Estudio Comparativo de Buenas Prácticas para la Recolección de la Evidencia Digital

Nicolás Armilla, Jorge Eterovic, Marisa Panizzi, Luis Torres

Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales,
Universidad de Morón.
Cabildo 134 – CP (1708) – Morón – Prov. de Bs. As. Tel: 5627-2000
nicolasarmilla@hotmail.com; jorge_eterovic@yahoo.com.ar; marisapanizzi@outlook.com;
torreslu@ar.ibm.com

Resumen

Este trabajo de investigación consiste en la comparación de un conjunto de buenas prácticas para la recolección de la evidencia digital. En la República Argentina se evidenciaba la ausencia de un manual, un procedimiento o de un código sobre la recolección de la evidencia digital. Esto conllevo a que una gran cantidad de casos quedasen inconclusos y sin resolución, hasta la creación de la Guía de obtención, preservación y tratamiento de evidencia digital de la Procuración General de la Nación Argentina, en Marzo del año 2016.

Se consideraron buenas prácticas de nivel internacional y nacional, entre ellas la Guía de buenas prácticas para evidencia digital de ACPO (Association of Chief Police Officers), la Guía para las mejores prácticas en el examen forense de tecnología digital de ISFS (Information Security and Forensic Society), la Guía para recolectar y archivar evidencia de RFC 3227 e Investigación en la escena del crimen electrónico del Departamento de Justicia de los Estados Unidos de América y la Guía de obtención, preservación y tratamiento de evidencia digital de la Procuración General de la Nación Argentina.

Se realizará una revisión sistemática para la identificación de los aportes y áreas de vacancias de las buenas prácticas consideradas.

Palabras clave: Informática forense, perito informático, evidencia digital, buenas prácticas, procedimientos en la informática forense.

Contexto

Este trabajo de investigación se encuentra radicado en el Instituto de Ingeniería de Software Experimental perteneciente a la Facultad de Informática, Ciencias de la Comunicaciones y Técnicas Especiales de la Universidad de Moron. El Instituto articula con las cátedras de tesis de la carrera Licenciatura en Sistemas y con la catedra de Auditoría y Seguridad de los Sistemas de información.

Introducción

Se han realizado una investigación exploratoria documental respecto a definiciones de informática forense, antecedentes actuales en el ámbito internacional y nacional.

Darahuge et al. definen la Informática Forense como el conjunto muldisciplinario de teorías, técnicas y métodos de análisis, que

brindan soporte conceptual procedimental a la investigación de la prueba indiciaria informática (Darahuge, 2011).

Kovacich define la Informática Forense como la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación (Kovacich, 2000).

Gómez define la Informática Forense como aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. O también lo define como una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnicos (Gómez Luis, 2012).

Listek en el Diario La Nación plantea que el Gobierno quiere normas claras para obtener pruebas digitales en los procesos judiciales (La Nación, 2016).

La Procuración General de la Nación menciona que uno de los temas que puede tocarse desde ahora es el relativo a la evidencia digital, ya que su adecuada obtención, conservación y tratamiento es un elemento clave, entre muchos otros, para asegurar el éxito de las investigaciones (Procuración General de la Nación, 2016).

Luego de revisar los antecedentes en nuestro país, nos planteamos como problema de esta investigación la escasa maduración de procedimientos para la recolección de la evidencia digital en la informática forense en la República Argentina.

- En los últimos años los peritos informáticos se basaron en procedimientos y buenas prácticas de otros países tales como Canadá, Estados Unidos, Reino Unido y Hong Kong. En la actualidad, a partir del año pasado se cuenta con la nueva resolución de la Procuración General de la Nación (Procuración General de la Nación. Argentina, 2016).

Los procedimientos y buenas prácticas más considerados en nuestro análisis se detallan a continuación:

- Guía de buenas prácticas para evidencia digital. (ACPO, 2012).
- Computación Forense - Parte 2: Mejores Prácticas. (ISFS, 2009).
- Guía para recolectar y archivar evidencia - RFC 3227. (RFC, 2002).
- Investigación en la escena del crimen electrónico. (NIJ, 2001).
- Guía de obtención, preservación y tratamiento de evidencia digital. (Procuración General de la Nación. Argentina, 2016).

Se ha detectado que el inconveniente de basarse en procedimientos y buenas prácticas de otros países presenta diferencia de factores tecnológicos, sociales, culturales y legales respecto a los de nuestro país.

En este estadio de la investigación, se ha realizado una revisión sistemática de los procedimientos y buenas prácticas tanto a nivel internacional como nacional contemplando un conjunto de dimensiones a considerar en el análisis y como resultado se ha obtenido la Tabla 1. Cuadro Comparativo de buenas prácticas y procedimientos a nivel internacional y nacional.

Tabla 1 - Cuadro comparativo de buenas prácticas y procedimientos a nivel internacional y nacional.

	Buenas prácticas y procedimientos a nivel internacional y nacional				
	Internacional				**Nacional**
	Guía de buenas prácticas para la evidencia digital (ACPO, 2012)	**Computación Forense - Parte 2: Mejores Prácticas (ISFS, 2009)**	**Guía para recolectar y archivar evidencia – RFC3227 (RFC, 2002)**	**Investigación en la escena del crimen electrónico (NIJ, 2001)**	**Guía de obtención, preservación y tratamiento de evidencia digital (Procuración General de la Nación, 2016)**
Evaluación de Escena		■		■	■
Herramientas y equipamientos		■	■	■	■
Dispositivos electrónicos				■	■
Recolección	■	■	■	■	■
Almacenamiento y transporte	■	■	■	■	■
Análisis	■				■
Reporte	■	■			

Líneas de Investigación, Desarrollo e Innovación

En el marco de la investigación, según la investigación exploratoria y documental realizada sobre buenas prácticas para la recolección de la evidencia digital en Argentina, se evidencia poca maduración y pruebas realizadas con el novedoso conjunto de buenas prácticas. También se observa que no existen recomendaciones para poder generar un reporte de forma óptima. Se pretende madurar en el conjunto de buenas prácticas para la recolección de la evidencia digital contemplando otras dimensiones en el procedimiento.

Resultados y Objetivos

El objetivo de este trabajo de investigación consiste en la comparación, propuesta de un procedimiento de un conjunto de buenas prácticas para la recolección de evidencia digital en Argentina, contemplando elementos de los existentes y proponiendo nuevos elementos.

En la actualidad, con la revisión de antecedentes se ha logrado la elaboración del instrumento que permitió analizar cada uno de los procedimientos considerados logrando identificar las áreas de vacancia existentes en cada uno de ellos.

Para la validación del procedimiento a construir, se simulará la recepción de un mail con amenazas, luego será analizado y se sacará una conclusión sobre los hechos.

Formación de Recursos Humanos

El equipo de investigación está compuesto por dos docentes-investigadores, un investigador en formación y un estudiante de la carrera Licenciatura en Sistemas de la Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales, Universidad de Morón.

Dicho trabajo de investigación dará como resultado una tesina de grado de la carrera Licenciatura en Sistemas.

Bibliografía

Darahuge Maria Elena – Arellano González Luis Enrique, Manual de informática forense 1, Buenos Aires, 2011.

Darahuge Maria Elena – Arellano González Luis Enrique, Manual de informática forense 2, Buenos Aires, 2012.

Kovacich Gerald, High-Technology Crime Investigator's Handbook: Working in the Global Information Environment, United States of America, 2000.

Gómez Luis A., La informática forense: una herramienta para combatir la ciberdelincuencia, Buenos Aires, 2012. http://www.minseg.gob.ar/node/1050

Listek Vanesa, El gobierno quiere normas claras para obtener pruebas digitales en los procesos judiciales, Diario La Nacion - Argentina, viernes 19 de agosto de 2016. http://www.lanacion.com.ar/1929918-EL-GOBIERNO-QUIERE-NORMAS-CLARAS-PARA-OBTENER-PRUEBAS-DIGITALES-EN-LOS-PROCESOS-JUDICIALES

Procuración General de la Nación, Guía de obtención, preservación y tratamiento de evidencia digital, publicada en la Resolución PGN-0756-2016-001, 31 de marzo de 2016.

ACPO: Association of Chief Police Officers, Good Practice Guide for Digital Evidence, Reino Unido, 2012.

ISFS: Information Security and Forensic Society, Computación Forense – Parte 2: Mejores Prácticas, Hong Kong, 2009.

RFC: Request for Comments, RFC 3227: Guía para recolectar y archivar evidencia, 2002. http://rfc-es.org/pendientes/rfc3227-es.txt

NIJ: National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders - Second Edition, Washington, 2001. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Piccirilli Dario, La forensia como herramienta en la pericia informática, Buenos Aires, 2013. http://sistemas.unla.edu.ar/sistemas/redisla/ReLAIS/relais-v1-n6-237-240.pdf

Piccirilli Dario. PROTOCOLOS A APLICAR EN LA FORENSIA INFORMÁTICA EN EL MARCO DE LAS NUEVAS TECNOLOGÍAS (PERICIA – FORENSIA y CIBERCRIMEN), La Plata – Prov. Buenos Aires, 2015.

ENFSI: European Network of Forensic Science Iinstitues, GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY, Europa, 2009. https://pdf.yt/d/D2rLh6ku8yFjUbt3

Acurio Del Pino Santiago, Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, Ecuador, 2009. http://www.oas.org/juridico/english/cyb_pan_manual