El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012

Santiago Roatta[1], María Eugenia Casco[2], Martín Fogliato[3],

[1] Facultad Tecnología Informática / Universidad Abierta Interamericana
Ovidio Lagos 934, Rosario, 0341-4356510
santiago.roatta@gmail.com

[2] Dirección de Inteligencia Criminal Estratégica de la Dirección General de Policía de Investigaciones / Ministerio de Seguridad de la Prov. De Santa Fe
Primera Junta 2823, 0342-4505100
mecasco@gmail.com

[3] Facultad de Derecho / Universidad Nacional de Rosario
Córdoba 2020, Rosario, 0341-4802634
gfogliato@netcoop.com.ar

Resumen. La evidencia digital bien procesada puede aprovecharse al máximo en distintos escenarios. En cada uno de ellos existe una orientación diferente respecto de lo que se pretende obtener: calidad probatoria, precisión en el análisis, restauración del servicio y/o el costo de la recolección de la evidencia. Los componentes clave que proporcionan credibilidad en la investigación son la metodología aplicada durante el proceso y la calificación de los individuos que intervienen en el desarrollo de las tareas especificadas en la metodología. Este trabajo presenta pautas para el manejo de la evidencia digital; sistematizando la identificación, adquisición, análisis y preservación de la misma. Estos procesos están diseñados para mantener la integridad de la evidencia, con una metodología aceptable para contribuir a su admisibilidad en procesos legales y en sintonía con las normas ISO/IEC 27037:2012 [1]. En concordancia con la ley provincial 13139 [2] (que tiene por objeto migrar el software propietario que utiliza la provincia de Santa Fe hacia software libre), un objetivo adicional es no solo generar nuevas herramientas y protocolos de análisis digital forense sino también evaluar aquellos ya existentes. Finalmente, se muestran los resultados del análisis y la valoración de algunas herramientas GNU disponibles.

Palabras Clave: Informática forense, Normas ISO/IEC 27037:2012.

1 Los orígenes de la informática forense

El análisis digital forense es la aplicación de técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Es una disciplina que comienza con los orígenes mismos de la electrónica digital pero se ha desarrollado de manera diferente. Mientras el hardware digital y la informática han tenido un desarrollo y difusión tan extendido, que son un acabado ejemplo de la llamado globalización; la informática forense tiene un modelo actuación propio según las leyes de cada país.

El campo de la informática forense se inició a fines de los años 70, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores.

En 1978, el estado de Florida reconoce los crímenes de sistemas informáticos en el Computer Crimes Act, en casos de sabotaje, copyright, modificación de datos y ataques similares. Nace Copy II PC de Central Point Software en 1981. También es conocida como copy2pc, que se usaba para la copia exacta de disquetes, que generalmente estaban protegidos para evitar copias piratas. El producto es posteriormente integrado en las Pc Tools. La compañía es un éxito y es comprada por Symantec en 1994. En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas Norton Utilities, entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente. Otras aplicaciones también serán útiles desde la perspectiva forense, como FileFix o TimeMark. Con el éxito de la suite de aplicaciones, Norton publica varios libros técnicos, como Inside the I.B.M. Personal Computer: Access to Advanced Features and Programming, del que su octava edición se publicó en 1999, 11 años después de la primera edición. En 1984 el FBI forma el Magnetic Media Program, que más tarde, en 1991, será el Computer Analysis and Response Team (CART). En 1986 Clifford Stoll colabora en la detección del hacker Markus Hess. En 1988 publica el documento Stalking the Wily Hacker contando lo ocurrido. Este documento es transformado en 1989 en un libro, anticipando una metodología forense. En 1987 nace la compañía AccessData, pionera en el desarrollo de productos orientados a la recuperación de contraseñas y el análisis forense con herramientas como la actual Forensic Toolkit (FTK). En 1988 se crea la International Association of Computer Investigative Specialists (IACIS), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE), una de las certificaciones más prestigiosas en el ámbito forense. En este mismo año se desarrolla el programa Seized Computer Evidence Recovery Specialists o SCERS, con el objetivo de formar a profesionales en computer forensics. El libro A forensic methodology for countering computer crime, de P. A. Collier y B. J. Spaul acuña en 1992 el término computer forensics. Otros libros posteriores continuarán desarrollando el termino y la metodología, como: High-Technology Crime: Investigating Cases Involving Computers de Kenneth S. Rosenblatt. En 1995 se funda el International Organization on Computer Evidence (IOCE), con objetivo de ser punto de encuentro entre especialistas en la evidencia electrónica y el intercambio de información. A partir de 1996 la Interpol organiza los International Forensic Science Symposium, como foro para debatir los avances forenses, uniendo fuerzas y conocimientos. En agosto de

2001 nace la Digital Forensic Research Workshop (DFRWS), un nuevo grupo de debate y discusión internacional para compartir información.

2 Panorama actual

El equipo participante en el proyecto tiene una gran experiencia sobre las necesidades, limitaciones y dificultades materiales que surgen a la hora de validar los resultados periciales de un sistema electrónico para formar parte en un proceso legal. A partir de este conocimiento, se está investigando acerca de los desarrollos preexistentes, el estado general del arte y experiencias anteriores. Mediante benchmarking y análisis teóricos se han validado algunas herramientas y se han desechado otras. Se ha generando un protocolo de actuación para profesionales de los equipos policiales que intervengan en la recolección de evidencia digital, para lo cual se ha tomado como punto de partida la experiencia de la provincia de Neuquén [3] y [4].
Hasta el año 2012, dos instituciones eran consideradas referencias ineludibles para el análisis forense, el National Institute of Standart and Technology [5] (NIST), y el Federal Bureau of Investigation [6] (FBI). Actualmente, la referencia es la norma de alcance global ISO/IEC 27037:2012. Bajo esta norma está realizado todo nuestro trabajo.
La citada norma proporciona pautas para el manejo de la evidencia digital; sistematizando la identificación, recolección, adquisición y preservación de la misma. Estos procesos deben diseñarse para mantener la integridad de la evidencia y con una metodología aceptable para contribuir a su admisibilidad en procesos legales. De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital. Esta norma internacional también proporciona directrices generales para la obtención de pruebas no digitales que pueden ser útiles en la etapa de análisis de la evidencia digital. La norma pretende orientar a aquellos responsables de la identificación, recolección, adquisición y preservación de potencial evidencia digital. Estos individuos incluyen: Digital Evidence First Responder (DEFRs) o especialista en evidencia digital de primera intervención, Digital Evidence Specialist (DESs) o especialista en evidencia digital, especialistas en respuestas a incidentes y directores de laboratorios forenses. De esta manera se asegura que las personas responsables de gestionar potencial evidencia digital lo hagan con prácticas aceptadas en todo el mundo, con el objetivo de realizar la investigación de una manera sistemática e imparcial, preservando su integridad y autenticidad. La norma también está destinada a aquellas personas que necesitan determinar la confiabilidad de la evidencia digital que se les presenta. Es aplicable a las organizaciones que necesitan formalmente establecer un marco de aceptabilidad. La evidencia digital a la que hace referencia puede obtenerse de diferentes tipos de dispositivos digitales, redes, bases de datos, etc. Se refiere a datos que ya están en formato digital y no abarca la conversión de datos analógicos a formato digital. La rigurosidad de la aplicación de una metodología adecuada se debe a la fragilidad de la evidencia digital. Como la norma no impone el

uso de herramientas o métodos particulares nosotros hemos utilizado exclusivamente software libre. Es importante destacar la pertinencia, importancia y ventajas que implicaría el hecho de trabajar con software libre en el ámbito de la informática forense de la justicia de la provincia de Santa Fe. La más relevante de ellas y tal vez la menos conocida es el principio de Kerckhoffs [7]; la efectividad del sistema no debe depender de que su diseño permanezca en secreto. El código fuente abierto permite auditar los programas impidiendo puertas traseras y disminuye el tiempo de reacción ante bugs. El diseñador se siente naturalmente obligado a programar de manera "académica y elegante" y una ventaja no menor es que gran parte de las aplicaciones GNU disponibles son gratis.

La norma ISO/IEC 27037:2012 no aborda los procedimientos legales, procedimientos disciplinarios y otras acciones relacionadas con el inadecuado manejo de la evidencia digital. La aplicación de esta norma internacional exige el cumplimiento de las leyes, normas y reglamentos nacionales. No sustituye los requisitos legales específicos de cualquier jurisdicción. En cambio, puede servir como una guía práctica para cualquier DEFR o DES en la investigación. La norma no hace ninguna referencia a requisitos específicos de cada jurisdicción que se refieren a cuestiones como la admisibilidad, la ponderación probatoria, la pertinencia y otras limitaciones que controlan el uso de la evidencia digital en los tribunales de justicia. Sin embargo puede ayudar al intercambio de evidencia digital entre jurisdicciones. Los usuarios de esta norma deben adaptar y modificar los procedimientos descriptos en esta norma internacional de conformidad con los requisitos legales de cada jurisdicción.

Es de suma importancia el concepto de Cadena de Custodia (CoC) estableciendo los recaudos mínimos a tener en cuenta:

- Un identificador univoco de la evidencia.
- Quién, cuándo y dónde se accede a la evidencia.
- El pasaje de la evidencia de un sitio a otro y tareas realizadas.
- Todo cambio potencial en la evidencia digital debe registrarse con el nombre del responsable y la justificación de las acciones realizadas.

2 Alcance del trabajo

Nuestro trabajo se enmarca en dos proyectos radicados en diferentes unidades académicas: Análisis Digital Forense, Conceptos y aplicaciones (proyecto acreditado en la Facultad de Ingeniería de la Universidad Nacional de Rosario) e Informática Forense con herramientas de software libre (proyecto acreditado en la Facultad de Tecnología Informática de la Universidad Abierta Interamericana). La diversidad del equipo de trabajo compuesto por especialistas en derecho, software y hardware genera un enfoque colaborativo, produce una visión multidisciplinaria de la problemática y no solo comprende actividades de investigación, sino que ha tenido impacto en docencia de grado y extensión. En la asignatura electiva Arquitectura y Diseño de Computadoras de ingeniería electrónica de la Universidad Nacional de Rosario ya se han incorporado retos forenses como problemas de ingeniería para comenzar proyectos de fin de carrera en el año 2012. En la asignatura Sistemas de Hardware de ingeniería en sistemas informáticos de la Universidad Abierta Interamericana se ha

presentado la problemática del diseño de un laboratorio de informática forense. En la asignatura Seguridad Informática de la Universidad Abierta Interamericana es donde mayor impacto se espera. En 2014 y 2015 hemos compartido nuestro trabajo de investigación con dependencias públicas de la provincia de Santa Fe. Colaborando y poniendo a disposición el know how del grupo académico de investigación en el diseño y desarrollo de las políticas de seguridad informática para la Dirección de Inteligencia Criminal Estratégica de la Dirección General de Policía de Investigaciones de Santa Fe. Está prevista la realización de convenios entre las universidades y la provincia de Santa Fe a fin de capacitar personal policial y del poder judicial.

3 Un Caso Real

Para reafirmar la necesidad de formalizar la aplicación de las ISO/IEC 27037:2012 como parte del procedimiento estándar para la provincia de Santa Fe, se presentan a continuación algunas circunstancias generadas en un allanamiento efectuado durante el mes de Julio del corriente año, en la mencionada provincia, sirviendo el mismo de ejemplo práctico: para el procedimiento de intervención en el lugar del hecho se hizo indispensable la presencia de personal policial especializado y de empleados judiciales permeables a la realidad que rodea los delitos actuales donde intervienen "herramientas" tecnológicas, en un porcentaje cada vez mayor, tanto de software como hardware, indistintamente. Es dable destacar que de cada investigación surgen diferentes particularidades. En esta oportunidad nos concentramos en una intervención originada en un informe proveniente de NCMEC[8] de carácter prioritario, por reincidencia, referente a material de pornografía infantil. La lógica de estas investigaciones hace fundamental el registro de los domicilios de los eventuales imputados para asegurar la evidencia digital y consecuentemente realizar el correspondiente informe forense. Este tipo de abordaje requiere particular atención por parte de los especialistas, tanto en la preservación del entorno inmediatamente después del acceso al lugar, como durante la requisa, haciéndose sumamente valiosa la presencia de un perito fotógrafo que realice las primeras vistas fotográficas y efectúe una minuciosa filmación de los detalles que puedan resultar de utilidad durante el análisis forense posterior. En este caso, se realizó la filmación correspondiente, luego ingresó el Jefe policial a cargo de procedimiento acompañado por el Especialista de Evidencia Digital de Primera Intervención (quién contó con ayuda de dos especialistas que trabajaron en el registro y documentación de los elementos recolectados). Debido a que se hallaron numerosos documentos con inscripciones varias, el aporte de los especialistas en informática forense se hicieron indispensables, pudiendo detectar contraseñas de encriptación, códigos y procedimientos minuciosamente documentados en cuadernos, hojas sueltas, revistas, posters y otros trozos de papel almacenados en grandes cantidades en la habitación del imputado. Sólo con esta pequeña reseña queda completamente comprobado que acceder al lugar del suceso siguiendo lo aconsejado por normas y estándares representa asegurar el éxito de la investigación. En este caso en particular, gracias a los conocimientos de los Especialistas se logró individualizar material de importancia

trascendental para iniciar nuevas investigaciones originadas en la intervención realizada en esa fecha. Determinase que es conveniente aplicar los amplios conocimientos del Especialista desde el primer acceso a la evidencia y que indefectiblemente podrá hallar información válida en cualquier lugar, en cualquier tipo de soporte y su participación es de carácter prioritario.

4 Conclusiones y líneas futuras

Nuestro resultado más importante ha sido el desarrollo con la empresa local Digilogic Ingeniería [9] de un prototipo de bloqueador de escritura por hardware SATA para la adquisición de evidencia digital de discos rígidos sin contaminar la evidencia. Este hardware es inédito en Argentina y está diseñado con tecnología de lógica programable (FPGAs).
Se han implementado dos cursos en concordancia con la ISO/IEC 27037:2012: Evidence First Responder (DEFRs) o *especialista en evidencia digital de primera intervención*, y Digital Evidence Specialist (DESs) o *especialista en evidencia digital*. Nuestro objetivo es extender estos cursos con personal policial y del poder judicial.
Luego de un muy extenso benchmarking se ha elegido la distribución Deft Linux como nuestra herramienta preferida por su facilidad de instalación, la cantidad y calidad de herramientas que incluye y su actualización permanente [10]. Para la extracción de evidencia de teléfonos móviles se escogió la distribución Santoku Linux [11].
A medida que se van obteniendo resultados, obviamente se generan nuevas preguntas e ideas. La línea de trabajo que asoma como más prometedora y en la que estamos trabajando actualmente es el análisis forense de teléfonos chinos shanzhai [12], teléfonos piratas que no se pueden acceder con las herramientas comerciales más conocidas como XRY[13] y UFED CHINEX[14]

Referencias

1. Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012
2.- "Ley Provincial 13139-2010". Boletín Oficial de la Provincia de Santa Fe del martes 23 de noviembre de 2010.
3.- L. S. Gómez "Protocolo de Actuación para Pericias Informáticas" Poder Judicial de la Provincia de Neuquén.
4.- L. S. Gómez, "Pericias informáticas sobre telefonía celular" Poder Judicial de la Provincia de Neuquén.
5- "Guide to Integrating Forensic Techniques into Incident Response", National Institute of Standards and Technology Special Publication 800-86 Aug 2006
6.-"Recovering and Examining Computer Forensic Evidence", Forensic Science Communications October 2000, Federal Bureau of Investigation

7.- Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883
8.-NCMEC, National Center for Missing and Exploited Children. USA
9.- www.digilogic.com.ar
10.- M. E. Casco; S. Roatta; N. Acosta; C. Kornuta; M. Marinelli "Análisis y Evaluación de Herramientas Libres Aplicadas a la Informática Forense" 40º Jornadas Científico – Tecnológicas UNaM, 2013.
11.- https://santoku-linux.com
12.- Junbin Fang, Zoe Jiang, Kam-Pui Chow, Siu-Ming Yiu, Lucas Hui, Gang Zhou, Mengfei He, Yanbin Tang "Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones" IFIP Advances in Information and Communication Technology Volume 383, 2012, pp 129-142
13.- https://en.wikipedia.org/wiki/XRY_(software)
14.- http://lang.cellebrite.com/es/mobile-forensics/products/standalone/ufed-chinex