Gestión de evidencia digital en dispositivos móviles

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

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

Este artículo es el resultado de la etapa exploratoria de la línea de investigación "Informática Forense" 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 iniciado en el año 2012 [1].

La línea atiende requerimientos relacionados con el proceso de obtención de evidencias digitales en dispositivos móviles, surgidos desde el ámbito judicial ante la implementación del Nuevo Sistema Procesal Penal en la Provincia de Santiago del Estero, planteando como desafío la definición de un protocolo para la gestión de evidencias digitales forenses obtenidas de dispositivos móviles. Este protocolo permitirá contar con un proceso de adquisición legalmente aceptable, apoyado en métodos científicos de recolección, análisis, validación y conservación de evidencias digitales obtenidas de dispositivos móviles.

Se tomarán como referencia las fases definidas en el Proceso Unificado de Recuperación de la Información PURI [2], que brinda una visión detallada y abarcadora de la labor de adquisición de evidencias digitales. Para garantizar el cumplimiento de las buenas prácticas tendientes a asegurar la calidad de los procesos aplicados y sus resultados, se considerará la familia de normas ISO/IEC 27000:

- ISO/IEC 27042:2015 *"Guidelines for the analysis and interpretation of digital evidence"* [3], que propone definiciones relacionadas a la evidencia digital.
- ISO/IEC 27037:2012 "*Guidelines for identification, collection, acquisition and preservation of digital evidence*"[4], que establece 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: relevancia, confiabilidad y suficiencia.

Según Cano [5], la dificultad para validar el cumplimiento de los principios del estándar radica en que el documento de la norma sólo los describe pero no especifica vías de acción para llevarlos a cabo, de las que se puedan derivar los mecanismos de validación asociados. Para hacerlo, se considerarán listas de verificación con preguntas relacionadas con cada uno de los principios.

Como resultado, se espera generar nuevo conocimiento científico-tecnológico, plasmado en un protocolo para la gestión de evidencias digitales extraídas de dispositivos móviles, que cumplan con los principios de calidad establecidos en los estándares. Para la gestión óptima de la evidencia digital, se plantea también la necesidad del diseño de un modelo de datos, que permitiría la democratización del conocimiento proporcionando acceso, recuperación y clasificación de las evidencias digitales en el tratamiento de las causas penales.

Referencias

1. Herrera, S., Najar P., Rocabado S., Fennema, C., Cianferoni, M. (2013). Optimización de la calidad de los sistemas móviles. Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/27200/Optimizaci%C3%B3n_de_la_calidad_de_los_sistemas_m%C3%B3viles.pdf?sequence=1
2. Di Iorio, A [et al.] (2015). Guía Integral de Empleo de la Informática Forense en el Proceso Penal. Universidad FASTA. Mar del Plata. Argentina.
3. ISO/IEC 27042:2015(en) Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en
4. ISO/IEC 27037:2012(en) Information technology— Security techniques— Guidelines for identification, collection, acquisition and preservation of digital evidence. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
5. Cano, J. (2013) IT-Insecurity. Disponible en: http://insecurityit.blogspot.com.ar/2013/09/reflexiones-sobre-la-norma-isoiec.html