INFORMÁTICA FORENSE: MÉTODOS, HERRAMIENTAS Y TÉCNICAS

Susana Herrera, Liliana Figueroa, Cecilia Lara, Graciela Viaña, Analía Méndez, Lilia Palomo, Luis Pianazzola

Instituto de Investigación en Informática y Sistemas de Información, Facultad de Ciencias Exactas y Tecnologías, Universidad Nacional de Santiago del Estero
sherrera@unse.edu.ar; lmvfigueroa@yahoo.com.ar; laraceciliacristina@gmail.com; gv857@hotmail.com; anmendez725@yahoo.com; lilia.palomo@gmail.com, luispianezzola@gmail.com

RESUMEN

Resulta relevante destacar los desafíos que genera el avance tecnológico para incorporar la utilización de la evidencia digital al sistema procesal penal, como prueba fundamental en la investigación de cualquier delito. En la provincia de Santiago del Estero y de manera gradual desde el año 2016 se ha implementado el Sistema Penal Acusatorio, siendo entonces necesario disponer de métodos, herramientas y técnicas que permitan una gestión eficiente del ámbito de trabajo en donde se realizan las actividades de informática forense en los distintos organismos e instituciones involucrados en este sistema.

Entonces, es necesario contar con métodos científicos que permitan recolectar, analizar y validar pruebas digitales que sean legalmente aceptables y que ayuden a resolver la investigación penal.

En esta propuesta se pretende llevar a cabo una investigación aplicada para proponer métodos, técnicas y herramientas forenses tendientes a garantizar una gestión eficiente de los laboratorios de informática forense que forman parte de las distintas instituciones del Sistema Penal Acusatorio en la Provincia de Santiago del Estero.

Palabras clave:

Informática forense, evidencias digitales, métodos–técnicas-herramientas forenses, laboratorios de informática forense.

CONTEXTO

En este artículo se presenta una propuesta de investigación que constituye una continuación de los proyectos “Computación Móvil: desarrollo de aplicaciones y análisis forense” y Métodos y Herramientas para el análisis forense”, financiados en 2017-2018 y 2019-2021 por el Consejo de Ciencia y Técnica de la Universidad Nacional de Santiago del Estero [4].

En estos proyectos se lograron, hasta la fecha resultados referidos al: análisis de la obtención legal de la evidencia digital en los códigos procesales de nuestro país, análisis de antecedentes jurisprudenciales sobre tratamiento de evidencia digital en dispositivos móviles, investigación y análisis de protocolos vigentes en otras jurisdicciones, propuesta de protocolo para la obtención de evidencia digital móviles en concordancia con las normas ISO/IEC 27037:2012 en el ámbito del Ministerio Público Fiscal de Santiago del Estero, y estudio de repositorios que permitan la construcción de un modelo de datos para el almacenamiento y la gestión de evidencias digitales extraídas de dispositivos móviles y evaluación sistémica del protocolo de actuación propuesto.

La implementación del sistema procesal penal acusatorio tiene que ver con un cambio de paradigma, reasignando los roles de los actores de la Justicia en el tratamiento de las causas. Con este sistema cambia la forma de llevar a cabo el proceso y recae en los fiscales la tarea de investigar.
En este sistema lo que se busca es ayudar a queg todos los actores de la justicia tengan pleno conocimiento de lo que pasa en el proceso. [1] En particular, en Santiago del Estero rige el código de procedimiento penal Ley Nº 6941 [9], donde la Investigación

Penal Preparatoria (IPP), es la etapa del proceso penal que tiene por objeto determinar la existencia de delitos y la individualización de los eventuales autores.
En este contexto, el modo de vincular un hecho criminoso con su autor, es a través de pruebas. Es sabido que la mayoría de las IPP cuentan con trabajos de investigadores y peritos; pero también es sabido que los cambios que se produjeron en estos últimos años hace necesario encontrar las huellas en el ámbito digital para encontrar las evidencias digitales que ayuden a resolver crímenes.

Atendiendo a esta realidad, los actores del sistema procesal penal acusatorio de la provincia de Santiago del Estero han tomado la iniciativa de implementar áreas específicas relacionadas a la informática forense, con el objetivo de dar respuesta a distintos ilícitos que tengan asociados dispositivos tecnológicos. En este sentido, se puede observar distintos niveles de avance en la gestión, mientras que algunos tienen incorporado en sus funciones un laboratorio de informática forense donde se han definido algunos procesos en relaciones a las tareas periciales, otros en cambio están en un proceso inicial de gestión y solamente brindan apoyo técnico a través de sus oficinas de informática.
En este ámbito se integrarán el personal especializado, la infraestructura física y tecnológica, las herramientas de hardware y software adecuas para el análisis de datos, con el fin de recolectar evidencias que cumplan los principios de admisibilidad y tengan validez en el proceso judicial [3].
Entonces, la creación, operación y organización de laboratorios judiciales dedicados a la realización de pericias informáticas es una temática en donde aún se demandan varios aspectos para lograr una gestión eficiente de los mismos. En este contexto se pueden identificar diferentes problemas tanto administrativos como los que se enfrentan los operadores judiciales y peritos informáticos:

- Algunos procesos vinculados a la obtención de la evidencia digital tienen una fuerte descripción desde una visión técnica, propiciando en algunos casos riesgos legales que garanticen su validez.
- Algunos organismos han ido incorporando estos espacios funcionales a partir de la incorporación de la infraestructura física, tecnológica y de las herramientas de software, sin una definición inicial de procesos que sostengan las actividades y tareas que se desarrollan.
- Se especifican procedimientos sin definir un acto administrativo resolutivo.
- Algunos de los organismos no cuentan con una estructura funcional y una descripción de los distintos puestos de trabajo, responsabilidades, perfiles para ocupar los puestos de trabajos.

- El costo elevado y la disponibilidad presupuestaria limita la adquisición de software especializado para la realización de las tareas de los peritos.
- La sobrecarga de las tareas diarias en relación a las pericias limita a los profesionales de disponer tiempo suficiente para diseñar casos de estudio de situaciones hipotéticas que propicien el uso eficiente de las herramientas en distintas situaciones de la investigación criminal.

- Las experiencias y las capacitaciones que se adquieren durante la realización de las pericias no se documentan para fomentar el autoaprendizaje organizacional.

- En los últimos años se ha incrementado el volumen de pericias sobre dispositivos tecnológicos y se plantean los siguientes inconvenientes:

  ✓ El proceso de obtención y análisis de las evidencias digitales es una tarea compleja que demanda un tiempo que en algunos casos excede los plazos procesales.
  ✓ No hay un software de informática forense que soporte la extracción de datos de todos los dispositivos móviles existentes en el mundo.
  ✓ Los requerimientos para los peritos forenses no están claros y definidos desde el inicio.
  ✓ Tomando como referencia el “Sistema de clasificación de herramientas forenses de

dispositivos móviles" desarrollado por Sam Brothers [2], que presenta cinco niveles sobre la extracción y el análisis requerido en cada dispositivo móvil teniendo en cuenta la solicitud y los detalles de la investigación. A partir de estos problemas, en esta propuesta se pretende investigar sobre estrategias que permitan gestionar de manera eficiente los distintos recursos involucrados en el entorno de los laboratorios de informática forenses, de manera tal que promueva el trabajo eficiente de la labor de los peritos ofreciendo un respaldo jurídico a su tarea.

1. INTRODUCCIÓN

La Informática forense es una rama de las ciencias forenses, que involucra la aplicación de la metodología y la ciencia para identificar, preservar, recuperar, extraer, documentar e interpretar [15] evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos encontrados en la escena del crimen [13], para luego usar dichas evidencias como elemento material probatorio en un proceso judicial [5] [4]; de esta manera constituye una disciplina auxiliar a la justicia, que consiste en la aplicación de técnicas que permiten adquirir, validar, analizar y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. [6]

Por otra parte, el FBI, considera que la Informática forense es la ciencia que se encarga de adquirir, preservar, analizar y presentar los datos que han sido procesados electrónicamente y almacenados en medios electrónicos aplicando técnicas científicas y analíticas, utilizando hardware y software especializado para realizar la tarea. [10]

En este contexto los elementos informáticos que se disponen en los celulares, las computadoras o los dispositivos de almacenamiento como imágenes, mensajes de texto, conversaciones de WhatsApp, videos, ubicación, etc. constituyen las evidencias necesarias para resolver diferentes tipos de casos judiciales. Todos estos elementos son trabajados en los Laboratorios de informática forense, en donde se realizan las extracciones forenses apoyadas con aparatología especializada y programas forenses; luego la información obtenida es procesada y analizada para conseguir la evidencia digital necesaria para las investigaciones. Por otra parte, en estos laboratorios no solo hay que recuperar la información, sino también realizar procedimientos de la forma adecuada para poder utilizar esta información como evidencia; entonces hay que garantizar la confiabilidad de la prueba y la cadena de custodia de la información, cuando se realiza una operatoria de estas características.

Una propuesta de los procedimientos para el establecimiento y gestión de Laboratorios informática forense son las enunciadas por [8], estas directrices proporcionan técnicas para el manejo y procesamiento de pruebas digitales; tienen como objetivo proporcionar un marco universal para establecer y administrar un Laboratorio de informática forense. Además, también se debe tener en cuenta el cumplimiento de principios básicos definidos por [7] para recoger y manipular pruebas digitales, estos principios sirven como marco de referencia y apoyan los procedimientos de actuación que se desarrollen en dichos laboratorios.

Otro aspecto importante que debe plantearse en los Laboratorios de informática forense a la hora de hacer el análisis de las evidencias, es la disponibilidad de herramientas forenses, entre las alternativas existen diferentes soluciones tanto pagas como gratuitas para este fin.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Considerando la amplitud de los aspectos relacionados con la informática forense, en el presente proyecto de investigación se diferencian las siguientes líneas de investigación:

- *Estudio de herramientas de informática forense,*
- *Desarrollo de aplicaciones de apoyo a la gestión de los laboratorios de informática forense.*

- *Técnicas y métodos para la gestión de laboratorios de informática forense.*

3. OBJETIVOS

El objetivo general de la investigación propuesta es:

Contribuir al mejoramiento de la gestión de las evidencias digitales en el ámbito del sistema judicial de Santiago del Estero.

Los objetivos específicos por cada línea de investigación que permitirán alcanzar el objetivo general son:

- *Estudio de herramientas de informática forense.*

a Estudiar comparativamente las arquitecturas de los dispositivos móviles.

b Evaluar herramientas de informática forense correspondientes a los niveles (1, 2 y 3) de la *Pirámide Móvil Forense*.

c Estudiar sistemáticamente herramientas correspondientes a los niveles superiores (4 y 5) de la *Pirámide Móvil Forense*.

- *Desarrollo de aplicaciones de apoyo a la gestión de los Laboratorios de informática forense.*

d Desarrollar una aplicación que de soporte a la formación inicial de peritos informáticos.

e Desarrollar nuevos módulos de la aplicación de gestión de experiencias de los peritos informáticos.

f Desarrollar un repositorio institucional para alojar evidencias digitales, permitiendo la búsqueda, visualización y recuperación de las mismas.

- *Técnicas y métodos para la gestión de laboratorios de informática forense.*

g Proponer modelos de gestión a las instituciones del sistema judicial de Santiago del Estero sobre la definición de normas, procesos y procedimientos.

Se trata de una investigación aplicada, desarrollada desde un enfoque cuanti-cualitativo, en el campo de la Informática Forense.

La investigación es aplicada porque los resultados que se obtengan se aplicarán inmediatamente la oficina de Informática Forense del Gabinete de Ciencias Forenses del Ministerio Público Fiscal, en el Gabinete de Informática Forense del Poder Judicial de la Provincia de Santiago del Estero, en la Policía de la provincia de Santiago del Estero, en la Oficina de Informática del Ministerio Publico de la Defensa.

4. FORMACIÓN DE RECURSOS HUMANOS

En cuanto a los RRHH, se espera consolidar y agrandar el equipo de investigadores de UNSE, iniciado en el año 2017. Se trabajará en forma conjunta y colaborativa con la oficina de Informática Forense del Gabinete de Ciencias Forenses del Ministerio Público Fiscal, con el Gabinete de Informática Forense del Poder Judicial de la Provincia de Santiago del Estero, la Oficina de Informática del Ministerio Publico de la Defensa y en la Policía de la provincia de Santiago del Estero.

La concreción de este proyecto contribuirá a la formación y capacitación de los investigadores, estudiantes de grado involucrados. Incentivará a los alumnos a iniciarse en las actividades de investigación y favorecerá la realización de sus trabajos finales de grado en las líneas de investigación de este proyecto

Los investigadores constituyen un equipo interdisciplinario conformado docentes de la UNSE e investigadores externos, de profesión en Informática, Electromecánica y Derecho.

5. REFERENCIAS

[1] Argentina.gob.ar. (2021, 6 de septiembre). Sistema acusatorio: nuevos roles y mayor eficacia. https://www.argentina.gob.ar/noticias/sistema-acusatorio-nuevos-roles-y-mayor-eficacia

[2] Ayers, R; Brothers, S; Jansen, W. (2014).Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revisión 1. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

[3] Calderón Valdiviezo RG, Guzmán Reyes GS, Salinas González JM, Aranda A. Diseño y Plan de Implementación de un Laboratorio

de Ciencias Forenses Digitales. (2011). file:///C:/Users/hp/Downloads/paper_laboratorio_forense_digital.pdf

[4] Castillo, C., Romero, A., Cano, J.: Análisis Forense Orientado a Incidentes en Teléfonos Celulares GSM: Una Guía Metodológica. Conf. XXXIV Conferencia Latinoamericana de Informática, Centro Latinoamericano de Estudios en Informática (CLEI). (2008). http://www.clei2008.org.ar/

[5] Del Pino, S.: Introducción a la informática forense. Pontificia Universidad Católica del Ecuador. (2007). http://www.alfa-redi.org/sites/default/files/articles/files/Acurio.pdf

[6] Di Iorio, Ana H. -La informática forense y el Proceso de recuperación de Información digital. Revista Democracia Digital e Governo Eletrônico (ISSN 2175-9391), n° 8, p. 326-339 - 2013.

[7] Digital Evidence: standards and principles", Forensic Science Communications, FBI, apr. 2000. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

[8] Directrices Mundial de INTERPOL para los Laboratorios Forenses Digitales. INTERPOL L Complejo Mundial para la Innovación de 2019. htps/Downloads/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory%20(2).pdf

[9] Ley provincial 6.941. Código Procesal Penal de la Provincia de Santiago del Estero (2009).

[10] Noblett M. G., Pollit, M. M. "FBI" FBI, October 2000. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

[11] Orta Martínez, R.: Informática Forense como Medio de Pruebas. https://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml

[12] Poder Judicial de Neuquén: Pericias informáticas sobre telefonía celular. (2013).http://200.70.33.130/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf

[13] Reith, M., Clint, C., Gunsch G.: An Examination of Digital Forensic Models. International Journal of Digital Evidence, Air Force Institute of Technology, Volume 1 Issue 3. (2002). www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.

[14] Unidad Fiscal Especializada en Ciberdelincuencia: Guía de obtención, preservación y tratamiento de evidencia digital. (2016). https://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2016/04/PGN-0756-2016-001.pdf

[15] Zdziarski, J.: iPhone Forensics, Recovering Evidence, Personal Data & Corporate Assets. O"Reilly Media, Inc. (2008)