La Necesidad de un Proceso Unificado de Recuperación de Información Digital en los Procesos Judiciales

Ing. Ana Haydée Di Iorio

2° CIIDDI - Florianópolis – Brasil -Mayo 2013

UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO

Agenda

- ✓ Introducción.
- ✓ Los delitos Informáticos en Argentina.
- ✓ La Informática Forense en la investigación.
- ✓ Las Pericias Informáticas - Clasificación.
- ✓ La necesidad de un PURI: Proceso Unificado de Recuperación de Información.
- ✓ Algunas deudas de la ciencia forense.
- ✓ Los nuevos desafíos.
- ✓ Reflexiones.

Introducción

De la Era Industrial a la Era de la Información

De la tierra como capital al conocimiento como capital.

La información, el conocimiento y la creatividad son la materia prima de la nueva "economía".

De la producción en serie a los servicios personalizados.

De los átomos a los bits

De los delitos tradicionales a los delitos de cuello blanco.

Los delitos informáticos en Argentina

Ley 26.388 Sancionada en Junio 2008

Consta de 15 artículos. *No es una ley especial* que regula este tipo de delitos con figuras propias y específicas, sino una ley que *modifica*, *sustituye e incorpora figuras típicas* a diversos artículos del Código Penal actualmente en vigencia.

En la ley **NO** hay una definición de Delitos Informáticos.

"Hechos ilícitos cometidos usando un equipo informático como medio o como fin"

La Informática Forense en la Investigación

UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO

Informática Forense

El **uso de IT** para **detectar** o evidenciar **actividad criminal**.

La informática forense es la ciencia de **adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio Computacional** (FBI)

La Ciencia de **obtener información** que pueda ser utilizada como **evidencia**.

Evidencia Digital: Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.
Principio de Intercambio de Locard: *"siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".*

Algunos datos del Depto. Judicial Mar del Plata

Año	Investigaciones remitidas
2008	21
2009	37
2010	110
2011	86
2012	72

Depto Judicial Mar del Plata – Prov. Buenos Aires
Hitos:
- 2008: Sanción de la ley 26,388
- 2011: Investigaciones en Dispositivos Móviles pasan a otro ámbito.

Fuente SIMP: Sistema Informático Ministerio Público.

Algunos datos del Depto. Judicial Mar del Plata

Delito	Investigaciones remitidas
Robo y Robo agravado	56
Hurto	43
Estafa	39
Amenazas	36
Lesiones Leves	35
Defraudación	22
Daño	20
Infracción Ley nº 11.723 - PI	17
Homicidio	5

Fuente SIMP: Sistema Informático Ministerio Público.

La Informática Forense como ayuda a la Investigación

¿ Informes Técnicos vs. Actuaciones Periciales ?

La Prueba Pericial: " Es el medio probatorio con el cual se intenta obtener para el proceso, un dictamen, fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba. "

"Se podrán ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinentes a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, técnica o arte." (art 244 C.P.P. Bs. As.)

Informática Forense

¿Quiénes pueden ser Peritos según el CPP Prov. Bs. As.?

"Si la profesión estuviese reglamentada, el perito deberá tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba expedirse. En caso contrario, o cuando no hubiera en el lugar del proceso, perito con título habilitante, podrá ser nombrada cualquier persona con conocimientos en la materia."
(art. 244 C.P.P. de la Prov. Bs. As.)

Informática Forense

¿Quienes pueden ser peritos según el CPCIBA - Consejo Profesional ?

Ley 13016 – promulgada el 13/01/2003. Define incumbencias en el art.7

En el año 2007 el consejo define en su artículo 2 el conjunto de actividades del art 7 que están autorizadas a realizar las matrículas de profesional y auxiliar informático:

13. Realizar arbitrajes, pericias y tasaciones relacionados con los Sistemas Informáticos y todo el equipamiento para el Procesamiento de Datos. Dictaminar e informar a las Administraciones e Intervenciones Judiciales como perito en su materia, en todos los fueros.

Tareas de Informática Forense

Objetivo de la Informática Forense: Encontrar Evidencia Digital !!

- Tareas Forenses sobre Equipos de Computación.
- Tareas Forenses sobre Dispositivos Móviles.
- Tareas Forenses sobre Redes de Comunicaciones.
- Tareas Forenses sobre Entornos Distribuidos.
- Tareas Forenses sobre Dispositivos Inteligentes. (Ej: Smart TV)

y más...

Reflexiones y Puntos de Partida

¿Se encuentran entrenados los funcionarios judiciales para hacer frente a estas nuevas modalidades delictivas? ¿Y para guíar la pericia?

¿Cómo probar que los procedmientos efectuados por los peritos son los adecuados?

¿Como saber si el tratamiento de la evidencia fue el adecuado?

¿El conocimiento y habilidades del perito son los esperados?

¿Están adecuados los códigos de procedmiento para la evidencia digital?

Proceso Unificado de Recuperación de la Información - PURI

UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO

Guías de Procedimientos de Informática Forense

Guías de Procedimiento:

- ACPO (Association of Chief Police Officers) – England, Wales and North Ireland. Good Practice Guide for Computer-Based Electronic Evidence. Oficial release version.
- NIJ (National Institute of Justice) Report – United States of America, Department of Justice. Forensic Examination of Digital Evidence: A guide for Law Enforcement.
- Law Enforcement Investigations - Active Army, Army National Guard, and US Army Reserve. FM 3-19.13. Chapter 11: Computer Crimes.
- Metodologías, Estrategias y Herramientas de la Informática Forense aplicables para la dirección nacional de comunicación y criminalistica de la policia Nacional de Ecuador.
- RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) [14], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.
- Guía de la IOCE (International Organization on Computer Evidence) "Guía para las mejores practicas en el examen forense de tecnología digital" (Guidelines for the best practices in the forensic examination of digital technology)
- Guía de Mejores prácticas de la ISFS (Sociedad de Seguridad Informatica y Forense) Hong Kong
- Guía Para El Manejo De Evidencia En IT - Estándares de Australia. APEC Telecommunications and Information Working Group.

La necesidad de un Proceso Unificado de Recuperación de la Información Digital

Objetivo: "Construcción de un proceso unificado que sirva de base en la tarea del Informático Forense en la recuperación de la información almacenada digitalmente en un equipo de computación."

Consiste en el estudio de las técnicas y herramientas disponibles en el mercado con el fin de generar un proceso unificado para recuperar información, y presentar propuestas de desarrollo de nuevas técnicas y herramientas en los nichos carentes.

Ante el panorama de la diversidad de soluciones existentes, se hace evidente la necesidad de un proceso formal unificado que valide la labor del profesional informático, que contemple la multiplicidad de dificultades y que permita tener una guía orientadora ante cada problemática.

Extracto de PURI

Proceso Unificado Propuesto

4 Fases: Adquisición, Preparación, Análisis y Presentación.

a) Fase de Adquisición: Comprende todas las actividades vinculadas con la generación de una réplica exacta del contenido digital alojado en los equipos.

b) Fase de Preparación: Involucra todas las tareas necesarias para generar el entorno de trabajo preciso para llevar a cabo la recuperación de la información.

Extracto de PURI

c) Fase de Análisis: Es el núcleo del proceso, donde se analiza el contenido adquirido en busca de vestigios de lo que se se quiere hallar.

- Extracción lógica
- Extracción física
- Análisis de relaciones

d) Fase de Presentación: En esta fase el informático forense debe documentar en una secuencia ordenada, y utilizando un método científico la lista de tareas realizadas, a fin de que el trabajo realizado tenga trazabilidad, y pueda ser reconstruido llegando a los mismos resultados.

Ejemplo de PURI Ampliado

Fase	Etapa	Tareas	Técnicas	Herramientas
1.Adquisición	1.1. Adquisición de medio de almacenamiento persistente	1.1.1. Bloqueo del medio de almacenamiento	1.1.1.1. Bloqueo por hardware	bridge
			1.1.1.2. Bloqueo por software	Windows: Modificación del registro bloqueando para escritura el puerto al que está conectado el disco. Linux: Montar el disco alterando la configuración bloqueando para escritura, o en solo lectura.
		1.1.2. Captura y resguardo de la imágen	1.1.2.1. Copia bit a bit del medio de almacenamiento	Comando dd de fau (forensic adquisition utilities)
		1.1.2 Opcional: compresión y división de la imágen	1.1.2.1 gzip y bz2	Opción 1: dentro del comando dd de fau Opción 2: comandos independientes
		1.1.3. Validación de original y copia	Generación valor hash sobre original y copia. Validación de resultados. Se recomienda: SHA1 (RFC 3174-2001), SHA2. (RFC 6668-2012) o MD5 (RFC1321-1992). Se recomienda documentar estos valores obtenidos y presentarlo en el informe final.	Opción 1: dentro del comando dd de fau. Opción 2: comandos independientes

Reflexiones y Desafios

UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO

Los desafíos actuales

- Validación de PURI para Smartphones. Proyecto actualmente en desarrollo por la UNIANDES de Ecuador.

- De la Computación Forense a la Forensia en Entornos Distribuidos.

- Generación de un Framework para recuperación de archivos mediante técnicas de Carving. Proyecto CIRA (Weinmann, Bruno)

- Forensia sobre datos alojados en memoria virtual. (Alberdi)

- Recuperación de información de Perfil. Proyecto PRIP (Carroza, Garros)

Reflexiones

- ✓ Las Nuevas Tecnologías llegaron para quedarse, y el derecho debe repensarse en función a esto.
- ✓ Las tareas de ayuda a la investigación no necesariamente tienen que ver con los denominados "delitos informáticos", sino con la recolección de "evidencia digital".
- ✓ Los operadores de justicia necesitan un marco que les permita conocer si la metodología utilizada para la obtención de la evidencia digital fue la adecuada.
- ✓ Las tareas de informática forense en general, y las pericias informáticas en particular, requieren de profesionales con conocimientos certificados, y actualizados permanentemente en nuevas técnicas y herramientas.

Reflexiones

- ✓ Es necesario un gran esfuerzo de investigación para abordar estas problemáticas con fuerte compromiso institucional.
- ✓ Es necesario incrementar el dialogo y trabajo conjunto entre profesionales de la informática y del derecho, entendiendo esto como una interdisciplina.
- ✓ La Universidad no puede mantenerse ajena a esta realidad. Tiene una responsabilidad social en torno a estas cuestiones.
- ✓ La Sociedad "somos nosotros". Tenemos aquí una invitación a construir una Sociedad mejor, desde la Universidad.

¡ Muchas Gracias !

Ing. Ana Haydée Di Iorio

dana@ufasta.edu.ar