Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales

Iván Mesias Hidalgo Cajo,
Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes, Docente Escuela Superior Politécnica de Chimborazo
Estudiante PhD. Universitat Rovira i Virgili.
Saul Yasaca Pucuna,
Magister en Informática Educativa
Técnico Docente Escuela Superior Politécnica de Chimborazo.
Byron Geovanny Hidalgo Cajo,
Máster Universitario en Ingeniería Computacional y Matemática
Docente Universidad Nacional de Chimborazo
Docente Escuela Superior Politécnica de Chimborazo.
Víctor Manuel Oquendo Coronado,
Ingeniero en Sistemas Informáticos
Docente Instituto Tecnológico Superior Riobamba.
Fanny Valeria Salazar Orozco,
Ingeniera en Contabilidad y Auditoría CPA.

Doi: 10.19044/esj.2018.v14n18p40 URL:http://dx.doi.org/10.19044/esj.2018.v14n18p40

Abstract

The aim of this research is to compare the different standards and methodologies of computer forensic analysis used in the examination of data in digital media. The research was developed based on the scientific method, and a standard and two analysis methodologies were specifically used, which were applied to ten researchers. The analysis variables were based on the feasibility of use and on the time of extracting information from the computer. Among the comparison results of the different methodologies analyzed, it was determined that for the Methodology UNE 71506: 2013, 60% of the researchers used it due to the feasibility of use because it is made up of a robust process (contains the most detailed steps of computer forensics). Reliable and applicable in any field necessarily supervised by specialists working in the area, compared to the National Institute of Standards and Technology that selected 30%, Integrated Digital Investigation Process 10%. Regarding the time of analysis in the examination of digital media with different

methodologies (Case study: Extraction of a file of 100 Mb, of a hard disk of 20 Gb in off mode. It is revealed that in the UNE 71506: 2013 it took less than 1 hour compared to the National Institute of Standards and Technology, which took between 1 and less than 2 hours, the Integrated Digital Investigation Process, which lasted longer than 3 hours. In addition, with the use of the Methodology UNE 71506: 2013, it was possible to have greater feasibility in the examination of digital media, since it is composed of four stages such as the preservation, acquisition, analysis and presentation of information results.

Keywords: Forensic analysis, methodologies, data, digital media

Resumen

El objetivo de la investigación es comparar las diferentes normas y metodologías de análisis forense informático utilizadas en la examinación de datos en medios digitales. La investigación se desarrolló basándose en el método científico, y se utilizó específicamente una norma y dos metodologías de análisis forense informático aplicado a diez investigadores. Las variables de análisis se basaron en la factibilidad de uso y en el tiempo de extracción de información del computador. Entre los resultados de comparación de las diferentes metodologías analizadas se determinó que para la Metodología UNE 71506:2013 decidieron utilizar 60% de investigadores por la factibilidad de uso debido a que está conformado por un proceso robusto (contiene la mayoría de etapas detalladas de análisis forense informático), fiable y aplicable en cualquier ámbito supervisados necesariamente por especialistas que trabajen en el área, frente al National Institute of Standards and Technology que seleccionaron el 30%, Integrated Digital Investigation Process el 10%. En cuanto al tiempo de análisis en la examinación de medios digitales con diferentes metodologías (Caso práctico: Extracción de un fichero de 100 Mb, de un disco duro de 20 Gb en modo apagado), se revela que en la Metodología UNE 71506:2013 se tomaron un tiempo menor de 1 hora frente a National Institute of Standards and Technology que tomó el tiempo entre 1 y menor a 2 horas, Integrated Digital Investigation Process que fue un tiempo mayor de 3 horas.Además, con la utilización de la Metodología UNE 71506:2013, se logró tener mayor factibilidad, en la examinación de los medios digitales, ya que está compuesta de cuatro etapas como es la preservación, adquisición, análisis y presentación de resultados de la información.

Palabras Clave: Análisis Forense, metodologías, datos, medios digitales.

Introducción

El análisis forense informático, en un sentido formal, es definido como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial (López-Delgado, 2007).

El análisis forense se puede realizar simplemente a nivel institucional o llegar al ámbito de la justicia civil o penal. A nivel mundial la legislación se está adecuando a los nuevos tiempos que vive el mundo (ITU, 2018), donde la mayoría de los delitos que existían en el mundo no digital se transladan al mundo virtual. Es importante destacar que en muchos países el fraude electrónico se encuentra en el podio de los delitos más efectivos (LexisNexis, 2014), considerándose muchas veces tan rentable como el narcotráfico

Existe varias metodologías disponibles para Informática Forense que incluye la Integrated Digital Investigation Process (Carrier and Spafford, 2003, Baryamureeba and Tushabe, 2004). Del mismo modo, normas para procesos forense es incluir documentos y recomendaciones desde organizaciones tal como la National Institute of Standards and Technology (NIST).

En España, AENOR es la agencia que regula la creación y adopción de normas. Recientemente, AENOR tiene publicado una completa Metodología para el Análisis Forense de las Evidencias Electrónicas (UNE 71506:2013). El estándar define el proceso de análisis forense dentro del ciclo de administración de evidencia digital (CCN_CERT Centro Criptológico Nacional, 2013).

Justificación/Problema

Las diversas metodologías que se utilizan en la Informática Forense pueden ser varias e independientes del sistema operacional donde se desarrollan las actividades de los investigadores forenses, además no existen estándares aceptados, aunque algunos proyectos están en desarrollo, como el C4PDF (Código de Prácticas para Digital Forensics), de Roger Carhuatocto, el Open Source Computer Forensics Manual, de Matías Bevilacqua Trabado, y las Training Standards and Knowledge Skills and Abilities de la International Organization on Computer Evidence.

Revisión de la literatura

La informática Forense consiste en la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal en la detección de alguna intrusión (Hidalgo Cajo, 2014).

Las diversas metodologías que se utilizan en la Informática Forense pueden ser varias e independientes del sistema operacional donde se

desarrollan las actividades de los investigadores forenses en informática se debe cumplir los siguientes requisitos con la información o evidencia identificada (Umaña Ramírez & Mosquera Navarrete, 2014).

- Para las copias de la información se debe utilizar medios forenses estériles.
- Mantener la integridad del medio original.
- Etiquetar, controlar y transmitir adecuadamente las copias de los datos, impresiones y resultado de la investigación (David C. Smith, 2008).

De esta forma la evidencia no será rebatida y tampoco descartada como medio probatorio.

Entre las principales Metodologías y Normas a nivel mundial de Análisis Forense, podemos describir a continuación:

Integrated Digital Investigation Process.

El proceso Forense Digital es un proceso científico y forense reconocido utilizado en investigaciones forenses digitales. Los investigadores forenses lo definen como una serie de pasos de la alerta incidente original a través de la presentación de informes de los resultados (Casey Eoghan, 2004). El proceso se utiliza principalmente en el ordenador y las investigaciones forenses móviles y consta de tres etapas: adquisición, extracción, análisis y presentación de informes (De León Huerta F. J., 2009).

No existe un procedimiento único para la realización de una investigación. Parece que un procedimiento intuitivo es aplicar las mismas fases básicas que son utilizadas por la policía en la escena del crimen físico, en el que en lugar de tener una escena de crimen digital (Arevalo & Alejandra, 2016). Tenga en cuenta que hay varios detalles que no se mencionará detalladamente.

National Institute of Standards and Technology - (NIST)

Esta metodología es enfocada al análisis forense de evidencia digital, la meta principal del análisis forense es el obtener una mejor comprensión del caso a investigar, encontrando y analizando los hechos relacionados a este caso. El análisis forense puede ser necesario en diferentes situaciones, tales como la recopilación de evidencia para los procedimientos judiciales y medidas disciplinarias internas, ayudando en el manejo de incidentes relacionados con código malicioso (malware) y problemas operativos. Independientemente de las necesidades, el proceso de análisis forense de acuerdo con el NIST debe realizarse en cuatro etapas, los detalles precisos de estas etapas pueden variar con relación al requerimiento del análisis forense, las políticas organizacionales, directivas y procedimientos, indicando así, las variaciones de cada etapa (Gutiérrez & Julián, 2009).

Metodología para el análisis forense de las evidencias electrónicas (Una Norma Europea - UNE 71506:2013)

AENOR ha hecho pública la UNE 71506:2013 Tecnologías de la Información (TI). Es la Metodología para el análisis forense de las evidencias electrónicas, cuyo objeto es establecer una metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas.

La UNE 71506, elaborada por el Comité Técnico de Normalización de AENOR AEN/CTN 71 Tecnologías de la Información, define el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, complementando todos aquellos otros procesos que conforman dicho sistema de gestión de las evidencias electrónicas, según se describe en las partes de la UNE 71505, cuya familia de normas ha sido así mismo publicada. Se pretende que esta norma proporcione respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades, ya que la obtención de evidencias electrónicas fiables y robustas ayuda a atribuir correctamente dichos hechos, pudiendo discernir si su causa tiene como origen un carácter intencional o negligente.

Con dicha información se consigue ubicar de forma acertada los instrumentos, acciones, fines y demás parámetros concernientes a dichas conductas.

La UNE 71506:2013 es de aplicación a cualquier organización con independencia de su voluntad o tamaño, así como también como a cualquier profesional competente en éste ámbito. Se dirige especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas (UNE 71506, 2013).

Propósito

- Comparar las diferentes metodologías y normas de análisis forense informático utilizadas por la ciencia forense digital.

MÉTODO

Tipos de investigación

Investigación documental: Consultas en diversas fuentes de investigación como son: bases de datos digitales, libros, revistas, manuales, internet, entre otros**.**

Método

Científico: Es un estudio sistemático, lógico y organizado de la proposición hipotética planteada para adquirir conocimientos y brindar una solución.

Descriptivo: Se realizó un estudio descriptivo que consiste en llevar a conocer situaciones relevantes a través de la descripción de las variables de investigación para exponer de manera cuidadosa los resultados a fin de extraer generalizaciones significativas.

Instrumentos y materiales

- Formularios Google drive.
- Microsoft Office Excel 2016, Complemento EzAnalyze
- Sistema Operativo (Windows)
- Metodologías y Normas de Análisis Forense Informático
- Computador

Procedimiento

El primer paso fue estructurar una encuesta en base a los métodos, criterios e indicadores para evaluar las diferentes metodologías de Análisis Forense Informático.

Las preguntas de la encuesta fueron planteadas en base a la escala Likert con 5 pesos para su valoración (Tabla 1).

Tabla 1. Pesos para la valoración de factibilidad de uso de las metodologías forenses

Escala	Interpretación	Peso
Totalmente Factible	Aceptación total	5
Parcialmente Factible	Conformidad	4
Factible	Indeciso, Neutro	3
No Factible	Disconformidad	2
Totalmente de factible	Indica un rechazo total	1

Una vez realizada la encuesta, se diseñaron y publicaron en la plataforma Google Drive, para la recogida de datos.

Se procedió a evaluar la encuesta después de haber aplicado las diferentes metodologías y aplicar la encuesta en los analistas forenses, para la tabulación y análisis de los resultados individuales se utilizó el procesador de datos Microsoft Office Excel.

Resultados

Para esta sección se exponen los resultados más relevantes:

- Porcentaje de selección de normas y/o metodologías, debido a responder a la factibilidad de uso, según la preferencia de los investigadores al comparar las diferentes metodologías de Análisis Forense.

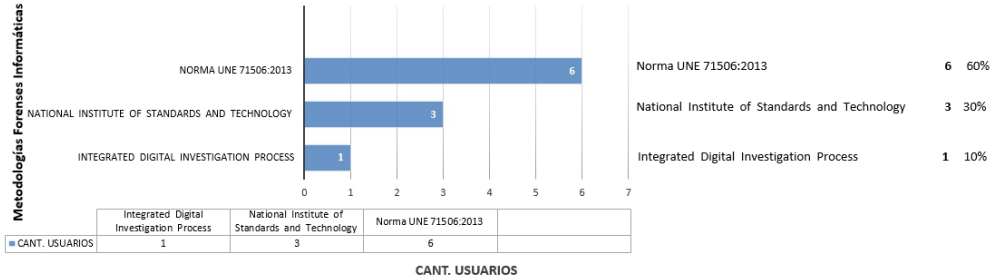

Figura 1. Porcentaje de factilidad de uso Normas y Metodologías de Análisis Forense.

La Figura 1, revela que para la Metodología UNE 71506:2013, utilizan 60%, porque contiene un proceso integrado y sistemático de cuatro etapas (Preservación, Captura/Adquisición, Análisis, Reporte) frente al National Institute of Standards and Technology que ocupa el 30% con un proceso también de cuatro etapas (Recolección, Revisión, Análisis y Reporte), el Integrated Digital Investigation Process alcanza 10% que está constituido por tres etapas (Adquisición, Extracción, Análisis y Presentación de informes).

- Tiempo requerido en la examinación de medios digitales (Caso práctico: Extracción de un fichero de 100 Mb, de un disco duro de 20 Gb en modo apagado).

Tabla 2. Metodologías/Normas Forenses segun el promedio de tiempo requerido para la examinación de medios digitales

METODOLOGÍAS ANÁLISIS FORENSE INFORMÁTICO	TIEMPO (Horas)		
	< 1	[1 - <2]	> 3
The Integrated Digital Investigation Process			x
The National Institute of Standards and Technology		x	
Metodología UNE 71506:2013	x		

La Tabla 2, revela que tiempo requerido por cada una de las metodologías/normas para la examinación de medios digitales (caso práctico: extracción de un fichero de 100 Mb en un disco duro de 20 Gb en modo apagado), para la Metodología UNE 71506:2013 se requiere aproximadamente 1 hora frente a la metodología del National Institute of Standards and Technology el cual emplea entre 1 y menor a 2 horas y el Integrated Digital Investigation Process demanda un tiempo mayor de 3 horas.

Conclusión

- El empleo de una metodología estandarizada proporciona un marco de trabajo sistemático que facilita las tareas de análisis, estudio, y adquisición de los elementos objeto de un peritaje informático.

- Estas metodologías añaden al proceso un alto grado de eficiencia, confiabilidad y seguridad que contribuye a dar una mayor veracidad a los resultados obtenidos en un peritaje informático, logrando de esta manera que el 60% de investigadores se sintieron más confiables con la Norma UNE 71506:2013, el 30% prefirió la metodología National Institute of Standards and Technology (NIST) y sobre la metodología Integrated Digital Investigation Process prefirió el 10%. El cuanto al tiempo requerido para la examinación de medios digitales la Norma UNE 71506:2013 requiere aproximadamente una hora frente a la metodología National Institute of Standards and Technology (NIST) el cual emplea entre 1 y menor a 2 horas y la metodología Integrated Digital Investigation Process demanda un tiempo mayor de 3 horas.
- Una línea de trabajo futura podría consistir en la implementación de una nueva Metodología de Análisis Forense Informático, para aumentar la efectividad y fiabilidad en los procesos de análisis en función del valor potencial de la información obtenida y del coste asociado a su obtención.

References:

1. Arevalo, A., & Alejandra, G. (2016). *DEFINICIÓN DE UNA METODOLOGÍA PRÁCTICA PARA LA ADQUISICIÓN Y ANÁLISIS DE EVIDENCIA DIGITAL EN EL CONTEXTO DE UN ANÁLISIS FORENSE DIGITAL ON LINE (Doctoral dissertation).*
2. Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation*, 121-130.
3. Casey Eoghan. (2004). *Digital Evidence and Computer Crime*. Elsevier ISBN 0-12-163104-4.
4. CCN_CERT Centro Criptológico Nacional. (2013). Ciberamenzas 2012 y Tendencias 2013 y tres guías CCN-STIC. *Seguridad de las Tecnologías de la Información y la Comunicación*.
5. De León Huerta F. J. (2009). *Estudios de metodologías de análisis forense digital.*
6. Gutiérrez, P., & Julián, A. (2009). *Recomendaciones para análisis forense en red.*
7. Hidalgo Cajo, I. (2014). *Análisis preliminar y Diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Forense Informático.* Tarragona.
8. ITU. (2018). *International Telecommunications union (ITU) [CH]*. Obtenido de http://www.itu.int/en/ITUD/Cybersecurity/Pages/Legal-Measures.aspx

9. LexisNexis. (Agosto de 2014). *Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs*. Obtenido de http://www.lexisnexis.com/risk/downloads/
10. López-Delgado, M. (Junio de 2007). *Análisis Forense Digital*. Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
11. Smith, D., & Petreski, S. (2008). A New Approach to Digital Forensic Methodology. *DEF CON*.
12. Umaña Ramírez, G., & Mosquera Navarrete, I. (2014). *Diseño e implementación de un centro de informática forense en la Universidad Autónoma de Occidente.* (Bachelor's thesis, Universidad Autónoma de Occidente).
13. UNE 71506. (2013). Tecnología de la Información (TI). *Metodología para el análisis forense de evidencias electrónicas*.