With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Justice, Freedom and Security

Automatización de tareas de análisis forense en delitos de pornografía infantil.

Autores

Alejandro Prieto Castro – INTECO
Juan Prieto Carballal – INTECO
Antonio Sepúlveda Carrero – INTECO

Resumen

El gran reto de las Fuerzas y Cuerpos de Seguridad del Estado en el análisis forense de dispositivos de almacenamiento incautados en delitos de pornografía infantil pasa por la automatización de tareas en la búsqueda de evidencias en archivos electrónicos.

Contenido

Las últimas operaciones contra la pornografía infantil en España, llevadas a cabo por el Cuerpo Nacional de Policía y la Guardia Civil, muestran la gran cantidad de dispositivos de almacenamiento que se incautan en los registros de domicilios de presuntos pederastas. Sin ir más lejos, en la llamada operación Astillas, efectuada por la Guardia Civil, se recopilaron 116 discos duros y 12 DVD además de otros tipos de soporte de almacenamiento que contenían alrededor de 500.000 archivos presuntamente ilegales[i].

En un caso más reciente, los investigadores del Cuerpo Nacional de Policía intervinieron alrededor de 700 discos con cerca de 1000 fotografías de una menor en actitud indecorosa[ii].

La labor forense que realizan las Fuerzas y Cuerpos de Seguridad del Estado sobre los dispositivos de almacenamiento es clave para el éxito de las operaciones contra la pornografía infantil. Las últimas noticias demuestran el excelente trabajo de los agentes analizando ingentes volúmenes de información. Este trabajo es complejo debido principalmente a dos factores. El primero es el elevado número de archivos que tienen que ser analizados. Actualmente la capacidad de los dispositivos de almacenamiento ha crecido exponencialmente, permitiendo almacenar millones de archivos en un *pendrive* o en un disco duro externo. En segundo lugar, es habitual que los criminales utilicen técnicas de ocultación de evidencias que dificulten los trabajos de análisis de los agentes.

Tal es la importancia de estos análisis forenses que normalmente son esenciales para determinar la naturaleza de la imputación del sospechoso. Un imputado, por ejemplo, podría ser acusado de tenencia de imágenes de pornografía infantil, pero también de distribución, al compartir el material delictivo por las llamadas redes de intercambio de archivos p2p. Son dos imputaciones diferentes y reguladas por el código penal. Qué

sea uno u otro delito puede resolverse tras un exhaustivo análisis forense de los dispositivos de almacenamiento incautados.
La eficacia y experiencia demostrada por el Cuerpo Nacional de Policía y la Guardia Civil en la resolución de casos de pornografía infantil hace que cualquiera que esté cometiendo este tipo de delito sea tarde o temprano puesto bajo tutela judicial. Por eso, el objetivo actual es minimizar el tiempo de análisis forense de los dispositivos incautados, aumentando la automatización de tareas en la búsqueda de evidencias.

Cuando un investigador tiene delante de sí un dispositivo intervenido debe considerar todas las casuísticas posibles. Para ello, toma como base tanto aquellos archivos que son visibles por un usuario normal, como aquellos que se encuentran ocultos, por ejemplo: cuando se borra un archivo, todavía puede ser recuperado ya que aún se pueden encontrar alojados físicamente en el dispositivo de almacenamiento. El sistema operativo y las aplicaciones instaladas son también fuentes de información que utiliza el investigador para realizar el análisis forense.

La automatización de tareas bajo los criterios de búsqueda utilizados por los investigadores es un paradigma fundamental en el futuro de los análisis de dispositivos externos. Estos análisis automáticos deben, al menos, mostrar los archivos del dispositivo ordenados por prioridad, donde los primeros serán aquellos con más posibilidades de ser evidencias o dar pistas valiosas para la resolución de un caso. Cabe fuera de toda duda, que la decisión de considerar que una fotografía, video o documento es una evidencia, es una tarea manual realizada por el investigador, más si cabe cuando se tratan de delitos de esta naturaleza.

La traslación de las metodologías utilizadas por los investigadores a procesos automáticos está demostrando ser un elemento imprescindible y a raíz de ello se aumenta más si cabe la eficacia policial contra los delitos informáticos y, en concreto, contra los delitos de pornografía infantil. El automatismo en la búsqueda de evidencias agiliza las tareas de los investigadores a lo largo de la resolución de un caso. La delegación de las tareas manuales a procesos automáticos de búsqueda y catalogación de archivos permite a los agentes centrarse en otras tareas en el curso de la investigación. La realización de esta catalogación de forma manual conllevaría un esfuerzo considerable que a la larga minaría la eficiencia y capacidad resolutiva de una persona, haciendo que se concentre más en el proceso de análisis que en la identificación de evidencias. Siendo automatizable, los agentes tienen finalmente un listado de los archivos de un dispositivo ordenados y catalogados en función de los criterios que se hayan establecido, facilitando la identificación de evidencias.

La ejecución de procesos automáticos tiene una misma naturaleza cuando se habla de análisis forense de dispositivos de almacenamiento. Las diferentes arquitecturas del hardware y del software encontrado en los dispositivos externos son conocidas, así como la forma de afrontarlos. Sin embargo, la particularidad de los criterios de búsqueda en función del delito cometido, es lo que marca la diferencia en el avance de este paradigma. Incluso dentro de los casos de pornografía infantil hay características que a cada uno le hace especial. Esta especificidad puede ser abordada en su totalidad dentro de la modificación o ampliación de los criterios de búsqueda dentro de un análisis forense. Personalizar en este ámbito hace que el ordenamiento y catalogación de archivos sea más efectiva. Los mecanismos y técnicas automatizadas consumen los criterios de búsqueda establecidos por el investigador, siendo de esta forma, dependientes del tipo de delito.

La experiencia del propio grupo investigador y la cooperación policial entre Grupos o entre Estados, es clave en la conformación de criterios de búsqueda específicos para los casos de delitos de pornografía infantil. Decidir qué y en dónde buscar dentro de

un dispositivo de almacenamiento suele provenir de la experiencia. La unión de esa experiencia o conocimientos adquiridos con el potencial que ofrece la automatización en el análisis genérico de dispositivos de almacenamiento, acrecienta la eficacia y eficiencia en la investigación, minimizando el tiempo dedicado para la resolución de un caso.

En la actualidad el gran trabajo de las Fuerzas y Cuerpos de Seguridad del Estado está obteniendo unos resultados fabulosos, y muchas de las personas que guardan, distribuyen o generan contenidos de pornografía infantil son puestos bajo el poder judicial. Gracias a la traslación de metodologías y criterios de búsqueda para que sean consumidos por procesos automáticos, el tiempo transcurrido desde que se obtiene una primera evidencia hasta que se cierra un caso está siendo mucho más corto.

La normalización de las metodologías y protocolos en la investigación y en el posterior registro de casos de pornografía infantil es una ayuda fundamental en el transcurso de los análisis forenses y en la posterior experiencia adquirida que complementen futuros casos. Esta normalización minimiza la dependencia en una persona en concreto, por lo que el cumplimiento de una metodología fija asegura la continuidad efectiva a lo largo del tiempo, manteniendo los niveles de calidad en la resolución de casos. Qué los registros de cada caso tengan una estructura fija debido a la implementación de estas metodologías establece una independencia temporal y de recursos humanos razonable, con todas las ventajas que ello conlleva.

La adaptación de la experiencia humana a los procesos y metodologías así como a los análisis automáticos son y serán motivo de estudio continuo para luchar contra los delitos de pornografía infantil. La gran cantidad de dispositivos confirma esta tesis, asumiéndose que no se debe obviar la implantación de metodologías consistentes en la investigación de casos y la incorporación de procesos automáticos en el análisis forense.

Por eso, uno de los objetivos del proyecto europeo ASASEC (http://asasec.eu/) contra los delitos de pornografía infantil es facilitar la identificación de evidencias en los dispositivos incautados en una operación policial, así como estandarizar metodologías en las investigaciones. ASASEC desarrolla un módulo capaz de analizar grandes volúmenes de datos de dispositivos de almacenamiento dando como resultado un listado priorizado de los archivos encontrados. Esta prioridad indica la probabilidad de que sea una evidencia. También, y debido a su naturaleza, establece una metodología útil y duradera a los agentes para la resolución de casos de pornografía infantil.

El papel de ASASEC como aglutinador de información bajo unos protocolos predefinidos además de favorecer el análisis forense incluyendo procesos automáticos, hace de él una herramienta fundamental en la lucha contra la pornografía infantil.

Conclusiones

Incautar gran cantidad de dispositivos en una operación contra la pornografía infantil hace necesario centrar los esfuerzos en minimizar el tiempo de análisis forense de estos dispositivos. Es factible identificar los criterios que utilizan los investigadores para buscar evidencias y automatizarlos. De esta forma se minimiza el tiempo de búsqueda y la labor del agente se centra en decidir si un archivo es una evidencia o no. Para ello, el investigador trabaja con una lista ordenada por prioridad con todos los datos necesarios para determinar la ilegalidad de un contenido.

Nada como el ojo humano es capaz de identificar archivos con contenido de pornografía infantil, pero aquellos procesos reiterativos y definidos por patrones, como es la catalogación y búsqueda de archivos, son automatizables. Descargar al agente humano de esta última tarea tiene evidentes ventajas en la resolución de este tipo de casos.

Uno de los propósitos del Proyecto Europeo ASASEC es éste. Otro elemento importante de esta solución software es la capacidad de establecer una metodología de trabajo y almacenamiento que ponga en valor la información obtenida durante la investigación de un caso de pornografía infantil.

---

[i] Operación Guardia Civil: http://www.europapress.es/catalunya/noticia-detenidas-27-personas-pornografia-infantil-16-provincias-20121015123618.html.

[ii] Operación Cuerpo Nacional de Policía: http://www.abc.es/20121031/espana/abci-detenido-abuso-sexual-menor-201210311102.html.