TRATAMIENTO DE EVIDENCIAS DIGITALES FORENSES EN DISPOSITIVOS MÓVILES

Liliana Figueroa, Cecilia Lara, Norma Lesca, Graciela Viaña, Adriana Binda

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

RESUMEN

En este artículo se presenta la investigación que se viene desarrollando en el Instituto de Investigaciones en Informática y Sistemas de Información de la Universidad Nacional de Santiago del Estero (UNSE) sobre obtención de evidencias digitales de dispositivos móviles. Para ello se considera como marco normativo el Nuevo Sistema Procesal Penal de la Provincia de Santiago del Estero

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.

En este contexto, y en el marco de la investigación, se han desarrollado actividades con el propósito de definir un conjunto de lineamientos a los que se puede recurrir al momento de realizar la obtención de evidencias digitales desde dispositivos móviles. Durante esta etapa, se han estudiado las buenas prácticas tendientes a asegurar la calidad de los procesos aplicados y sus resultados.

Palabras clave:

Informática Forense, dispositivos móviles, evidencias digitales, protocolo de extracción de datos, calidad de la evidencia digital.

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 [5]. Está financiada por el Consejo de Ciencia y Técnica de la UNSE. La investigación comenzó en el año 2017 y finalizará en el año 2018, y hasta la fecha se han obtenido resultados parciales en relación a los procesos que permitan garantizar la integridad de las evidencias digitales obtenidas de dispositivos móviles.

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.

En ese ámbito, 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 y la gestión de evidencias digitales empleando repositorios digitales (acceso, almacenamiento, recuperación, seguridad) de las evidencias digitales.

La presente investigación se desarrolla en acuerdo y colaboración con el Gabinete de Ciencias Forenses del Ministerio Público Fiscal de Santiago del Estero, para lo cual se ha firmado un convenio que permite realizar la investigación de manera conjunta.

1. INTRODUCCIÓN

La Informática Forense es disciplina que surge a partir de sucesos que han afectado a

la sociedad globalizada e informatizada actual, en donde se observa el crecimiento una serie de delitos que están afectando diferentes áreas de la sociedad [4].

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. Para ello, se encarga de recolectar pruebas digitales para fines judiciales, mediante la aplicación de técnicas de análisis y de investigación.

Haciendo una analogía con la criminalística [1], es necesario establecer un conjunto de herramientas, estrategias y acciones que ayuden a identificar hechos y evidencias relacionados con la Informática

Es por ello, que es necesario 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 [3,8]. Todo esto en el marco del Código Procesal Penal de cada provincia, ya que deben adaptar un modelo generalizado para realizar este tipo de investigaciones a las necesidades locales.

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].

Para mantener la integridad de la evidencia y de ese modo garantizar su admisibilidad en el proceso penal se requiere de procedimientos que sigan una metodología para tal fin. En este sentido, la norma ISO/IEC 27037:2012 "Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence" [7] puede considerarse como marco de referencia para el tratamiento de evidencia digital, ya que proporciona pautas para su identificación, sistematización, recolección, adquisición y preservación.

Según esta norma, la evidencia digital está gobernada por tres principios fundamentales que definen la formalidad de una investigación y son condiciones necesarias y suficientes para que se recaben, aseguren y preserven elementos probatorios sobre medios digitales. Éstos son:

- *Relevancia*: condición técnicamente jurídica que habla sobre los elementos pertinentes a la situación que se analiza, con el fin de probar o rechazar una hipótesis sobre los hechos.
- *Confiabilidad*: acción orientada a saber si la evidencia que se extrae u obtiene es lo que debe ser. Se busca validar la repetibilidad y la auditabilidad del proceso aplicado para obtener la evidencia digital.
- *Suficiencia*: condición por la que con las evidencias recolectadas y analizadas hay suficientes elementos para sustentar los hallazgos y verificar las afirmaciones sobre la situación investigada.

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.

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.

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 trata de una investigación descriptiva-cualitativa, dado que si bien se definió una hipótesis que relaciona 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.

4. RESULTADOS OBTENIDOS

A la fecha se obtuvieron los siguientes resultados parciales:

1. *Relevamiento y análisis comparativos de protocolos y guías nacionales e internacionales para el tratamiento de la evidencia digital.* Tal como se destaca en [9], se han analizado las fases definidas en el Proceso Unificado de Recuperación de la Información PURI, que brinda una visión detallada y abarcadora de todo lo concerniente a la labor relacionada a la adquisición de evidencias digitales. Allí también, se consideran las normas ISO/IEC 27000, las cuales brindan una serie de definiciones relacionadas a la evidencia digital y establecen los principios fundamentales que definen la formalidad de una investigación: relevancia, confiabilidad y suficiencia.
2. Análisis jurídico-legal sobre tratamiento de evidencias digitales. Se ha analizado normativa y jurisprudencia nacional e internacional relacionada con el tratamiento de la evidencia digital sobre dispositivos móviles. Se han estudiado comparativamente diferentes códigos de procedimiento, analizando sus regulaciones sobre el proceso de obtención de la evidencia digital.
3. Relevamiento de las herramientas de hardware y software que se usan para obtener evidencias de móviles.
4. *Lineamientos para el tratamiento de evidencias digitales forenses sobre*

dispositivos móviles: se han identificado fases, a saber: recepción del requerimiento judicial, recolección y preservación de la evidencia digital, identificación del requerimiento judicial, adquisición de la copia forense, extracción y análisis de la evidencia digital, preparación del informe o dictamen pericial y la remisión de los elementos peritados y entrega del dictamen. Estas fases intentan garantizar el cumplimiento de las buenas prácticas que aseguren la calidad de los procesos aplicados y sus resultados, considerando los principios fundamentales de relevancia, confiabilidad y suficiencia establecidos en la norma ISO/IEC 27037[7].

A futuro, se pretende aplicar una lista de verificación con preguntas relacionadas con cada uno de los principios que establece la norma, debido a que el mencionado estándar sólo se describen los principios, pero no se especifican líneas de acción para llevarlos a cabo, a partir de las cuales se puedan derivar los mecanismos de validación asociados [2]

Al finalizar la investigación se espera contar con 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 [10].

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.

5. FORMACIÓN DE RECURSOS HUMANOS

La Directora y Codirectora del proyecto pertenecen al Departamento de Informática de la UNSE. Los asesores pertenecen a LIDI-FI-UNLP y FCE-UNSala.

Los investigadores de esta línea específica de Informática Forense constituyen un equipo interdisciplinario conformado por cinco docentes de la UNSE y de la Universidad Nacional de Salta (UNSa), con profesión en Informática y Derecho. Estos poseen distintas categorías de investigación y algunos desempeñan sus actividades profesionales en: Poder Judicial de la Provincia de Santiago del Estero, Gabinete de Ciencias Forenses del Ministerio Público Fiscal de Santiago del Estero y Poder Judicial de la Provincia de Salta.

El equipo de investigación se encuentra asistiendo y asesorando a alumnos de grado y posgrado de UNSE y UNSa que realizan sus trabajos de finalización de carrera en temáticas relacionadas con esta línea de investigación. Estos se encuentran en la etapa de propuesta inicial.

6. 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. CANO, J. (2013) IT-Insecurity. Disponible en http://insecurityit.blogspot.com.ar/2013/09/reflexiones-sobre-la-norma-isoiec.html
3. 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.

4. DARAHUGE, M. (2011). Manual de Informática Forense. Buenos Aires. Errepar.
5. HERRERA, S., 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. ISO/IEC 27037:2012(en) Information technology— Security techniques— Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
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. LESCA, N., LARA, C., FIGUEROA, L., VIAÑA, G. (2017). Gestión de evidencia digital en dispositivos móviles. Jornadas Argentinas de Informática - Simposio Argentino de Informática y Derecho. ISSN: 2451-7526
10. LEY 6.941. (2009). Código Procesal Penal de Santiago del Estero. Disponible en http://www.jussantiago.gov.ar/jusnueva/Normativa/Ley6941.pdf
11. VARSALONE, J., KUBASIAK, R. (2009). Mac Os X, iPod and iPhone Forensic Analysis DVD Toolkit. Syngress Publishing, Inc, pp. 355-475.