GUÍA METODOLÓGICA SOBRE LAS TÉCNICAS Y HERRAMIENTAS DE SOFTWARE LIBRE, APLICADAS A LA INFORMÁTICA FORENSE

Gerardo Díaz Jurado[1]
Jaime Usme Acuña[2]

Resumen:

El trabajo de investigación tiene por objeto la creación de una guía metodológica sobre las técnicas y herramientas de software libre, aplicadas informática forense como una respuesta a la necesidad de aportar nuevo material de conocimiento de carácter académico e investigativo a esta ciencia.

Palabras clave:

Informática forense, evidencia digital software libre, seguridad informática, guía metodológica, delito informático, incidente.

Abstract:

The research aims at the creation of a methodological guide on the techniques and free software tools, applied computer forensics as a response to the need to provide new material for an academic knowledge of this science and research

Key Words:

computer forensics, free software, computer security, Methodological guide, cybercrime, incident, digital evidence.

---

[1] Gerardo Díaz Jurado: Ingeniero de sistemas, candidato a magister en software libre. Convenio Universidad Autónoma de Bucaramanga (UNAB) y la Universidad Oberta de Catalunya (UOC).e-mail: g-d12@hotmail.com.

[2] Jaime Usme Acuña: Ingeniero de sistemas, especialista en teleinformática, candidato a magíster en Software Libre, Convenio Universidad Autónoma de Bucaramanga (UNAB) y la Universidad Oberta de Catalunya (UOC). E-mail: jaimeusme.a@gmail.com

INTRODUCCIÓN

La informática forense, es una ciencia que se desprende de la rama de la seguridad informática, con el fin de esclarecer todos los hechos alrededor de un crimen informático. Sin embargo solo algunos países desarrollados, han proliferado el uso de la informática forense como una ciencia, para ello invierten en investigación, herramientas y preparación de personal idóneo en el tema.

En el contexto hispanoamericano se presenta una ausencia de conocimientos en el tema de la informática forense, lo que se refleja en:

- Déficit de material académico e investigativo, elaborado en idioma español
- La no inclusión de esta ciencia en el pensum académico de las universidades.
- Poca difusión de este tema en la Internet, en especial en idioma español.
- Deficiencia en tecnología especializada en el manejo de la informática forense.
- Falta de conocimiento en las entidades y organizaciones en los procedimientos a seguir para la aplicación de la informática forense, en un caso delictivo.
- Alto índice de impunidad en los casos de delitos Informáticos.

Cada una de estas variables detectadas, son abordadas directamente en la investigación, dando como resultado la necesidad de aportar un material de carácter académico e investigativo, mediante la elaboración de una guía metodológica sobre las técnicas y herramientas en software libre, aplicadas a la informática forense.

A partir del desarrollo de esta guía, se intenta dar solución a cada una de las variables que componen la formulación del problema, mediante la consecución de los siguientes objetivos.

Elaboración de un documento escrito de carácter académico e investigativo, compuesto por la siguiente temática:

- Fases en el proceso de investigación en la informática forense

- Metodologías y estrategias en la recolección y tratamiento de la evidencia digital
- El uso de las mejores herramientas en Software Libre para el proceso de detección e investigación
- Cómo enfrentar un ataque o problema de intrusión
- La elaboración del informe pericial.

Planteamientos de nuevos métodos de detección y seguimiento a cada una de las evidencias y rastros digitales, encontrados en una investigación forense de sistemas informáticos. Este planteamiento está plasmado en uno de los capítulos de la guía metodológica.

Difusión del material académico, mediante la publicación en un blog en la dirección http://software-libre-if.blogspot.com/, con el uso de las herramientas en Software libre aplicadas a la informática forense, como la mejor alternativa eficaz, robusta y confiable.

De igual manera también será difundido parte del material académico de la guía de referencia, en la comunidad web dragonjar(dirección web *http:/*www.dragonjar.org*/)*, como un aporte científico a la investigación en las ciencias de la informática forense.

1. MARCO TEÓRICO Y ESTADO DEL ARTE

1.1. Informática forense

La informática forense es el conjunto multidisciplinario de técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, para acceder a la reconstrucción y recolección de evidencias que permitan esclarecer un hecho delictivo.

El proceso de investigación en la informática forense, permite determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un hecho delictivo a nivel informático.

Esta rama de las ciencias forenses, se ha caracterizado por la rigurosidad en sus procedimientos de investigación, exigiendo que quienes llevan a cabo todo el proceso investigativo, sean personas ampliamente capacitadas.

En este sentido, la informática forense, demanda un alto grado de preparación, técnica y científica para llevar a cabo una investigación acorde al contexto presentado.

1.2. Objetivos de la informática forense

La informática forense persigue 3 objetivos:

- Lograr esclarecer los hechos y actores delictivos para que la ley someta al responsable a compensar los daños causados por el crimen o intrusión
- Apoyo y peritaje a la investigación del crimen.
- Creación y aplicación de medidas correctivas para prevenir casos similares

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

1.3. Evidencia digital

La informática forense busca desarrollar un estudio total de todo tipo de evidencia digital que se encuentre involucrada en un incidente, debiendo realizar la recopilación, preservación, análisis y reportes de la evidencia, con el propósito de hacer que esta evidencia cobre valor legal, y que así mismo, sea admisible a la hora de entablar procesos judiciales en los cuales la evidencia tenga carácter determinante en el mismo.

Para llevar a cabo este proceso y desarrollarlo de forma confiable, a la hora de hacerlo legalmente válido, es necesario considerar la evidencia digital de dos formas. La primera de ellas consiste en ver la evidencia digital como una prueba ordinaria en un caso ordinario, en el sentido que esta dado su contenido, generalmente ayuda a identificar involucrados en un incidente delictivo y sus responsabilidades en él. La segunda forma de consideración, va más allá y considera la evidencia digital, como una forma de evidencia no latente requiriendo ser tratada dentro de un marco legal válido, dado por estándares, para realizar su recolección y preservación.

1.4. Delitos informáticos

Crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de

Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

1.5. Tipos delitos informáticos

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es imaginable, entre ellos los más importantes se señala los siguientes:

- Fraudes
- Sabotaje informático
- Espionaje informático uso de software ilegal
- El robo de servicios
- El acceso no autorizado a servicios informáticos

1.6. Fases en la investigación forense en sistemas informáticos.

Para llevar a cabo una investigación forense es necesario documentarse sobre ciertos aspectos como normas legales existentes para la obtención de las pruebas o resultados, tener conocimiento sobre las condiciones bajo las cuales, la evidencia será considerada como Admisible, Autentica, Completa, Confiable, Creíble; Conocer el procedimiento para llevar a cabo una investigación, cuándo debe llevarse a cabo y las cuestiones legales a tener en cuenta, dependiendo del país donde se lleve a cabo.

Las fases que aplica toda investigación forense a sistemas informáticos son cuatro (4):

- Identificación
- Adquisición
- Análisis de datos
- Preparación del informe

Es importante tener claro que en cada una de las estas cuatro fases de investigación, se dan una serie de procedimientos, que deben ser aplicados dependiendo del caso.

1.7 Antecedentes de la Investigación

La idea de investigación surge, de la necesidad de contribuir a la construcción de conocimientos en la ciencia de la informática forense, mediante la elaboración de una guía metodológica con un compendio sobre las técnicas y herramientas en software libre aplicadas a la informática forense.

Son muy escasas las fuentes documentadas e investigaciones en el idioma español, que existen actualmente en el tema de la informática forense. En la actualidad se conocen algunas publicaciones realizadas

por el Dr Jeimy Cano, uno de uno de los tres(3) expertos e investigadores en la ciencia de la informática forense a nivel Latinoamericano.

1.8 Aspectos Metodológicos

Esta investigación es de tipo exploratoria, y utiliza como fuentes primarias instrumentos como:

Entrevista: Aplicadas a personal investigativo de la policía Nacional de Colombia, Personal experto de la comunidad investigativa dragonjar.

Encuestas: Las encuestas fueron aplicadas a treinta(30) estudiantes de las facultades de ingenierías, de universidades con presencia en la región.

Los instrumentos utilizados como fuentes secundarias son:

Consultas: Como principal herramienta de consulta se utilizó la Internet, para acceder a diversas comunidades académicas e investigativas en la ciencia de la informática forense.

Documentación: Como referencia para la elaboración de la guía metodológica, se utilizó una guía elaborada en idioma ingles denominada "First Responder Guide to Computer Forense".

3. DESARROLLO DE LA GUÍA METODOLÓGICA SOBRE LAS TÉCNICAS Y HERRAMIENTAS APLICADAS A LA INFORMÁTICA FORENSE

La inclusión de los temas desarrollados en la elaboración de la guía metodológica, son una respuesta al dictamen obtenido en los resultados de la investigación.

El contenido de la guía metodología contiene información relevante que guía de manera metódica la ejecución de procedimientos de informática forense, ejecutados bajo plataformas libres

La guía metodológica está compuesta por Cinco capítulos que se resumen a continuación:

Capitulo I. Fases De La Investigación En La Informática Forense:

En este capítulo se relacionan cada uno de los procesos que hacen parte de las cuatro (4) fases de investigación: Investigación preliminar, recolección de evidencia, análisis de la evidencia y elaboración del informe final.

Capitulo II La Evidencia Digital:

Capitulo que trata todos los temas relacionados con el proceso de adquisición y tratamiento de la evidencia digital, según los principios de las buenas prácticas sugeridas por las guías ACPO[3] y la guía IOCE[4].

Capitulo III Aspectos técnicos de la Informática Forense:

La simplicidad del lenguaje utilizado en este capítulo y la descripción de cada proceso técnico inmerso en una investigación forense a sistemas informáticos, permiten identificar cómo funcionan los dispositivos, sistemas operativos, herramientas de software y otros elementos que hacen parte de la investigación.

Capitulo IV Herramienta de investigación Forense:

Para elaborar este capítulo fue necesario clasificar las herramientas de la siguiente manera:
A nivel de software: Herramientas para la recolección de evidencia, Herramientas para el análisis de evidencias.
A nivel de Sistemas operativos: Distribuciones forenses Unix/Linux, como Linux Caine, Deft, Helix, Backtrack.
A nivel de Hardware: Kit de herramientas forenses: Destornilladores, pinzas, discos duros, computadores, adaptadores, etc.

Capítulo V Elaboración del Informe Final:

Aquí se evidencia la metodología para elaborar un informe final del proceso de investigación, teniendo en cuenta los dos tipos de informes sugeridos:

Informe Técnico: Elaborado con un lenguaje, características y especificaciones de profundidad y grado de comprensión elevada.

Informe Ejecutivo: Elaborado con especificaciones aptas para ser comprendidas por personal no experto en aspectos técnicos.

Finalmente como proceso de investigación se evalúa la efectividad y operatividad de la guía propuesta, a través de la aplicación de la metodología expuesta a un caso práctico de investigación a un reporte de intrusión a un sistema.

4. ALCANCES DE LA PROPUESTA

[3] La **ACPO**. Association of Chief Police Officers (Asociación de Jefes de Policía).

[4] IOCE: International Organization of Computer Evidence.

El resultado de la investigación, nos ha permitido desarrollar una guía metodológica, que va a permitir a cualquier persona documentarse y conocer sobre la metodología y los procesos que se deben seguir en un caso de investigación forense a sistemas informáticos, así como el uso de las mejores herramientas disponibles en software libre.

El material académico e investigativo estará dispuesto para su consulta en la comunidad web dragonjar[5](http://www.dragonjar.org/), la cual se especializa en el tema de la seguridad informática y donde participan investigadores, estudiantes, novatos y expertos en el tema.

De igual manera con el fin de difundir y promover el uso del software libre como la mejor alternativa robusta y confiable aplicada a la informática forense, se ha dispuesto de la publicación de un blog, en la dirección web: http://software-libre-if.blogspot.com/.

Figura x publicación del blog, software libre la mejor alternativa para la informática forense.

5. Conclusiones

A través del trabajo de investigación, se llegó a la producción de un material académico e investigativo en idioma español, con un compilado de las diversas metodologías, técnicas y herramientas aplicadas a la informática forense.

Este material fue elaborado mediante consultas a diversas fuentes, autores, profundización y complejidad del tema de la Informática Forense, dando como resultado el desarrollo de una guía metodológica, con temas que ilustran y explican de una manera simple y concisa aspectos fundamentales como:

- Fases en el proceso de investigación en la informática forense

[5] Dragonjar: Comunidad de investigadores, estudiantes, profesionales y entusiastas de la Seguridad Informática

- Metodologías y estrategias en la recolección y tratamiento de la evidencia digital

- El uso de las mejores herramientas en Software Libre para el proceso de detección e investigación

- Cómo enfrentar un ataque o problema de intrusión

- La elaboración del informe pericial.

Como parte del proceso de investigación, se realizó y documento paso a paso la aplicación de la guía metodológica a un caso práctico de un problema de intrusión a un sistema de una empresa. Esto con el fin de evaluar su efectividad y operatividad en los procesos de investigación de la Informática.

Los resultados obtenidos fueron satisfactorios, ya que se llegaron a conclusiones importantes como:

- El ambiente procedimental de la informática forense estandariza su actuar en cuatro fases(Investigación preliminar, recolección evidencia, análisis, informe final) cada una de las cuales guía su pertinencia al existo de una investigación forense a sistemas informáticos

- La metodología, los procesos y las herramientas utilizadas son inherentes a cada caso de investigación.

- El software libre es la mejor alternativa, como herramienta para el análisis forense, gracias a su operatividad, funcionalidad, simplicidad en su manejo y reducción de costos por licencias de uso.

BIBLIOGRAFÍA

- Avances en criptografía y seguridad de la información, Benjamín Ramos Álvarez, Primera Edición.

- B Carrier y E Spafford. “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.
- B Carrier, “The Sleuthkit & Autopsy”. http://www.sleuthkit.org/. Última consulta: Febrero de 2008. Knoppix en español. KNOPPIX (2008). http://www.knoppix-es.org/. Última consulta: Febrero de 2008.

- Diccionario de internet, Primera Edición, Editorial Complutense

- Dirección y gestión de los sistemas de información, Carmen de Pablo Herederos, Segunda Edición

- Fundamentos de tecnología documental, Carlos Manuel Da Costa Carballo, Primera Edición.

- Incident Response", Special Publication 800-86, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD August 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. Ultimo consulta: Febrero de 2008.

- http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7AFB6C- 325D-BF515A44FDEE7459.pdf. Última consulta: Febrero de 2008. Kent, S Chevalier, T Grance and H Dang. " Guide to Integrating Forensics into.

- http://www.criptored.upm.es/guiateoria/gt_m335a.htm. Última consulta: Febrero de 2008. EnCase Forensic. Guideance Software (2007). http://www.guidancesoftware.com/p roducts/ef_index.asp. Última consulta: Febrero de 2008.

- http://www.criptored.upm.es/guiateoria/gt_m180b.htm

- http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

- http://www.isecauditors.com/downloads/present/hm2k4.pdf

- http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/JeimyCano_VIJNSI.pdf
- http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

- M López. "Análisis Forense Digital". Universidad Nacional de Educación a Distancia. Junio de 2006. España.

- Peritajes informáticos, Emilio del Peso Navarro, Segunda Edición, Madrid España.
- The Forensic Toolkit. Foundstone Network Security (2007). http://www.found stone.com/us/resources/proddesc/forensictoolkit.htm. Última consulta: Febrero de 2008. B Carrier, "The Sleuthkit & Autopsy". http://www.sleuthkit.org/. Última consulta: Febrero de 2008. Knoppix en español. KNOPPIX (2008). http://www.knoppix-es.org/. Última consulta: Febrero de 2008.

- Seguridad de la información, Javier Areitio, Primera Edición, Editorial Clara María de la Fuente Roja

- Seguridad informática, Purificación Aguilera, Primera Edición, Editorial Editex