Métodos y herramientas para el análisis forense de dispositivos móviles

Susana Herrera, Liliana Figueroa, Daniel Ghunter, Cecilia Lara, Graciela Viaña, Analía Mendez, Norma Lesca

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; dgunther@unse.edu.ar; laraceciliacristina@gmail.com; gv857@hotmail.com; anmendez725@yahoo.com; norma.lesca@gmail.com

RESUMEN

Ante los desafíos que genera la evidencia digital en el sistema procesal penal como prueba en la investigación de delitos, la justicia necesita una regulación adecuada que permita obtener evidencias digitales legalmente aceptables, que ayuden a resolver conflictos según métodos científicos de recolección, análisis y validación. Aunque en algunas provincias de nuestro país existen guías de buenas prácticas y protocolos de actuación que orientan el trabajo pericial informático, Santiago del Estero no cuenta con normativa al respecto.

Como resultado del proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", se propuso un conjunto de lineamientos a los que recurrir al momento de obtención de evidencia digital de dispositivos móviles, pero éste aún no se validó para su utilización como protocolo aprobado por el Ministerio Publico Fiscal y el Poder Judicial de la provincia.

Este proyecto pretende realizar investigación aplicada para validar el protocolo propuesto, así como el cumplimiento de estándares que garanticen la calidad de los procesos y sus resultados, tomando como referencia la familia de normas ISO/IEC 27000. Además, atendiendo requerimientos identificados durante el desarrollo del proyecto mencionado anteriormente, se investigará sobre herramientas tecnológicas de apoyo a la adquisición y gestión de evidencias digitales obtenidas de dispositivos móviles.

Palabras clave:
Computación móvil, análisis forense, protocolo para el tratamiento de evidencias digitales.

CONTEXTO

En este artículo se presenta una propuesta de investigación que constituye una continuación del proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", llevado adelante durante 2017 y 2018, financiado por el Consejo de Ciencia y Técnica de la Universidad Nacional de Santiago del Estero [4].

En dicho proyecto se lograron resultados referidos al análisis de la obtención legal de la evidencia digital en los códigos procesales de nuestro país, de antecedentes jurisprudenciales sobre tratamiento de evidencia digital en dispositivos móviles, investigación y análisis de protocolos vigentes en otras jurisdicciones, una propuesta de lineamientos para la obtención de evidencia digital en móviles en el ámbito del Ministerio Público Fiscal de Santiago del Estero y el estudio de repositorios que permitan la construcción de un modelo de datos para la gestión de las evidencias [15].

El mencionado protocolo, organizado en fases, abarca el proceso completo del tratamiento de la evidencia digital. Pone énfasis en las actividades y técnicas relacionadas con dispositivos móviles, constituyendo una herramienta para la planificación y control de dicho proceso en la investigación penal preparatoria. No obstante, se requiere de una revisión y evaluación que permita garantizar la validez

y eficacia probatoria de las evidencias digitales obtenidas en el proceso.

Por otro lado, se determinó que durante el examen de dispositivos móviles, los peritos informáticos se enfrentan a las siguientes dificultades:

1. No existe un software de informática forense que soporte la extracción de datos desde todos los dispositivos móviles existentes en el mercado.
2. Existe un gran número de programas diseñados para el sistema operativo Android donde los datos pueden ser interesantes para los investigadores de pruebas de penetración, pero hasta el momento no se cuenta con programas de apoyo de análisis forense de sus registros y datos.
3. Los requerimientos para los peritos forenses no están claros y bien definidos desde el inicio de la investigación.
4. Los delincuentes suelen eliminar los archivos de la memoria de sus dispositivos móviles, tratando de ocultar información sobre el crimen cometido.
5. Los laboratorios de informática forense no siempre pueden permitirse la compra de software especializado, debido a su alto costo.

En este contexto, se advierte la necesidad de trabajar en la validación del protocolo de actuación para el análisis de evidencias forenses obtenidas de dispositivos móviles propuesto anteriormente, y de incluir guías de actuación buscando aportar soluciones a los problemas que enfrentan los peritos informáticos.

1. INTRODUCCIÓN

Tradicionalmente, el concepto de evidencia se asoció al de evidencia física. Sin embargo, con el auge de las tecnologías de la información y la comunicación, surgió la evidencia digital, que también puede ser usada como medio de prueba en juicio [9].

En comparación con la evidencia tradicional, la digital es única: es sensiblemente frágil, anónima y volátil. Si fue presentada correctamente y su cadena de custodia no fue alterada, puede llegar a ser decisiva para resolver cualquier clase de delito.

La Informática Forense es una disciplina de las ciencias forenses que involucra la aplicación de metodologías científicas para identificar, preservar, recuperar, extraer, documentar e interpretar [16] evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos [11], para usar luego dichas evidencias como elemento probatorio en un proceso judicial [3,2].

Por otra parte, el empleo de dispositivos móviles se incrementó notablemente en los últimos diez años, debido a su facilidad de uso y a la propiedad de mantener en contacto permanentemente a sus usuarios. Esto generó un cambio significativo en el modo de comunicación de las personas, pero también incrementó su uso en actividades delictivas [8].

El análisis forense sobre dispositivos móviles es un campo relativamente nuevo, por lo que sus procedimientos y normas aún se encuentran en desarrollo [14]. Para lograr un análisis forense digital confiable y que la evidencia que se recoja sea admisible, auténtica, completa, fiable, entendible y creíble, es importante seguir los lineamientos formales establecidos en un protocolo de actuación.

Actualmente, la norma de alcance global de referencia para el análisis forense es la ISO/IEC 27037:2012 [6], aplicable a las organizaciones que necesiten establecer un marco formal de aceptabilidad. Dicha norma proporciona pautas para el manejo de la evidencia digital, sistematizando su identificación, recolección, análisis y preservación, y asegurando que los responsables de gestionar evidencia digital lo hagan con prácticas mundialmente aceptadas, de manera sistemática e imparcial. De acuerdo a ella, la evidencia digital es gobernada por los principios

fundamentales de relevancia, confiabilidad y suficiencia.

Por otro lado, para la adquisición de datos y clasificación de herramientas, es posible tomar como referencia el "Sistema de clasificación de herramientas forenses de dispositivos móviles" [1], que presenta la Pirámide Móvil Forense con cinco niveles de extracción y análisis requeridos en cada dispositivo móvil, teniendo en cuenta la solicitud y los detalles de la investigación.

En relación a la problemática referida, las principales contribuciones desarrolladas en el ámbito de nuestro país son:

- *"Guía de obtención, preservación y tratamiento de la evidencia digital"* [13] de la Unidad Fiscal Especializada en Ciberdelitos de la Procuración General de la Nación. Este trabajo brinda una serie recomendaciones utilizadas a nivel mundial y de herramientas de investigación, abordando el modo en el que se debe obtener, observar y tratar la evidencia digital para mejorar los niveles de eficiencia en persecución penal.
- *"Protocolo de actuación para pericias informáticas del Poder Judicial de Neuquén"* [10], donde se aborda la pericia sobre telefonía celular como parte de la especialidad de la informática forense, un procedimiento para pericias informáticas sobre telefonía celular y el uso del Universal Forensic Extraction Device (UFED).
- *"Guía integral de empleo de la informática forense en el proceso penal"*[5], del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InfoLab), que presenta los aspectos básicos a considerar en las labores de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales en el proceso penal, a fin de garantizar su validez y eficacia probatoria.
- *"Guía de procedimientos para pericias de dispositivos móviles"* [12] del Poder Judicial de Río Negro, donde se presenta la metodología del ciclo de vida de la evidencia digital, considerando en estado en que se encuentra el equipo y el lugar donde se lleva a cabo la intervención.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Considerando la amplitud de los aspectos relacionados con la informática forense sobre computación móvil, el presente proyecto de investigación se refiere a:

Informática Forense: métodos y herramientas para el análisis forense de dispositivos móviles.

A partir de él, 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.
- Repositorio digital para la gestión de evidencias digitales extraídas de dispositivos móviles.

3. OBJETIVOS

El objetivo general de la investigación propuesta es:

- *Contribuir al mejoramiento de la calidad del proceso de obtención de evidencias digitales obtenidas de dispositivos móviles en el ámbito judicial de Santiago del Estero.*

Los objetivos específicos que permitirán alcanzar el objetivo general son:

- *Validar el Protocolo para la obtención de evidencias digitales de dispositivos móviles en el ámbito judicial de Santiago del Estero.*
- *Ampliar el Protocolo de obtención de evidencias digitales de dispositivos móviles considerando el sistema de clasificación de*

herramientas forenses de dispositivos móviles.

- *Analizar alternativas de construcción de repositorio digital para la gestión de evidencias digitales extraídas de dispositivos móviles.*

En esta propuesta se pretende llevar a cabo una investigación aplicada para validar el Protocolo de Actuación propuesto en el proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", para el cumplimiento de buenas prácticas tendientes a garantizar la calidad de los procesos aplicados y los resultados obtenidos, tomando como referencia la familia de normas ISO/IEC 27000, más específicamente las normas ISO/IEC 27037:2012 [6] y 27042:2015 [7].

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, la variable a estudiar es la "optimización de la gestión de evidencias criminales obtenidas de dispositivos móviles", que podrá ser evaluada a través de indicadores cuantitativos que se pueden aplicar a casos de prueba especialmente diseñados.

Durante la validación de la aplicabilidad del protocolo propuesto se realizarán experiencias de puesta en marcha con el propósito de lograr un consenso técnico en la materia, y permitiendo que se generen nuevas versiones del mismo a partir de las sugerencias y recomendaciones derivadas de los informes de estas experiencias.

Se considera que la validación del mencionado protocolo, y su posterior aceptación por parte del Ministerio Público Fiscal y el Poder Judicial de Santiago del Estero, traerán un beneficio muy importante para la justicia santiagueña, dado que actualmente no existe un procedimiento claro y definido al respecto. Esto permitiría mejorar la calidad de las evidencias digitales y ayudará en la labor de los fiscales y peritos 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. El asesor es experto en Informática Forense y jefe del área de Informática Forense del Poder Judicial de Río Negro.

Los investigadores constituyen un equipo interdisciplinario conformado por cuatro docentes de la UNSE y un investigador externo, con profesión en Informática, Electromecánica y Derecho. Estos poseen distintas categorías de investigación y algunos desempeñan sus actividades profesionales en el Poder Judicial de la Provincia de Santiago del Estero y el Gabinete de Ciencias Forenses del Ministerio Público Fiscal de Santiago del Estero.

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

5. REFERENCIAS

1. AYERS, R.; BROTHERS, S.; JANSEN, W. (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revision 1. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf
2. CASTILLO, C.; ROMERO, A.; CANO, J. (2008). Análisis Forense Orientado a Incidentes en Teléfonos Celulares GSM: Una Guía Metodológica. XXXIV Conferencia Latinoamericana de Informática, Centro Latinoamericano de Estudios en Informática (CLEI). http://www.clei2008.org.ar/

3. DEL PINO, S. (2007). Introducción a la informática forense. Pontificia Universidad Católica del Ecuador. http://www.criptored.upm.es/guiateoria/gt_m592b.htm
4. FENNEMA, M.; FIGUEORA, L.; VIAÑA, G.; LESCA GOMEZ, N.; LARA, C. (2017). Tratamiento de evidencias digitales forenses en dispositivos móviles. XIX Workshop de Investigadores en Ciencias de la Computación. ISBN 978-987-42-5143-5.
5. INFO-LAB. (2015). Guía integral de empleo de la informática forense en el proceso penal. http://info-lab.org.ar/images/pdf/14.pdf
6. 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
7. ISO/IEC 27042:2015 (en) Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en
8. MELLAR, B. (2004). Forensic Examination of Mobile Phones. Digital Investigation – Elsevier. United Kingdom. http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf
9. ORTA MARTINEZ, R. (2013). Informática Forense como Medio de Pruebas. http://www.dragonjar.org//informatica-forense-como-medio-de-prueba.xhtml
10. PODER JUDICIAL DE NEUQUÉN. (2013). Pericias informáticas sobre telefonía celular. http://200.70.33.130/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf
11. REITH, M.; CLINT, C.; GUNSCH G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, Air Force Institute of Technology, Volume 1 Issue 3. www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.
12. SUP. TRIBUNAL DE JUSTICIA DEL PODER JUDICIAL DE RÍO NEGRO. (2015). Guía de procedimientos para pericias de dispositivos móviles. http://digesto.jusrionegro.gov.ar/bitstream/handle/123456789/455/Ac011-15.pdf?sequence=1&isAllowed=y
13. UNIDAD FISCAL ESPECIALIZADA EN CIBERDELITOS. (2016). Guía de obtención, preservación y tratamiento de evidencia digital. http://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2016/04/PGN-0756-2016-001.pdf
14. VARSALONE, J., KUBASIAK, R. (2009). Mac Os X, iPod and iPhone Forensic Analysis DVD Toolkit. Syngress Publishing, Inc, pp. 355-475.
15. VIAÑA, G.; FIGUEORA, L.; LARA, C.; LESCA GOMEZ, N. (2018). Protocolo de actuación para recolección y preservación de la evidencia digital móvil en el Sistema Procesal Penal de Santiago del Estero. VI Congreso Nacional de Ingeniería en Informática y Sistemas de Información. ISSN 2347-0372.
16. ZDZIARSKI, J. (2008). iPhone Forensics, Recovering Evidence, Personal Data & Corporate Assets. O‟Reilly Media, Inc.