Pericias informáticas para casos de pornografía infantil

Lic. Gerardo Nilles y Lic. Gastón Silva.

Informática Forense. Poder judicial de Río Negro. Laprida 292. Viedma. Rio Negro.
gnilles@jusrionegro.gov.ar, gsilva@jusrionegro.gov.ar

Abstract. La gran cantidad de casos de pornografía infantil denunciados por la NCMEC (National Center for Missing and Exploited Children) dieron lugar a que desde el área de informática forense del poder judicial de Río Negro se investigaran las mejores técnicas y herramientas para dar respuesta a los puntos de pericia solicitados por los juzgados. Este trabajo presenta las técnicas investigadas y la metodología aplicada por el área para la resolución de casos de pornografía infantil denunciados por reporte de la NCMEC.

Keywords: Informática Forense, Pornografía infantil, técnicas de búsqueda, PhotoDNA, procedimiento operativo.

1 Introducción

La explotación sexual infantil no es un delito nuevo, sin embargo se potencia con el ingreso irrestricto a las redes sociales. Muchos delincuentes escondidos detrás de nombres falsos en sus perfiles de Internet piensan que no podrán ser detectados, pero a través de los rastros que dejan online pueden ser descubiertos.

Cerca de 750 mil pedófilos de todo el mundo circulan a diario por internet en búsqueda de pornografía infantil. El dato corresponde a un informe reciente de Unicef, según el cual casi el 20% de toda la pornografía que circula por la web tiene como protagonistas a niños y adolescentes. [1]

Los precios elevados hacen que se trate de un negocio por demás rentable. Desde 50 euros por acceder a imágenes que ya llevan tiempo circulando por la red hasta llegar a miles de euros por disponer de un "paquete" con material de pornografía infantil. [2]

Fig. 1. Estadísticas Alarmantes

En 2012, el actual ministro de Justicia de la Nación, Germán Garavano creó el Equipo Especializado en Delitos Informáticos de la Fiscalía de la ciudad de Buenos Aires.

A partir de un convenio firmado en octubre de 2013 entre la Argentina y el National Centre for Missing and Exploited Children (NCMEC), un organismo norteamericano que aborda cuestiones relacionadas con niños desaparecidos y explotados sexualmente, el ingreso de casos de pornografía infantil en el país aumentó significativamente.

Hoy, el 89% de las investigaciones corresponden a pornografía infantil. Hay más de 1800 casos de esta índole, sin contar los reportes que aún se encuentran a la espera del resultado de las primeras medidas encomendadas al Cuerpo Judicial de Investigaciones.

El NCMEC tiene un acuerdo con todas las redes sociales, que deben notificarle cuando se encuentran ante una foto que tiene contenido pornográfico relacionado con menores o cuando se detecta en algún chat una conversación relacionada con el mismo tema. Si la red social no da aviso, las multas alcanzan a los 150.000 dólares.

Cuando la Homeland Security o el FBI detectan una IP (dirección de Internet) ubicada en el país con relación a un delito de explotación infantil, envían un reporte a la fiscalía para que puedan investigar. La fiscalía trabaja juntamente con las distintas áreas de cibercrimen de las policías Metropolitana y Federal y del Cuerpo Judicial de Investigaciones.

Con el dato de una cuenta de correo o de una dirección IP correspondiente a la Argentina comienzan una investigación. En el 80% de los casos trabajan con la fiscalía de la ciudad de Buenos Aires. [3]

En el caso de la provincia de Río Negro, el reporte es recibido por la Procuración General, que solicita actuaciones al juzgado. Cuando el juzgado interviniente dispone allanamientos, el material informático secuestrado es remitido al área de informática forense del poder judicial de Rio Negro. Durante el año 2015 el 20% de los casos ingresados al área de informática forense corresponden a casos de pornografía infantil con reporte de NCMEC.

El material secuestrado es acompañado por el reporte de NCMEC y los puntos de pericia solicitados por el juzgado. Los puntos de pericia representan los distintos ítems sobre los cuales deberá dictaminar el perito y en estos casos generalmente consisten en detectar, en los elementos secuestrados, copias de las imágenes reportadas por el NCMEC y cualquier otro tipo de material relacionado con la pornografía infantil.

El área de informática forense sigue una metodología de trabajo para el manejo de la evidencia digital que consta de cuatro etapas: Identificación, Preservación, Análisis y Presentación.

En todas las etapas se trabaja siguiendo procedimientos operativos estandarizados con un control de calidad previo realizado en el laboratorio pericial. Este control de calidad incluye testeo y pruebas de concepto de las técnicas y herramientas.

En la etapa de análisis, utilizando técnicas y herramientas forenses, se intenta dar respuesta a los puntos de pericia solicitados por el juzgado.

2 Evolución de las técnicas utilizadas:

2.1 Técnica de búsqueda en vivo

Una búsqueda en vivo es un proceso que implica una comparación elemento por elemento con el objeto de búsqueda y por lo tanto consume mucho tiempo.

Una vez procesada la totalidad de la evidencia con algún software forense se compara cada uno de los elementos obtenidos por el software con los objetos de la búsqueda.

Esta técnica tiene la ventaja de ser muy simple pero como desventaja es extremadamente lenta y propensa a errores.

2.2 Aplicación de filtros de imágenes

El filtrado permite seleccionar un subconjunto de los elementos analizados aplicando algún criterio.

Una forma de acotar el tiempo de la búsqueda en vivo es filtrar los elementos obtenidos. Utilizando software forense, se puede optar por exportar solo los archivos de imagen de manera de realizar las búsquedas sobre este subconjunto de la evidencia.

Esta técnica es un poco más rápida que la anterior, ya que descarta todos aquellos archivos que no deben analizarse, pero sigue siendo una técnica de búsqueda exhaustiva propensa a errores.

2.3 Filtro utilizando metadatos

Los metadatos son datos sobre los datos. Por ejemplo los datos EXIF contienen información de cómo se ha tomado una fotografía, incluyendo la cámara (marca, modelo, etc).

Utilizando los metadatos de las imágenes buscadas pueden refinarse los filtros. De esta manera, conociendo el tamaño, fecha de modificación o datos EXIF de las imágenes buscadas, puede configurarse el software forense para filtrar aquellas imágenes que coincidan en estos valores con las imágenes buscadas.

2.4 Filtrado por tono de piel

Algunas herramientas forenses incorporan entre sus funciones un analizador del tono de piel. Estas herramientas tienen la capacidad de identificar rápidamente y con eficacia los archivos de interés basado en el porcentaje del tono de piel contenido en el mismo, para esto utilizan la tecnología de análisis de imágenes basado en píxeles. Un píxel es la menor unidad homogénea en color que forma parte de una imagen digital.

Una vez realizado este análisis se genera una galería organizada por el contenido de tono de la piel. Esto permite acelerar en gran medida la búsqueda de rastros de pornografía infantil. Utilizando estas herramientas se puede reducir el número de archivos de imagen que un investigador debe ver.

Este tipo de herramientas fueron diseñadas para cubrir la brecha tecnológica que los depredadores/abusadores sexuales han explotado durante años, y que es la falta de una forma rápida y precisa de identificar las imágenes de valor probatorio en medio de un gran volumen de datos.

La utilización de esta tecnología permite a los investigadores un acceso inmediato a los datos, permitiendo la posibilidad de priorizar los resultados. Una vez que el software a localizado imágenes de interés, el investigador puede revisar los resultados y tomar la decisión en cuanto a que archivos me-

recen mayor investigación, cuales apoyan una suposición de presencia de material de pornografía infantil o incluso dar con el o los archivos buscados. [4]

La ventaja de esta técnica es la automatización de parte del reconocimiento de imágenes.

2.5 Técnica de búsqueda utilizando los hash de los archivos

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (un archivo, por ejemplo) una salida alfanumérica de longitud fija que representa un resumen de toda la información que se le ha dado, es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos.

Fig. 2. Ejemplo de función hash sobre un archivo de imagen
Valor de hash: bf36959f2619d4a790a644f9c5b256d4

- **Identificación y eliminación de archivos conocidos**

La utilización de esta técnica permite eliminar archivos que no son relevantes para la investigación, tales como archivos conocidos de aplicaciones y de Sistemas operativos. El analista puede recurrir a Bases de datos de hashes validados tales como los creados por el NSRL (National Software Reference Library) o bases de datos propias generadas a partir de la creación de una lista de hashes criptográficos a partir de aplicaciones y sistemas operativos verificados.

A medida que se van procesando las evidencias se van generando los hashes de los archivos recuperados y se comparan con los hashes contenidos en las bases de datos de archivos conocidos. Aquellos con resultado positivo son excluidos de los archivos a analizar permitiendo a los investigadores reducir el espacio de búsqueda.

- **Búsqueda automática de pornografía infantil mediante el uso de hashes criptográficos**

La eliminación de archivos conocidos reduce en forma drástica el campo de búsqueda, aunque el constante crecimiento en las capacidades de almace-

namiento y uso diario de los dispositivos tecnológicos genera grandes volúmenes de archivos de imágenes que no son eliminados mediante la utilización de esta técnica. Como consecuencia, en el laboratorio de informática forense del poder judicial de Río Negro, se procedió a la búsqueda de técnicas de reconocimiento automatizado basada en los valores criptográficos de las imágenes. Se utilizaron las bases de datos de valores hash de archivos reconocidos de pornografía infantil obtenida de organismos internacionales de protección de la niñez y mediante la utilización de herramientas forenses se compararon los hashes de los archivos de la causa contra la base de datos. No se obtuvieron resultados significativos mediante el uso de esta técnica debido a que una mínima modificación en el archivo cambia totalmente el valor criptográfico del mismo.

Claramente, la ventaja de esta técnica es la reducción de los tiempos de búsqueda. Otra ventaja es la posibilidad de contar con bases de datos consistentes y verificadas por distintos organismos.

La principal desventaja es que pequeñas modificaciones en un archivo (un bit) generan valores de hash distintos. Esta técnica deja de ser útil si la imagen buscada sufrió alguna modificación en forma o tamaño. [6]

Fig. 3. Valor de hash sobre la imagen reducida en un 1% en tamaño.
Valor de hash: b38aea1a250f35ff9aefd3cb3b10d715

2.6 Huellas digitales de datos

Hasta ahora, se han considerado búsquedas de una copia exacta de un objeto de referencia; un problema mucho más difícil es encontrar objetos similares.

Los hashes son frágiles por diseño, incluso si un solo bit en un archivo cambia, el valor calculado de hash será completamente diferente. Si insertamos un solo carácter en un archivo todo el hash del bloque siguiente al cambio también cambiará.

Así, el hash basado en bloques hará poco para abordar el problema de la fragilidad.

En su lugar, es necesario un mecanismo más inteligente llamado huellas digitales de datos, que puede generar una firma de los datos que es más resistente a las modificaciones.

El término "huella digital" significa cosas diferentes en diferentes ámbitos. En este trabajo se considerará una forma más relajada de la toma de huellas digitales que no pretende ser infalsificable. La idea esencial ha existido durante décadas y es bastante genérica y simple.

Para cada objeto se seleccionan rasgos característicos para compararlos con las características seleccionadas de otros objetos, utilizando alguna medida de correlación para sacar conclusiones.

Este enfoque podría ser aplicado en diferentes niveles de abstracción, aquí se considerarán a los objetos de datos como cadenas de bytes donde el objetivo es encontrar sus similitudes. [6]

La investigación sobre huellas digitales de datos de Michael Rabin data de 1981 y su propósito original fue producir un algoritmo simple de comparación de cadenas y un procedimiento para resguardar los archivos de cambios no autorizados.

2.7 PhotoDNA, el estándar creado por Microsoft

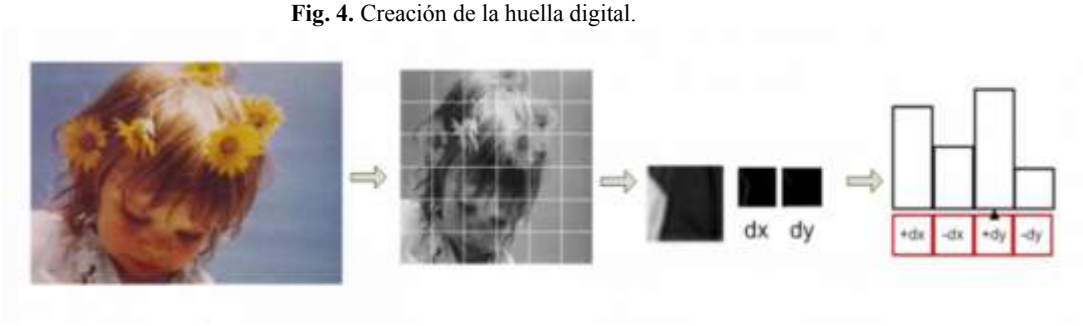
PhotoDNA es una tecnología innovadora, desarrollada por Microsoft, que compila las firmas digitales de imágenes para ser comparadas con una base de datos con las huellas digitales de archivos categorizados como pornografía infantil, reduciendo significativamente el tiempo que los investigadores pasan realizando búsquedas de este tipo de material.

La tecnología PhotoDNA fue donada en 2009 al propio NCMEC para que cualquier compañía tecnológica pueda usarla de forma totalmente gratuita. Ellos también la aplican en todos sus productos. De hecho, Twitter y Facebook reconocen utilizarla en sus servicios. Lo más seguro es que otros miembros de la Coalición Tecnológica, como Yahoo, AOL o Time Warner Cable implementen también PhotoDNA o algún otro procedimiento similar en sus servicios de correo y alojamiento web.

¿Cómo funciona PhotoDNA? Una imagen en Internet puede transformarse de manera sencilla: o se cambia la extensión, o el tamaño o incluso se modifican ligeramente los colores. PhotoDNA es capaz de reconocer todos estos pequeños cambios en una misma imagen manteniendo el mismo identificador. El proceso que sigue esta tecnología es el siguiente:

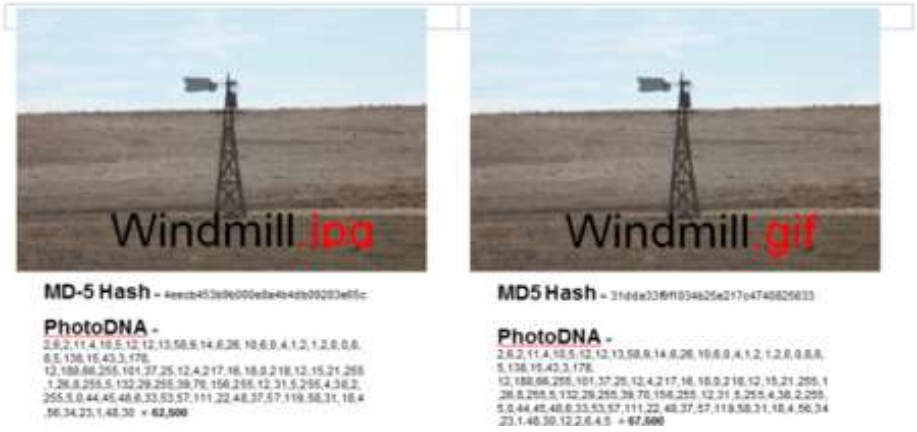
1) Obtienen cada imagen a analizar y la convierten a escala de grises, modificando también el tamaño hasta que encaje con el tamaño por defecto establecido por ellos.
2) Dividen esta imagen (ya con tamaño modificado y en escala de grises) en cuadrados más pequeños.
3) Para cada cuadrado calculan distintos parámetros, como la variación del tono de negro de cada pixel.
4) Con dichos valores se crea un histograma.
5) Estos valores numéricos, finalmente, se convierten en la firma única o hash que se asigna a cada imagen.

Fig. 4. Creación de la huella digital.



A partir de uno de estos hashes no se puede reconstruir la imagen. Ni siquiera se puede decir qué sale en ella o cómo es la fotografía. Simplemente sirven para hacer de "huella digital " o identificación única de una fotografía. Si dos hashes son muy parecidos puede detectarse que la imagen es casi la misma, salvo con breves modificaciones. Microsoft nos da un ejemplo de dos imágenes distintas (cada una tiene distinto formato) pero con un PhotoDNA casi igual, con lo que aparecería como positivo. [7]

Fig. 5. Dos imágenes casi iguales con una firma PhotoDNA similar: se detectarían como si fuese la misma



3 Procedimiento:

En función del estudio y pruebas realizadas de las diferentes técnicas, sus ventajas, desventajas y observación de los resultados, en el Área de informática forense del poder judicial de Rio Negro se elaboró un procedimiento operativo estandarizado con el objetivo de otorgarle el marco formal adecuado que permite ofrecer rigurosidad y control de calidad en la integración de métodos y técnicas para la búsqueda de material de pornografía infantil en casos con reportes de NCMEC.

SOP. Análisis de evidencia digital en casos de pornografía infantil

Propósito:

Este procedimiento pertenece a la extracción y recuperación de datos de medios digitales que puedan tener valor probatorio en investigaciones criminales de casos de pornografía infantil.

Alcance:

Este procedimiento se aplica al examen y análisis de una imagen forense.

Equipamiento:

Hardware:

a. Computadora Forense

Software:

a. Software Forense

Limitaciones:

Los resultados dependerán de las capacidades y limitaciones de las herramientas elegidas, como así también la experiencia del perito.

Procedimiento:

Los pasos del procedimiento deben ser documentados con suficiente detalle, de manera que permita a otro forense, competente en la misma área, ser capaz de identificar que se ha hecho y evaluar los resultados independientemente.

1. Recuperación de datos

a. Realizar una restauración de los datos de la evidencia digital.
b. Descartar los archivos conocidos utilizando las bases de datos criptográficas.
c. Exportar todos los archivos de imágenes.

2. Llevar a cabo búsquedas

2.1 Imágenes del caso

a. Calcular la "huella digital" de los archivos buscados y almacenarlos en una base de datos del caso.
b. Realizar una comparación automática de los valores de los hashes de los archivos de la evidencia contra la base de datos del caso.

2.2 Material con contenido pornográfico infantil

2.2.1 Realizar una comparación automática de los valores de los hashes de los archivos de la evidencia contra la base de datos de archivos con contenido Pornográfico Infantil conocido.

2.2.2 Para los archivos no detectados en el paso anterior:

a. Aplicar filtro por tono de piel.

b. Realizar una búsqueda visual en aquellos elementos filtrados por tono de piel.

3. Identificación y análisis.

a. En caso de obtener positivos identificar los mismos dentro de la evidencia digital.

Fin del Procedimiento.

Este procedimiento general se aplica utilizando técnicas y herramientas forenses específicas ya testeadas en el laboratorio.

El área de informática forense, como miembro del proyecto VIC, cuenta con acceso a las bases de datos actualizadas de imágenes categorizadas como pornografía infantil.

El propósito del proyecto VIC es crear un ecosistema colaborativo de datos e información entre las agencias que trabajan en contra de la explotación sexual infantil.

En particular para las búsquedas de las imágenes por similitud, se utiliza la tecnología PhotoDna integrada con el software Griffeye Analyze. Este software, que está liberado para agencias de investigación, permite procesar eficientemente grandes volúmenes de imágenes, permitiendo identificar el material relevante a través de rutinas automatizadas y navegación visual. Cuenta también con filtros de tonos de piel, catalogado como nivel de desnudez. Además permite realizar búsquedas contra bases de datos de firmas digitales.

La utilización de esta herramienta, combinada con el acceso a las bases de datos del proyecto VIC, como así también la posibilidad de crear nuevas bases de datos de hashes, permite realizar pericias de calidad en casos de pornografía infantil.

En caso de hallarse material de interés, no incluido dentro de las bases de datos categorizada, ni dentro del conjunto de archivos denunciados en el reporte, como miembros de proyecto VIC, el área pone a disposición del proyecto esos hashes para que sea evaluada su incorporación al conjunto general de archivos categorizados.

4 Conclusión

Actualmente, la tarea de decidir si las imágenes contienen pornografía infantil es un trabajo manual y tedioso debido a que muchas de las herramientas y técnicas existentes ofrecen resultados inexactos.

Además, la clasificación de imágenes en pornográficas y no pornográficas no siempre es posible. Incluso para los seres humanos puede ser una decisión subjetiva. Después de horas de navegación por imágenes, los investigadores son propensos a perder elementos cruciales porque simplemente se cansan.

A pesar de que la automatización completa en este campo podría no ser posible, la asistencia en la clasificación a través de software es indispensable. En la actualidad todavía hay mucho para mejorar en los algoritmos de detección disponibles para contenidos pornográficos, sin embargo la estandarización del proceso y el uso de tecnologías colaborativas y de vanguardia permiten obtener resultados de calidad en este tipo de investigaciones.

En el área de informática forense del Poder Judicial de Rio Negro, la utilización del procedimiento propuesto, que es producto de la investigación de técnicas, tecnología y metodologías, ha permitido reducir significativamente los tiempos de análisis para casos de pornografía infantil. Este procedimiento forma parte de la librería de procedimientos del área y como tal, está sujeto a revisiones y modificaciones periódicas con el objetivo de mantener su correctitud y eficacia.

5 Referencias:

1. Chicos en riesgo aumentan los casos de pedofilia a través de la web, http://www.lanacion.com.ar/1883303-chicos-en-riesgo-aumentan-los-casos-de-pedofilia-a-traves-de-la-web

2. Detrás de la pornografía infantil mezcla de perversión y negocio, http://www.eldia.com/policiales/detras-de-la-pornografia-infantil-mezcla-de-perversion-y-negocio-69166

3. Delitos sexuales una red judicial y tecnológica contra los pedófilos, http://www.lanacion.com.ar/1807758-delitos-sexuales-una-red-judicial-y-tecnologica-contra-los-pedofilos

4. MacForensicsLab Field Agent, http://www.macforensicslab.com/index.php?main_page=product_info&products_id=277

5. Skin Sheriff: A Machine Learning Solution for Detecting Explicit Images. http://www.syssec-project.eu/m/page-media/3/sfcs14_platzer_skin_sheriff.pdf

6. Hashing and Data Fingerprinting in Digital Forensics, http://roussev.net/pubs/2009-IEEE-SP--hashing.pdf

7. Microsoft PhotoDNA | Project VIC, http://www.projectvic.org/about-microsoft-photodna/