MÉTODOS Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES

Graciela Viaña, Liliana Figueroa, Cecilia Lara, Analía Méndez, Norma Lesca, Daniel Ghunter

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

RESUMEN

La evidencia digital genera grandes desafíos al utilizarse en el sistema procesal penal como prueba en la investigación de delitos, por lo que la justicia necesita contar con una regulación adecuada que permita obtener evidencias digitales legalmente aceptables, que ayuden a resolver conflictos según métodos científicos de recolección, análisis y validación.

En este sentido, Santiago del Estero requiere de guías de buenas prácticas y/o protocolos de actuación que orienten el trabajo pericial informático, así como contar con estrategias que permitan almacenar y mantener las evidencias digitales obtenidas de dispositivos móviles.

En esta etapa de la investigación, y con la intención de validar el conjunto de lineamientos obtenido como resultado del proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", se propone establecer un instrumento de validación teniendo en cuenta el cumplimiento de estándares internacionales de calidad.

Por otro lado, se encuentran en etapa de evaluación los aspectos a considerar en el diseño de un repositorio para el almacenamiento de la evidencia digital obtenida de dispositivos móviles, así como la exploración sistemática y análisis del sistema de clasificación de herramientas forenses de dispositivos móviles [1].

Palabras clave:

Computación móvil, análisis forense, lineamientos para el tratamiento de evidencia digital, repositorio digital.

CONTEXTO

La presente línea de investigación se encuentra inserta en el proyecto "Métodos y herramientas para el análisis forense de dispositivos móviles" (23/C156), iniciado en el año 2019, financiado por el Consejo de Ciencia y Técnica de la Universidad Nacional de Santiago del Estero [5]. Este proyecto es una continuación de trabajos realizados desde el año 2017 en el proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense" [4].

Como producto de estas investigaciones se lograron resultados referidos al análisis de la obtención legal de la evidencia digital, estudio de antecedentes jurisprudenciales sobre tratamiento de evidencia digital en dispositivos móviles, investigación y análisis de protocolos vigentes en otras jurisdicciones y una propuesta de protocolo de actuación para la obtención de evidencia digital en móviles en el ámbito del Ministerio Público Fiscal de Santiago del Estero [17].

Actualmente, el equipo de investigación tiene como propósito fijar estrategias de validación de la propuesta de protocolo para que sea factible su implementación tomando como principal referencia la familia de normas ISO/IEC 27000, realizar el estudio de repositorios que permitan la construcción de un modelo de datos para la gestión de las evidencias digitales y analizar la aplicabilidad de las herramientas de los niveles superiores de la pirámide móvil forense.

Con este fin, se establecieron convenios con el Ministerio Público Fiscal y el Poder Judicial de Santiago del Estero, instituciones

donde se pretende llevar a cabo la validación en campo de los resultados alcanzados.

1. INTRODUCCIÓN

La justicia se encuentra actualmente ante el desafío de la utilización de la evidencia digital como prueba fundamental en la investigación de diferentes delitos [10]. El empleo de dispositivos móviles se incrementó notablemente y por consiguiente su uso en actividades delictivas [9].

En este contexto, es necesaria una regulación adecuada para la obtención de evidencia digital desde dispositivos móviles, apoyada en métodos científicos, que considere los aspectos de fragilidad, anonimidad y volatilidad que diferencian a la evidencia digital de la física, y que garantice su posterior validez en juicio.

La Informática Forense involucra la aplicación de la metodología y la ciencia para identificar, preservar, recuperar, extraer, documentar e interpretar [18] evidencias procedentes de fuentes digitales, para facilitar la reconstrucción de los hechos en la escena del crimen [12] y utilizarlas posteriormente como material probatorio en un proceso judicial [2,3].

A diferencia de la Informática Forense clásica, la Informática Forense sobre móviles es un campo relativamente nuevo, donde las normas y procedimiento se encuentran aún en desarrollo [16]. La admisibilidad de un análisis forense sobre móvil está determinada por la formalidad con que se realice el proceso de recolección, control, análisis y presentación de la evidencia, donde los protocolos desempeñan un rol fundamental.

Aunque en algunas provincias de nuestro país existen guías de buenas prácticas y protocolos de actuación relacionados con la evidencia digital, Santiago del Estero no cuenta con normativa al respecto. En este sentido, las principales contribuciones desarrolladas en el país son:

- *"Guía de obtención, preservación y tratamiento de la evidencia digital"* [15] de la Unidad Fiscal Especializada en Ciberdelitos de la Procuración General de la Nación. Aborda cómo se debe obtener, observar y tratar la evidencia digital para mejorar la eficiencia en el ámbito penal.
- *"Protocolo de actuación para pericias informáticas del Poder Judicial de Neuquén"* [11]. Aporta 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"* [6], del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InfoLab). Presenta los aspectos básicos a considerar en la búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales.
- *"Guía de procedimientos para pericias de dispositivos móviles"* [14] del Poder Judicial de Río Negro. Propone una metodología del ciclo de vida de la evidencia digital.

Como respuesta a la necesidad planteada en la provincia de Santiago del Estero, se propuso un conjunto de lineamientos a los que recurrir para la obtención de evidencia digital de dispositivos móviles [17], que se encuentra en proceso de validación para su utilización como protocolo por el Ministerio Publico Fiscal de Santiago del Estero. La mencionada propuesta, organizada en fases, abarca el proceso completo de tratamiento de la evidencia digital, con especial énfasis en las actividades y técnicas relacionadas con dispositivos móviles, constituyendo una herramienta que permita a los peritos y operadores judiciales realizar una adecuada planificación y control de las actividades periciales durante la investigación penal preparatoria.

Para diseñar las actividades de validación de la propuesta del protocolo, tendientes a garantizar la calidad de los procesos aplicados y sus resultados, se tomaron como

principal referencia los siguientes estándares internacionales:

- La norma ISO/IEC 27042:2015 "*Guidelines for the analysis and interpretation of digital evidence*" [8], que propone una serie de definiciones relacionadas a la evidencia digital.
- La norma ISO/IEC 27037:2012 "*Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*" [7], que establece los 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.
- Las directrices RFC 3227 – "*Guidelines for Evidence Collection and Archiving*" [13], que ofrecen una guía de alto nivel para recolectar y archivar evidencia, estableciendo principios a respectar durante dichos procesos, así como consideraciones legales.

Durante el desarrollo de la investigación, se logró determinar que los principales problemas con los que se enfrentan los peritos informáticos de la provincia son: la ausencia de herramientas que permitan la extracción de datos desde todos los dispositivos móviles del mercado, los requerimientos recibidos no se encuentran claramente definidos desde el inicio, y la imposibilidad de compra de paquetes de software especializado debido a su alto costo.

Para abordar dichos problemas y realizar los ajustes pertinentes en la propuesta de protocolo, se tomó como referencia "El Sistema de Clasificación de Herramientas Forenses de Dispositivos Móviles" [1], que presenta la Pirámide Móvil Forense, poniendo especial atención en los niveles superiores de la misma. Según esta propuesta el nivel de extracción y el análisis requerido dependen de la solicitud y los detalles de la investigación, y cada nivel tiene su propio conjunto de requerimientos de aplicación. Los niveles más altos requieren un examen más completo y de habilidades adicionales de los peritos, que pueden no ser aplicables en todos los dispositivos y situaciones.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El presente proyecto de investigación se refiere a:

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

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. RESULTADOS OBTENIDOS Y ESPERADOS

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 adelante una investigación aplicada para validar el Protocolo de Actuación propuesto, para el cumplimiento de buenas prácticas que garanticen tanto la calidad de los procesos aplicados como de los resultados obtenidos, tomando como referencia estándares internacionales mencionados anteriormente.

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.

Para realizar la validación de la aplicabilidad del protocolo propuesto se planificaron reuniones de trabajo y experiencias de puesta en marcha en el ámbito del Ministerio Público Fiscal de Santiago del Estero, con el fin 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 elaborados como resultado de dichas experiencias.

Se considera que la validación de la propuesta de protocolo, y su posterior aceptación por parte del Ministerio Público Fiscal y el Poder Judicial de Santiago del Estero, traerán un beneficio significativo para la justicia santiagueña, dado que actualmente no existe un procedimiento claro y definido que brinde un marco de trabajo a las actividades periciales. 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 Gabinete de Ciencias Forenses del Ministerio Público Fiscal de Santiago del Estero y en el Juzgado Federal 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 finales de carrera en temáticas relacionadas con esta línea de investigación, los que se encuentran actualmente en etapa de finalización.

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. HERRERA S.; FIGUEROA L.; GHUNTER D.; LARA C.; VIAÑA G.; MÉNDEZ A.; LESCA N. (2019)"Métodos y herramientas para el análisis forense de dispositivos móviles". XXI Workshop de Investigadores en Ciencias de la Computación. http://redunci.info.unlp.edu.ar/docs/Libro_WICC_2019-con_paginas.pdf
6. INFO-LAB. (2015). Guía integral de empleo de la informática forense en el proceso penal. http://info-lab.org.ar/images/pdf/14.pdf
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. 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
9. 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
10. ORTA MARTINEZ, R. (2013). Informática Forense como Medio de Pruebas. http://www.dragonjar.org//informatica-forense-como-medio-de-prueba.xhtml
11. PODER JUDICIAL DE NEUQUÉN. (2013). Pericias informáticas sobre telefonía celular. http://200.70.33.130/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf
12. 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.
13. RFC3227 - Guidelines for Evidence Collection and Archiving. https://www.ietf.org/rfc/rfc3227.txt
14. 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
15. 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
16. VARSALONE, J., KUBASIAK, R. (2009). Mac Os X, iPod and iPhone Forensic Analysis DVD Toolkit. Syngress Publishing, Inc, pp. 355-475.
17. 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.
18. ZDZIARSKI, J. (2008). iPhone Forensics, Recovering Evidence, Personal Data & Corporate Assets. O"Reilly Media, Inc.