Tratamiento de Evidencias Digitales Forenses en Dispositivos Móviles

Marta C. Fennema, Liliana M. Figueroa, Graciela Viaña, Norma B. Lesca, Cecilia C. Lara

Instituto de Investigación en Informática y Sistemas de Información, Facultad de Ciencias Exactas y Tecnologías, Universidad Nacional de Santiago del Estero
fennema@unse.edu.ar, lmvfigueroa@yahoo.com.ar; gv857@hotmail.com;
{norma.lesca, laraceciliacristina}@gmail.com

RESUMEN

En este artículo se presenta una propuesta de investigación atendiendo los requerimientos específicos planteados desde el ámbito judicial ante la implementación del Nuevo Sistema Procesal Penal en la Provincia de Santiago del Estero, respecto del proceso de obtención de evidencias digitales.

El proceso de adquisición de evidencias digitales debe ser legalmente aceptable, apoyándose en métodos científicos que permitan recolectar, analizar y validar las mismas, recurriendo entonces a la Informática Forense.

Es en este contexto que se propone el estudio y definición de un protocolo para la gestión de evidencias digitales forenses obtenidas de dispositivos móviles.

Otra cuestión a investigar es el diseño de un repositorio de evidencias digitales extraídas de dispositivos móviles, que permita almacenar, recuperar, distribuir y compartir las evidencias forenses (de manera abierta y segura), definiendo las herramientas de repositorios que son apropiadas para

Palabras clave:

Informática Forense en dispositivos móviles, evidencias digitales, protocolo de extracción de datos, repositorio de evidencias.

CONTEXTO

La presente línea de investigación se encuentra inserta en el proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", que propone una continuación del trabajo en el ámbito de la computación móvil iniciada en el año 2012, financiado por el Consejo de Ciencia y Técnica de la Universidad Nacional de Santiago del Estero [5].

La justicia moderna necesita ampliar la mirada a la hora de obtener evidencias y pruebas digitales, que sean legalmente aceptables y que ayuden a resolver conflictos apoyándose en métodos científicos que permitan recolectar, analizar y validar pruebas digitales.

Es en ese ámbito que se advierte la necesidad de trabajar en el estudio y definición de un protocolo para el análisis de evidencias forenses obtenidas de dispositivos móviles. En respuesta a ello, se propone investigar: protocolos de intervenciones forenses, equipamientos dedicados para la extracción de información y la gestión (acceso, almacenamiento, recuperación, seguridad) de la información obtenida.

1. INTRODUCCIÓN

La Informática Forense es una nueva de directamente de una serie de sucesos que han afectado a la sociedad globalizada e informatizada de fines del siglo XX y principios del XXI, en donde se observa el auge de una serie de delitos que están afectando diferentes áreas de la sociedad [3].

Esta disciplina de las ciencias forenses aplicadas en medios informáticos, considera las tareas propias asociadas con la evidencia, procura descubrir e interpretar la

información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. Así también, es la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos [1].

Está dedicada a la recolección de pruebas digitales para fines judiciales, mediante la aplicación de técnicas de análisis y de investigación. El propósito de esta disciplina es determinar los responsables de los delitos, así como también esclarecer la causa original de un ilícito o evento particular para asegurar que no se vuelva a repetir.

Según [1], la criminalística ofrece un espacio de análisis y estudio sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones criminales, por lo tanto, es necesario establecer un conjunto de herramientas, estrategias y acciones que ayuden a identificar estos hechos y evidencias dentro del contexto informático. Por consiguiente, se hace indispensable la aplicación de procedimientos estrictos y cuidadosos, desde el momento en que se realiza la recolección de la evidencia, hasta que se obtienen los resultados posteriores a la investigación [2,8]. Si bien existe un modelo generalizado para realizar este tipo de investigaciones, cada región necesita adaptarse al Código Procesal Penal y al contexto tecnológico propio.

Para que una evidencia digital pueda ser usada en procesos judiciales, debe cumplir con las siguientes características:

- Admisibilidad: toda evidencia recolectada debe ajustarse a ciertas normas jurídicas para presentarlas ante un tribunal.
- Autenticidad: la evidencia debe ser relevante al caso, y el investigador forense debe estar en capacidad de representar el origen de la misma.
- Completitud: la evidencia debe contar todo en la escena del crimen y no una perspectiva en particular.
- Fiabilidad: las técnicas usadas para obtener la evidencia deben gozar de credibilidad y ser aceptadas en el campo en cuestión, evitando dudas sobre la autenticidad y veracidad de las evidencias.
- Entendimiento y Credibilidad: se debe explicar con claridad y pleno consentimiento, qué proceso se siguió en la investigación y cómo la integridad de la evidencia fue preservada, para que ésta sea comprensible y creíble en el tribunal.

Como en cualquier investigación forense, existen una variedad de enfoques que se pueden utilizar para la recolección y análisis de información. Un aspecto clave para ello es que el procedimiento que se siga, no modifique la fuente de información de ninguna manera, o que de ser esto absolutamente necesario, el analista esté en la capacidad de justificar por qué realizó esta acción [6].

En la actualidad, el empleo de dispositivos móviles se ha incrementado notablemente, principalmente por su facilidad de uso y la propiedad de mantener en contacto permanente a sus usuarios. A partir de esto, se ha generado un cambio significativo en la forma en que las personas se comunican, pero también por su proliferación, se ha incrementado su uso en actividades de orden delictivo.

A diferencia de la Informática Forense clásica, el análisis forense sobre dispositivos móviles, es un campo relativamente nuevo y los procedimientos y normas para su análisis aún se encuentran en desarrollo [11]. Un análisis forense que se lleve a cabo sobre un dispositivo móvil, puede ser admitido o no en un juicio dependiendo de lo que considere el juez y la formalidad con que se desarrolle el procedimiento de recolección, control, análisis y presentación de las evidencias.

En el ámbito de la Informática Forense, en nuestro país, se han desarrollado varios proyectos, entre los cuales se destacan:

- Facultad de Ingeniería de la Universidad FASTA:

a. *Guía Integral de Empleo de la Informática Forense en el Proceso Penal: PAIF-PURI* [4]. *Es una* Guía de Actuación en Informática Forense para ser adoptada y promovida por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo, tanto para peritos como para investigadores judiciales, en base a lo establecido por el Proceso Unificado de Recuperación de Información. El Proceso PURI ha sido desarrollado por el Grupo de Investigación en Informática Forense y Sistemas Operativos, formalizando un proceso general que guía a peritos informáticos en la obtención de información digital que pueda ser considerada como evidencia válida por los operadores de justicia.

b. *Proyecto INVESTIGA* [7]. Ambiente integrado de visualización y análisis de datos, tiene como objetivo el desarrollo de un sistema informático que permita la consolidación de datos provenientes de múltiples fuentes en un ambiente integrado que facilite su visualización y análisis. El sistema informático objetivo de este proyecto pretende reemplazar al software que actualmente utiliza el Ministerio Público con fines similares, ganando en flexibilidad e independencia tecnológica.

c. *Proyecto FOMO* (Forensia en Equipos Móviles) [7]. Tiene como objetivo el desarrollo de un sistema informático que permita realizar la extracción forense de la información contenida en equipos de telefonía móvil. Se pretende, de esta forma, reemplazar al software privativo y extranjero que actualmente utiliza el Ministerio Público con fines similares; desarrollándose un sistema informático propio específicamente orientado a Smartphones Android y Nextel, ganando en flexibilidad e independencia tecnológica.

d. *Proyecto GT-LIF* [7]: Guía Técnica para la Implementación de un laboratorio de Informática Forense Judicial, tiene como objetivo el desarrollo de una Guía Técnica para la implantación de un laboratorio de Informática Forense para ser utilizada por el Ministerio Público de la Provincia de Buenos Aires y en el resto de las provincias, a través del Consejo Federal de Procuradores. Esta guía técnica complementa la "Guía integral de empleo de la Informática Forense en el proceso penal". Se espera que una vez finalizado el proyecto se cuente con una guía que permita estimar y evaluar los aspectos claves de diseño de un laboratorio forense a nivel estratégico, institucional, edilicio, estructural y tecnológico.

- Facultad de Ingeniería en Sistemas, Universidad Abierta Interamericana, Sede Rosario. Se encuentra desarrollando el Proyecto "Análisis Digital Forense, Conceptos y Aplicaciones" [10], que tiene como principal objetivo generar nuevas herramientas y protocolos de análisis digital forense que sean pertinentes de ser utilizados en nuestro país.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Considerando la amplitud de los aspectos relacionados con la computación móvil, la línea de investigación se refiere a:

Informática Forense: protocolo y gestión de evidencias digitales obtenidas de dispositivos móviles.

A partir de ella, se proponen dos líneas de investigación derivadas, consideradas desde el ámbito de la justicia penal de Santiago del Estero:

- Protocolo de actuación para la extracción de evidencias digitales de dispositivos móviles.
- Modelo de datos para la gestión de las evidencias.

3. OBJETIVOS

El objetivo general de la investigación propuesta relacionada a esta línea de investigación es:

- *Contribuir al progreso del campo de la Computación Móvil mediante el análisis forense de dispositivos móviles.*

Los objetivos específicos que permitirán alcanzar el objetivo general son:

- *Definir un protocolo de actuación en la extracción de evidencias digitales de dispositivos móviles en el marco del nuevo Código Procesal Penal de la provincia de Santiago del Estero.*

- *Diseñar un repositorio de evidencias digitales extraídas de dispositivos móviles en el marco del proceso penal mencionado.*

Se plantea una investigación descriptiva-cualitativa, dado que si bien se puede definir una hipótesis que relacione variables, la misma no alcanzará a ser corroborada en el plazo de dos años que dura esta investigación.

La hipótesis planteada es la siguiente:

El uso de un protocolo preestablecido de Informática Forense para móviles y de un repositorio especializado, optimiza la gestión de evidencias digitales extraídas de los dispositivos móviles.

Como puede observarse en la misma, la variable a estudiar es la "optimización de la gestión de evidencias criminales obtenidas de dispositivos móviles", la cual en futuras investigaciones podrá será evaluada a través de indicadores cuantitativos que se pueden aplicar a casos de prueba especialmente diseñados.

Se espera generar nuevo conocimiento científico-tecnológico, plasmado en un protocolo para la recolección y tratamiento de evidencias digitales criminales extraídas de dispositivos móviles, acompañado de un modelo para la gestión óptima de dichas evidencias en el ámbito del Poder Judicial y del Ministerio Público Fiscal de la Provincia de Santiago del Estero, y de acuerdo a lo establecido en el nuevo Código Procesal Penal de la provincia.

Se considera que la obtención del mencionado protocolo traerá un beneficio muy importante para la justicia santiagueña, dado que actualmente no existe un procedimiento claro y definido. Permitiría mejorar la calidad de las evidencias digitales y ayudará en la labor de los fiscales de la provincia.

4. FORMACIÓN DE RECURSOS HUMANOS

La Directora y Codirectora del proyecto pertenecen al Departamento de Informática de la Universidad Nacional de Santiago del Estero. Los asesores pertenecen a LIDI-FI-UNLP y FCE-UNSala. El resto de los integrantes son docentes investigadores de la Universidad Nacional de Santiago del Estero, con distintas categorías de investigación.

5. REFERENCIAS

1. CANO, J. (2006). Introducción a la informática forense: Una disciplina técnico-legal. Revista Sistemas, Asociación Colombiana de Ingenieros de Sistemas (ACIS). Vol.96, pp. 64-73. http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf
2. CASTILLO, C., ROMERO, A., CANO, J. (2008). 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). http://www.clei2008.org.ar.
3. DARAHUGE, M. (2011). Manual de Informática Forense. Buenos Aires. Errepar.
4. DI IORIO, ANA HAYDEE. [et al.] (2015). Guía Integral de Empleo de la Informática Forense en el Proceso Penal. Universidad FASTA. Mar del Plata. Argentina.
5. Herrera, Susana I., Najar Ruiz P., Rocabado S., Fennema, C., Cianferoni, M. (2013). Optimización de

la calidad de los sistemas móviles. http://sedici.unlp.edu.ar/bitstream/handle/10915/27200/Optimizaci%C3%B3n_de_la_calidad_de_los_sistemas_m%C3%B3viles.pdf?sequence=1

6. HOOG, A. (2009). iPhone Forensics: Annual Report on iPhone Forensic Industry. Chicago Electronic Discovery.
7. INFO-LAB. (2016). Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Universidad FASTA, Ministerio Público Fiscal de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon. Buenos Aires. Argentina.
8. LEIGLAND, R. (2004). A Formalization of Digital Forensics. International Journal of Digital Evidence. University of Idaho. Volume 3, Issue 2. http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2- 8F98- 8F7597844CF74DF8.pdf.
9. MEYERS, M., ROGERS, M. (2004). Computer Forensics. The Need for Standardization and Certification. International Journal of Digital Evidence, CERIAS, Purdue University, Volume 3 Issue 2. http://ww.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.
10. PADULA, EUGENIO J.; FOGLIATO, NELSON M.; CASCO, MARIA E. (2016). Análisis Digital Forense, Conceptos y Aplicaciones. Facultad de Ciencias Exactas, Ingeniería. Universidad Nacional de Rosario. Rosario, Santa Fe. Argentina.
11. VARSALONE, J., KUBASIAK, R. (2009). Mac Os X, iPod and iPhone Forensic Analysis DVD Toolkit. Syngress Publishing, Inc, pp. 355-475.