Gestión del conocimiento aplicada al peritaje informático

Leopoldo Sebastián M. Gómez [1,2], Hernán Horacio Herrera [1]

[1] Laboratorio Pericial Informático (LPI)
Poder Judicial del Neuquén

[2] Programa de Magíster en Informática (dirección de tesis)
Universidad Nacional de La Matanza

sebastian.gomez@jusneuquen.gov.ar

CONTEXTO

Esta línea de investigación apoya la actualización profesional y capacitación permanente de recursos humanos especializados en informática forense dentro del Poder Judicial del Neuquén.
Se contribuye a nivel académico con la Escuela de Posgrado de la UNLaM, mediante la dirección externa de tesistas de la Maestría en Informática.

RESUMEN

Desde el Laboratorio Pericial Informático del Poder Judicial del Neuquén se impulsan actividades de I+D orientadas a la gestión del conocimiento aplicada al peritaje informático. Se pretende generar un cuerpo de conocimientos que sea útil para la formación de profesionales auxiliares de la Justicia noveles, reduciendo los tiempos de aprendizaje de metodologías, técnicas y herramientas de informática forense. Se ha instrumentado la implementación de un repositorio de información digital que permitirá compartir el conocimiento especializado con otras instituciones judiciales y de las fuerzas de seguridad. Se espera integrar tecnologías de enseñanza virtual para contribuir con una futura formación a nivel de posgrado de especialistas en peritaje informático, haciendo énfasis en la investigación de delitos informáticos.

Palabras clave: *digital forensics, knowledge management*

1. INTRODUCCION

Durante la investigación de actividades delictivas, habitualmente se plantea un conjunto de objetivos o medidas tendientes a esclarecer un presunto ilícito. Esta modalidad de trabajo permite definir tres capas de abstracción a partir del caso judicial. El nivel superior, que mantiene la visión del caso en forma integral, es el marco de trabajo en el que se mueven los profesionales del derecho (jueces, fiscales, defensores, abogados, etc.). En el segundo nivel se establece la interacción entre los profesionales de diversas disciplinas. En este ámbito se plantean los objetivos -requerimientos periciales o informes técnicos- sobre los cuales actúan profesionales informáticos, contadores, médicos forenses, etc. Finalmente, el último nivel es el que pertenece en forma exclusiva a los expertos en la disciplina a la que pertenezca la actividad forense solicitada como objetivo para la investigación.

El avance constante de la tecnología obliga a los especialistas informáticos a mantener una actualización profesional permanente en desmedro de otros tiempos que son necesarios para la colaboración entre colegas. La posibilidad de capturar el conocimiento forense juega un rol crucial en el entrenamiento y la diseminación de mejores prácticas [1]. Es por ello que la gestión del conocimiento se presenta como un método adecuado para superar las limitaciones de tiempo y recursos humanos, contribuyendo a reducir la creación individual de información

redundante y permitiendo compartir en forma eficiente una mayor cantidad de recursos.

Aunque varias organizaciones han presentado definiciones alternativas del concepto de informática forense, se pueden encontrar algunas relaciones entre las metodologías [2]. Se necesita contar con un esquema de trabajo metódico y disciplinado para el desarrollo de labores periciales. La síntesis y ordenamiento sistemático de los componentes involucrados en tareas periciales permite reducir los tiempos del trabajo mediante la ejecución paralela de actividades forenses, siempre que se cuente con recursos humanos especializados y herramientas adecuadas [3].

En informática forense no existe una ventaja inmediata en el suministro de información a terceros. Los temores razonablemente fundados de que la información y experiencia documentada pueda ser utilizada con fines ilícitos para mejorar las actividades delictivas motivan a que los especialistas no deseen compartir el conocimiento aplicado al desarrollo de sus labores cotidianas [4].

2. LINEAS DE INVESTIGACION y DESARROLLO

La estructuración de contenidos periciales en un repositorio digital con los niveles de acceso apropiados permitiría al investigador menos experimentado contar con una valiosa fuente de información, accediendo a recursos compartidos ofrecidos por otros profesionales expertos. Contar con recursos humanos capacitados para el tratamiento de evidencia digital es uno de los principales puntos críticos para conducir la investigación a resultados exitosos [5]. Estas lecciones literalmente ahorran al perito o analista forense docenas de horas de investigación y métodos de prueba y error [6].

Por otra parte, las ventajas ofrecidas por un gestor de contenidos periciales minimizaría la necesidad de contar con personal especializado para la edición y publicación de información. Asimismo, es viable incorporar un mecanismo que permita el intercambio seguro de información sensible o relevante entre analistas forenses y el personal policial. No menos importante es destacar la necesidad de utilizar tecnologías de código abierto, considerando los escasos recursos financieros con que cuentan los organismos judiciales y policiales.

La posibilidad de recopilar el conocimiento de investigación en informática forense, como así también las prácticas de laboratorio y la casuística juegan un rol crucial en el entrenamiento de nuevos peritos y la difusión de mejores prácticas en la comunidad forense.

Para motivar a los especialistas a compartir sus conocimientos se requiere implementar una solución tecnológica que integre en forma simple y clara las áreas clave del trabajo operativo pericial y facilite el acceso a los recursos en formato digital.

Se cuenta con un corpus importante de reseñas científicas de informática forense que han sido recopiladas en forma manual y son utilizadas como material de consulta del Laboratorio Pericial Informático del Poder Judicial del Neuquén. Dichos documentos digitales conformarán los contenidos mínimos del repositorio de información digital para la implementación de un sistema de gestión de contenidos periciales.

A la fecha, sólo se han detectado implementaciones de relevancia en esta línea de trabajo en instituciones extranjeras de gran porte como el Defense Cyber Crime Center (DC3) [7], quienes en forma conjunta con Oklahoma State University's Center for Telecommunications and Network Security (CTANS), auspician el desarrollo y operación del National Repository for Digital Forensics Intelligence (NRDFI) [8]. El material digital organizado en este sistema de gestión de conocimiento es accesible solamente a las agencias de seguridad y fuerzas de la ley de EEUU y países asociados al Five Eyes Agreement (Australia, Canadá, Inglaterra y Nueva Zelanda).

3. RESULTADOS OBTENIDOS/ESPERADOS

La esencia de generar un repositorio de información digital consiste en capturar y compartir las mejores practicas de los peritos con aquellos que tengan que descubrir o desarrollar las mismas técnicas o similares. Un repositorio digital debe soportar virtualmente cualquier tipo de archivo de texto o binario, enlaces a páginas web, y permitir realizar búsquedas sobre todo el contenido que en él se almacene.

Se pretende obtener un cuerpo mínimo de conocimientos mediante la recolección de trabajos sobre informática forense y evidencia digital que sean de mayor aceptación en la comunidad forense, principalmente guías de mejores prácticas, guías de procedimientos y manuales de informática forense. Se han aplicado entrevistas estructuradas para comprender las necesidades de los peritos durante sus actividades operativas, con el objeto de refinar el repositorio hacia una taxonomía de tópicos forenses de uso frecuente.

Por otra parte, se ha seleccionado la tecnología apropiada para la gestión de contenidos periciales y se implementará un sistema informático capaz de integrar todas las áreas clave pertenecientes al dominio de trabajo de los especialistas en informática forense. Se definirán niveles de acceso con el objeto de garantizar el acceso restringido a información clasificada. Los usuarios del gestor de contenidos periciales tendrán acceso a la información en función a los permisos que le otorgue un administrador local.

Se espera contar con un repositorio organizado de contenidos educativos especializados que junto a la tecnología de e-learning adecuada permita ser compartido con otros profesionales del país y Latinoamérica, principalmente del ámbito judicial y de las fuerzas de seguridad.

4. FORMACION DE RECURSOS HUMANOS

En esta línea de I+D se está apoyando a un alumno avanzado para la elaboración del proyecto de tesina de grado de Licenciatura en Ciencias de la Computación en la UNCo, y de un alumno de posgrado en la Maestría en Informática de la UNLaM. En el Poder Judicial del Neuquén se aplicarán los resultados obtenidos a la capacitación interna de profesionales que se incorporen al Laboratorio Pericial Informático para formarse como especialistas en peritaje informático.

5. BIBLIOGRAFIA

[1]. Bruschi, D., Monga, M. and Martignoni, L., (2004), "How to Reuse Knowledge about Forensic Investigations", Proceedings of the Digital Forensic Research Workshop. Accedido el: 26/03/2009 de http://dfrws.org/2004/day3/D3-Martignoni_Knowledge_reuse.pdf

[2]. Sansurooah, K., (2006), "Taxonomy of computer forensics methodologies and procedures for digital evidence seizure", Proceedings of the 4th Australian Digital Forensics Conference, ISBN 0-7298-0624-3.

[3]. Gómez, L., (2006), "La investigación de actividades delictivas con alta tecnología", JAIIO, Simposio de Informática y Derecho.

[4]. Biros, D., Weiser, M. and Whitfield, J., (2007), "Managing Digital Forensic Knowledge: An Applied Approach" Proceedings of the 5th Australian Digital Forensics Conference.

[5]. Gómez, L., (2004), "El tratamiento de la Evidencia Digital", JAIIO, Simposio de Informática y Derecho.

[6]. Harrison, W., Aucsmith, D., Heuston, G., Mocas, S., Morrissey, M., & Russelle, S., (2002), "A lessons learned repository for computer forensics", International Journal of Digital Evidence, 1(3).
Accedido el: 26/03/2009 de http://www.utica.edu/academic/institutes/ecii/publications/articles/A049D6C7-93E9-51F2-A468BF90038985DB.pdf

Referencias citadas

[7] Defense Cyber Crime Center
http://www.dc3.mil

[8] National Repository for Digital Forensics Intelligence
http://www.nrdfi.net