información almacenada electrónicamente. Cuando una

prueba es públicamente disponible, los investigadores no pueden alterar ninguna información o proporcionar evidencia falsa sin que se detecte.

Vizster: es una herramienta de visualización interactiva para redes sociales en línea que permite explorar la estructura de la comunidad de servicios de redes sociales, admite una serie de características de búsqueda exploratoria, que proporcionan visualización de los datos de perfil.

Prefuse: es un entorno de software basado en Java extensible para la creación interactiva de aplicaciones de visualización de la información. Puede utilizarse para crear aplicaciones independientes, componentes visuales y applets, pretende simplificar los procesos de visualización, control y asignación de datos, así como la interacción del usuario.

Yasin, Ahmad, Kausar, Kim y Seo (2015), usaron en su artículo las aplicaciones Vizster y Prefuse, para seleccionar nodos y bordes específicos mediante la aplicación de filtros específicos en la red, y para preservar la privacidad de los actores dentro del conjunto de datos, utilizaron las identificaciones de chat simbólicos en lugar de direcciones de correo electrónico reales para identificar de forma exclusiva a los actores/nodos.

Archivo de formato OOXML: formato de archivo abierto y estándar cuyas extensiones más comunes son .docx, .xlsx y .pptx. Se lo utiliza para representar y almacenar hojas de cálculo, gráficos, presentaciones y documentos de texto.

Fu, Sun y Xi (2015) proponen una herramienta forense para documentos de formato OOXML para investigar los posibles métodos de ocultación de información, el objetivo es evitar la comunicación encubierta y proporcionar tecnología de detección de seguridad para los documentos electrónicos que descargan los usuarios.

A la venta se encuentran algunas aplicaciones para análisis forense de evidencias, ya que no hay una sola solución para todos los problemas en las investigaciones forenses; por lo tanto, muchos software especializados dentro de la informática forense han surgido y continúan surgiendo. Algunos están dirigidos a atender el análisis forense de redes, es decir que se ocupan de las investigaciones en las infraestructuras de red; otros al análisis forense de correos electrónicos, como su nombre indica, investiga los casos relacionados con el correo electrónico; también se encuentran soluciones para el forense móvil que se especializa en dispositivos de mano.

Según Sridhar, Bhaskari y Avadhani (2011), se presentan varios tipos de investigación forense digital, tales como: “system forensics”, “network forensics”, “web forensics”, “data forensics”, “proactive forensics”, “e-mail forensics”, “enterprise forensics”, “cyber forensics”, “digital forensics”; por lo cual son muchos los campos en los cuales se desenvuelve el forense informático y se necesitan soluciones informáticas que apoyen esta labor. Es así, que en cinco de los artículos revisados la investigación está dirigida a las “network forensics”, tres artículos a los “system forensics” y el resto a los otros tipos de investigación previamente señalados.

Medios analizados

En los artículos revisados se encontró que los medios más analizados y motivos de estudios fueron las computadoras y dispositivos móviles, las redes y la nube. Siendo también analizados los archivos creados por el usuario.

Cuando se analizan computadoras o dispositivos móviles se encuentran dos escenarios, el uno que corresponde a “logs”, que son un registro de eventos de un sistema durante un periodo de tiempo en

particular. Los profesionales en seguridad informática usan un log para conocer datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un equipo en particular o aplicación. El otro escenario es cuando se analizan los archivos creados por el usuario, tales como archivos con extensiones .docx y .xlsx, entre otros.

Al analizar las redes de computadoras se puede encontrar un escenario complejo, pues es necesario comprender la manera de cómo los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Se encuentra en los artículos científicos evaluados, que la mayoría de los entendidos, dirigen su investigación a analizar información de computadoras, redes, teléfonos celulares y de la nube. Con el uso creciente de computadoras, muchas suelen convertirse en víctimas de crímenes relacionados con la informática. Los crímenes informáticos pueden entenderse bien conociendo las diversas amenazas a la seguridad (Rajesh y Ramesh, 2016, p.1).

Señalan Chen, Li y Haddad (2017), que en los últimos años, se ha sido testigo de un rápido crecimiento en la cantidad de dispositivos móviles e inteligentes en el mundo. Si bien los dispositivos móviles se convierten en una parte indispensable de la vida cotidiana, ha aumentado la preocupación por su seguridad y privacidad. En particular, los métodos de autenticación tradicionales, como la contraseña, el PIN o el patrón de deslizamiento de pantalla táctil, adolecen de diversos tipos de ataques.

En la nube, los datos de un solo usuario pueden estar en cientos de servidores físicamente dispersos, en sistemas que utilizan diferentes arquitecturas en la nube. Además, no hay un formato estándar para los diversos tipos de registros o la información que deben contener. Todo esto puede hacer que recopilar evidencia sea desafiante (Zawoad y Hasan, 2016). Se encuentran soluciones que marcan y almacenan ciertos documentos dentro de las organizaciones que se consideran relevantes en un litigio futuro.

Áreas de mayor aplicación de la ciencia forense

En la revisión realizada se evidencia que las áreas en las que más interviene el forense informático son en la informática y la legal; el análisis realizado por el profesional en mención es principalmente para dar cumplimiento a la ley, pero actualmente se practica cada vez más en el mundo corporativo empresarial para encontrar evidencia de actividades no relacionadas con las laborales y comerciales. Grigaliunas, Toldinas, y Venckauskas (2017) indican que el análisis forense digital no es una disciplina limitada a las agencias de justicia o aplicación de la ley. Cada vez más organizaciones privadas incluyen departamentos forenses en sus equipos, con el objetivo de aumentar la seguridad general de su infraestructura.

En algunos artículos encontrados, los estudios indican que se analiza la evidencia no solo para dar cumplimiento a la ley, sino que indican que el análisis forense digital se utiliza en el lugar de trabajo.

> De esta manera, las empresas privadas y también las instituciones gubernamentales, pueden establecer cómo se usan sus computadoras. Puede conocerse claramente qué intenciones tiene un empleado cuando usa la computadora: propósitos de la compañía o propósitos personales. Los archivos de registro de la computadora y las cookies y el caché de Internet son las primeras ubicaciones donde los investigadores buscarán (Bubulan, 2015, p. 61).

Vincze (2016), señala que si bien los organismos de administración de justicia publican directrices para buscar y confiscar computadoras, y obtener evidencia electrónica en investigaciones criminales,

en realidad, las escenas del crimen pueden ser impredecibles. Adicionalmente, muchas veces las órdenes de búsqueda e incautación no pueden completarse de antemano con una gran precisión, por ello el desarrollo del proceso forense digital es complejo.

Sahinoglu, Stockton, Barclay, y Morton (2016), manifiestan que cumpliendo con las leyes, en actividades de carteles de drogas, lavado de dinero, incluso en casos de homicidio, se puede deducir mucha evidencia útil mediante el uso de información forense digital.

El predominio de las investigaciones analizadas en este artículo son dirigidas al área de la informática, ya que se encuentran soluciones para análisis al hardware y al software, además se han desarrollado modelos de confiabilidad de evidencia que facilitan la labor del forense informático. El problema en el campo de la informática forense, justamente es la falta de estándares universalmente aceptados que cualquiera pueda ver y al menos tener una idea del nivel de competencia del experto (Vincze, 2016).

> La existencia de pruebas, incluida la evidencia digital, es fundamental en la investigación de casos de delitos informáticos porque con esta evidencia, el investigador y el analista forense pueden descubrir un caso con una cronología completa y luego identificar a alguien como sospechoso y posiblemente formalizarlo posteriormente. Según la ley en Indonesia, la evidencia digital se puede dividir en los siguientes tipos: archivo lógico, archivo de audio, archivo eliminado, archivo de video, archivo perdido, archivo de imagen, archivo slack, correo electrónico, archivo de registro, nombre de usuario y contraseña, archivo encriptado, SMS, MMS, BBM, archivo de esteganografía, registro de llamadas y archivo de oficina (Syambas y El Farisi, 2014, p. 144).

Los avances tecnológicos y la proliferación de nuevos servicios explican un aumento dramático en la complejidad que los profesionales forenses deben manejar. Específicamente, la evidencia ya no se limita a un solo host, sino que se disemina entre diferentes ubicaciones físicas o virtuales, como redes sociales en línea, carteras de criptomonedas, maquinaria "CaaS", recursos en la nube y unidades de almacenamiento personal conectadas a la red. Por esta razón, se necesita más experiencia, herramientas y tiempo para reconstruir completa y correctamente la evidencia (Caviglione, Wendzel y Mazurczyk, 2017).

A nivel legal, Miranda, Moon, y Park (2016), indican en su artículo, que las restricciones jurisdiccionales y la falta de cooperación internacional hacen que las investigaciones transfronterizas sean costosas en tiempo y valor. En consecuencia, se necesita una cooperación internacional más sólida para la ciencia forense de la nube.

Discusión

El trabajo de investigación se ha realizado en base al método de revisión sistemática explicado en la sección anterior; no se incluye ninguna evaluación de la calidad de la literatura revisada; la única consideración relacionada con la calidad de un documento es la cantidad de artículos dentro de la literatura que se cita en este trabajo.

El propósito de este estudio fue proporcionar una visión general del campo del forense informático, al revisar y analizar la literatura publicada, lo que permite llegar a un conocimiento de los programas de cómputo disponibles para realizar actividades relacionadas a la informática forense, y qué componentes tecnológicos son los que más analizan estos expertos.

Existen un número bastante amplio de soluciones para analizar tanto hardware como software; son mayoritarios los documentos científicos encontrados, entre los evaluados en la revisión sistemática

de literatura y los no seleccionados, en los cuales se exponen desarrollos propios, es decir programación hecha a la medida por especialistas, para dar solución a problemas o necesidades específicas.

Por ejemplo, el sistema, Two-Step Injection (TSI), desarrollado y propuesto por Syambas y El Farisi (2014) que utiliza un método de clonación que conserva los metadatos originales y cumple la cadena de custodia para proporcionar pruebas aceptables, originales, completas y confiables. El proceso de copiado y clonación se realizó en la instalación del módulo de contenidos, copia del historial de acceso a internet de Firefox y Chrome, copia de archivos de Yahoo Messenger; clonación de los archivos de las carpetas "Mis documentos" y "Mis imágenes". Esto proporciona una clonación exitosa de los datos para que puedan ser utilizados como evidencia válida en la corte.

En los artículos revisados se señala que al programar aplicaciones propias, a medida, que apoyan a los forenses informáticos en la labor realizada, se encuentran como ventajas: reducción de los gastos, ahorro de tiempo, garantía de calidad, facilidad de mantenimiento. Para las necesidades de investigaciones forenses digitales particulares, es necesario elegir y usar el software forense digital óptimo para cada etapa de la investigación, teniendo en cuenta que los criterios y subcriterios de optimización deben satisfacer las necesidades de cada etapa de la investigación. (Stanivukovic y Randjelovic, 2016).

En un proceso forense digital, exactamente lo que se está buscando y cómo lo buscan depende de muchos factores, incluida la naturaleza del dispositivo, la de la supuesta actividad y el software instalado. Los examinadores de evidencia digital deben poder recuperar información de varios modelos de teléfonos celulares (por ejemplo, Android, Apple y Blackberry), computadoras de escritorio, computadoras portátiles, tabletas, dispositivos de almacenamiento externo, localizadores de GPS y varios otros dispositivos. Los métodos, herramientas y técnicas que son adecuados para un propósito, no se pueden seleccionar sin una comprensión adecuada de los requisitos de la consulta (Vincze, 2016).

Adicionalmente, se plantean otras formas de desarrollo a medida, las cuales dan facilidades a las actividades forenses informática, como la creación de un algoritmo de clave simétrica fuerte, utilizando una clave de 128 bits generada aleatoriamente, expuesto por Johnson, Daily y Kongs (2014), para el control electrónico de camiones pesados; la clave simétrica se descifra y se usa para descifrar el informe; debido a que los datos están fuertemente encriptados, no pueden ser alterados o manipulados de manera significativa sin ser detectados. Esto significa que si incluso 1 bit se modifica en el archivo cifrado, entonces todo el contenido del archivo descifrado no tendrá sentido y los valores de hash no coincidirán en los módulos de control electrónico de camiones pesados y los datos no son válidos para el análisis forense.

Entre las aplicaciones genéricas más empleadas se encuentra DFF, que es un marco de código abierto en el mercado forense digital. Los profesionales de la seguridad, los examinadores de la ley, los estudiantes o un usuario básico de computadoras tienen acceso a las últimas funciones de la industria forense digital de forma completamente gratuita. Más que eso, tienen la oportunidad de contribuir y desarrollar el software para satisfacer todas las necesidades (Bubulan, 2015).

Los software comerciales que los autores revisan en sus artículos y que apoyan la labor del forense informático, tienen como limitante que van solo dirigidos a una labor específica; por lo cual ellos también coinciden en que hay mucho por desarrollar en aplicaciones para este enfoque. Por ejemplo, los métodos de autenticación tradicionales, como la contraseña, el PIN o el patrón de deslizamiento de pantalla táctil, adolecen de diversos tipos de ataques de ingeniería social. Por lo tanto, es conveniente aprovechar otros tipos de métodos de autenticación para proteger mejor los dispositivos

móviles. (Chen, Li, y Haddad, 2017). Los dispositivos móviles son los equipos que más se analizan y a donde van dirigidos los algoritmos desarrollados, y al ser de evolución constante conlleva a que no tengan una absoluta seguridad y privacidad por lo que adolecen de ataques constantes de filtración de información y virus.

Ya sea que se evalúen las aplicaciones de tipo código abierto, gratuitas, comerciales o desarrollos a medida, lo cierto es que día a día crece el número de estas herramientas informáticas forenses; en el artículo de Rajesh y Ramesh (2016) se mencionan herramientas informáticas forenses: Encase, Sleuth Kit, SANS Investigative Forensics Tool Kit (SIFT), X-ways Forensics y Oxygen Forensics Suite; las cuales suman a las valoradas en los trabajos de investigación seleccionados.

Si bien el área de aplicación a la que van dirigidos muchos de los estudios evaluados, es en la misma ciencia informática, es decir son investigaciones que aportan a las herramientas de hardware y software que serán utilizadas genéricamente, se pensaría que el forense informático solo necesita saber de computación, sin embargo, el análisis forense digital moderno es un esfuerzo multidisciplinario que abarca varios campos, incluidos el derecho, la informática, las finanzas, las redes, la minería de datos y la justicia penal.

Los profesionales enfrentarán cada vez más un conjunto mixto de desafíos y problemas relacionados con la eficiencia del procesamiento de pruebas digitales y los procedimientos forenses relacionados (Mazurczyk, Caviglione y Wendzel, 2017); siendo estos protocolos requeridos, propuestos como solución por los especialistas, como modelos de confiabilidad de evidencia. Se requiere adicionalmente, una internacionalización de las políticas jurídicas para pedir una orden judicial, así como para la recolección de evidencia digital y presentación de informes ante la justicia de los países involucrados en un delito que trascienda fronteras.

Como ya se señaló, el campo de la tecnología presenta rápidos cambios que también hacen mejorar y cambiar los estándares y las prácticas forenses. La necesidad de educar a personas calificadas para luchar contra estos crímenes ha surgido a medida que las tasas de criminalidad del ciberespacio aumentan día a día (Merve, İbrahim, y Hüseyin, 2016). Las mejoras y cambios llegan también a las herramientas y técnicas, además de a los software desarrollados, que en muchos casos llevan a inversiones costosas que no son recuperables de manera fácil e inmediata.

Además de haber abordado las preguntas de investigación y proporcionar una visión general en el área del forense informático, también en la revisión se encontraron varios elementos complementarios que aportan al conocimiento de esta ciencia y su evolución. Miranda, Moon y Park (2016) señalan, que se han identificado un total de 20 desafíos de escenarios forenses digitales en la nube, de los cuales siete son legales, nueve arquitectónicos y cuatro técnicos, y proporcionan posibles soluciones para superarlos.

Para los desafíos técnicos, propone la minería de datos, el análisis forense móvil y las redes sociales. Para desafíos arquitectónicos, son útiles el uso de análisis forense móvil, análisis forense en vivo y técnicas personalizadas en la nube. Para superar los desafíos legales, se necesita una mayor cooperación internacional, asesoramiento legal y capacitación.

La investigación forense informática tiene muchos años en el medio, sin embargo, la brecha entre los delitos informáticos y los medios para responder a ellos todavía existe. La continua falta de acuerdo sobre definiciones, los procesos estandarizados y los estándares de acreditación están impidiendo el crecimiento de la informática forense en una disciplina científica madura. Esto tiene consecuencias para la credibilidad de la disciplina ante los ojos de la ley y, por lo tanto, el enjuiciamiento exitoso de

casos. La ocupación previa con el enfoque mecanicista de "copiar todo sin alterar el original, analizar la copia, presentar hallazgos incuestionables" es problemática: conlleva el riesgo de que se pierdan pruebas valiosas al no investigar alternativas como la reconstrucción del entorno investigado, memoria forense y análisis de sistemas en vivo (Bem, Feld, Huebner, y Bem, 2008).

Si bien ahora se han visto tres generaciones distintas de herramientas informáticas forenses: pasada, presente y futura, la ciencia forense se encuentra en una etapa no consolidada en su aplicación. La idea de pioneros forenses como el Dr. Edmond Locard sigue siendo tan relevante ahora como lo fue en 1923. A menudo se dice que la seguridad de la información es un proceso y no un producto, y esto también se aplica a la informática forense. Lo que es seguro es que la capacitación adecuada, junto con el acceso a las mejores herramientas y metodologías, es primordial (Culley, 2003).

Conclusiones

En esta revisión se encuentra que trece artículos proponen soluciones para análisis de hardware y software al mismo tiempo. Son varios los autores que han desarrollado algoritmos y sistemas que facilitan la realización de las actividades profesionales de un forense informático, los cuales han sido probados en casos de estudios específicos, con lo que se concluye que se cuenta con tecnología suficiente y avanzada en este campo, al menos bajo necesidades específicas regulares.

Actualmente, con el desarrollo tecnológico que se vive, casi no hay delito donde los dispositivos digitales, las tecnologías de comunicación y las computadoras no están involucradas de manera directa o indirecta, lo que hace tan necesaria la actividad profesional del forense informático, es así que se visualizó en los artículos científicos que los autores proponen desarrollos propios para realizar esta actividad.

Luego de haber pasado por revisiones en las que predomina la actitud subjetiva, experiencia, conocimiento e intuición de los investigadores, se muestran los software forenses recomendados y analizados, tales como: "EnCase Enterprise v4", "FTK imager 3.1.1", "DFF – Digital Forensic Framework", "Open Cloud Forensics (OCF)", "Vizster", "Prefuse", además del uso del archivo de formato "OOXML".

En los artículos evaluados, la investigación forense fue dirigida a computadoras, redes, dispositivos móviles y a la información en la nube. Siendo el análisis a la nube la más delicada y compleja, debido a que muchas de las aplicaciones forenses digitales tradicionales, como el acceso físico a la evidencia, no son válidas en la nube, particularmente en nubes públicas, privadas virtuales y de la comunidad. La recopilación y organización de pruebas depende en gran medida de proveedores de servicios en la nube que son los que suministran los datos forenses o sea la evidencia.

Se aplica mucho las diligencias del forense informático en las áreas comerciales y legales; varias de las soluciones propuestas van dirigidas al área de la informática en general, ya que se encontró en los artículos nuevas soluciones informáticas y modelos de confiabilidad de evidencia, para adaptarse a la evolución de la tecnología y a la falta de procedimientos y pautas para analizar los datos y la evidencia en general; ya que no se encontró la aplicación de dos o más modelos para análisis de la información iguales en los artículos revisados. Además, en varios artículos los autores señalan que encuentran como limitante la aplicación de la ley, ya que en todos no se cumplen los mismos estándares; por ejemplo al pedir una orden judicial para recolección de evidencia digital.

Se espera que este artículo contribuya al conocimiento del tema y sirva de guía para profundizar en más investigaciones de este tipo. Como trabajo futuro se buscará conocer en detalle las herramientas tecnológicas para análisis de información en la nube ya que se torna complejo el análisis al estar en cientos de servidores físicamente dispersos. Un campo que no ha sido cubierto en la literatura, es el

perfil laboral o profesional que debe tener el forense informático, por lo cual existe la oportunidad de desarrollar adicionalmente una revisión sistemática en publicaciones relacionadas a este tema.

Referencias bibliográficas:

Bem, D., Feld, F., Huebner, E., & Bem, O. (2008). Computer Forensics - Past, Present and Future. *Journal of Information Science and Technology*, *4*(2), 1–18. Recuperado de http://www.cis.gsu.edu/rbaskerville/cis8630/Bernetal2008.pdf

Bubulan, C. (2015). Digital Forensics Capabilities in an Open Source Framework. *Journal of Mobile, Embedded and Distributed Systems, 1*(2), 60–65.

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy, 15(6), 12–17. doi: 10.1109/MSP.2017.4251117

Chen, L., Li, W., & Haddad, R. (2017). Special Issue on Mobile Systems, Mobile Networks, and Mobile Cloud. *Security, Privacy, and Digital Forensics. Information*, *8*(3), 1–4. doi: 10.3390/info8030099

Cisar, P., Cisar, M., & Bosnjak, S. (2014). Cybercrime and Digital Forensics – Technologies and Approaches. En B. Katalinic (Ed.), Daaam International Scientific Book (1a ed., Vol. 13, pp. 525–542). doi: 10.2507/daaam.scibook.2014.42

Culley, A. (2003). Computer forensics: past, present and future. *Information Security Technical 13*(3), 32–36. doi: 10.1016/S1363-4127(03)00204-8

Fu, Z., Sun, X., & Xi, J. (2015). Digital forensics of Microsoft Office 2007–2013 documents to prevent covert communication. *Journal of Communications and Networks*, *17*(5), 525–533. doi: 10.1109/JCN.2015.000091

Govan, M. (2014). The Application of Peer Teaching in Digital Forensics Education. *Innovation in Teaching and Learning in Information and Computer Sciences*, *1*(1), 1–7. doi: 10.11120/ital.2014.00012

Grigaliunas, S., Toldinas, J., & Venckauskas, A. (2017). An Ontology-Based Transformation Model for the Digital Forensics Domain. *Elektronika Ir Elektrotechnika*, *23*(3), 78–83. doi: 10.5755/j01.eie.23.3.18337

Irons, A., y Thomas, P. (2016). Problem based learning in digital forensics. *Higher Education Pedagogies, 1*(1), 95–105. doi: 10.1080/23752696.2015.1134200

Johnson, J., Daily, J., & Kongs, A. (2014). On the Digital Forensics of Heavy Truck Electronic Control Modules. *SAE International Journal of Commercial Vehicles*, *7*(1), 72–88. doi: 10.4271/2014-01-0495

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Joint Technical Report, 15*(2), 1–33. Recuperado de http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Li, C.-T., & Lin, X. (2017). A fast source-oriented image clustering method for digital forensics. *Eurasip Journal on Image and Video Processing*, *20*(1), 1–16. doi: 10.1186/s13640-017-0217-

Mazurczyk, W., Caviglione, L., & Wendzel, S. (2017). Recent Advancements in Digital Forensics. *IEEE Security & Privacy*, *15*(6), 10–11. doi: 10.1109/MSP.2017.4251106

Merve, O., İbrahim, K., & Hüseyin, Ç. (2016). General Evaluation and Requirement of Computer Forensics Education. *Bilişim Teknolojileri Dergisi, Cilt, 9*(2), 137–146. doi: 10.17671/btd.31631

Miranda Lopez, E., Moon, S., & Park, J. (2016). Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry, 8*(10), 1–20. doi: 10.3390/sym8100107

Rajesh, K. V. N., & Ramesh, K. V. N. (2016). Computer Forensics: An Overview. *I-Manager's Journal on Software Engineering, 10*(4), 1–6. doi: 10.26634/jse.10.4.6056

Sahinoglu, M., Stockton, S., Barclay, R., & Morton, S. (2016). Metrics-Based Risk Assessment and Management of Digital Forensics. *Defense Acquisition Research Journal, 23*(2), 152–177. doi: 10.22594/dau.16-748.23.02

Seo, J., Lee, S., & Shon, T. (2015). A study on memory dump analysis based on digital forensic tools. *Peer-to-Peer Networking and Applications*, *8*(4), 694–703. doi: 10.1007/s12083-013-0217-3

Sridhar, N., Bhaskari, Dr. D. L., & Avadhani, Dr. P. S. (2011). Plethora of Cyber Forensics. *International Journal of Advanced Computer Science and Applications, 2*(11), 110–114. doi: 10.14569/IJACSA.2011.021118

Stanivukovic, D., & Randjelovic, D. (2016). Application of multiple criteria decision making in the selection of digital forensics software. *Military Technical Courier, 64*(4), 1083–1101. doi: 10.5937/vojtehg64-8938

Subbaraman, N. (2014). Museums go high-tech with digital forensics. *Communications of the ACM, 57*(10), 19–21. doi: 10.1145/2659762

Syambas, N. R., & El Farisi, N. (2014). Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics. *Journal of ICT Research and Applications, 8*(2), 141–156. doi: 10.5614/itbj.ict.res.appl.2014.8.2.5

Varol, A. (2017). Review of Evidence Collection and Protection Phases in Digital Forensics Process. *International Journal Of Information Security Science, 6*(6), 39–47. Recuperado de https://www.ijiss.org/ijiss/index.php/ijiss/article/view/267/pdf_49

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research, 17*(2), 183–194. doi: 10.1080/15614263.2015.1128163

Yasin, M., Qureshi, J. A., Kausar, F., Kim, J., & Seo, J. (2015). A granular approach for user-centric network analysis to identify digital evidence. *Peer-to-Peer Networking and Applications*, *8*(5), 911–924. doi: 10.1007/s12083-014-0250-x

Zawoad, S., & Hasan, R. (2016). Trustworthy Digital Forensics in the Cloud. *Computer, 49*(3), 78–81. doi: 10.1109/MC.2016.89

Contribución del autor:

Autor	Contribución
Marco Espinoza Mina	Concepción y diseño, redacción del artículo y revisión del documento.