FOMO: Una plataforma de Análisis Forense de Dispositivos Móviles

Ana H. Di Iorio[1], Fernando Greco[2], Ariel Podestá[2], Emanuel Gaspar[2], Bruno Constanzo[1], Julián Waimann[1], Sebastián Lasia[2] *Investigadores InFo-Lab, Universidad FASTA - Argentina, {diana, bconstanzo, julianw}@ufasta.edu.ar[1], {fmartingreco, arielpodesta, emagaspar, seba.lasia}@gmail.com[2]*

***Abstract*— In this work we present a Project to develop and implement an integrated environment for the forensic analysis of mobile devices. The novel design proposed by this development enables potential improvements in the process of forensic analysis and investigative activities.**

Palabras Claves— informática forense, dispositivos móviles

I. INTRODUCCION

HACIA fines de la década pasada el progreso tecnológico resultó en la aparición de los smartphones, teléfonos celulares de altas prestaciones, más similares a una computadora que a un teléfono celular clásico. Restringidos en tamaño, capacidad de cálculo, batería y prestaciones en general, los smartphones tuvieron que utilizar sistemas operativos distintos de aquellos que se utilizaban en las computadoras de escritorio o notebooks.

Cada uno de los sistemas operativos móviles desarrollados expone una determinada interfaz a los programadores (una API) y servicios asociados con las distintas partes del equipo[1]. La evolución tecnológica fue incrementando las capacidades de los teléfonos, y se fueron introduciendo mejoras tanto a los equipos como a los sistemas operativos y las interfaces. Sin embargo, la herencia tecnológica hace que aún se mantengan marcadas diferencias con respecto a los sistemas operativos de computadoras clásicas y, por lo tanto, diferencias en las formas a las que se puede acceder a la información de un dispositivo móvil.

Con la incorporación de la tecnología en prácticamente todos los aspectos de la vida cotidiana, es cada vez más necesario poder recuperar información de los dispositivos móviles que pueda ser considerada evidencia digital. Sin embargo el análisis de dispositivos móviles es aún un tema complejo, lleno de mitos, verdades a medias, desconocimiento y muchos desafíos. En este panorama, surgieron algunas empresas que, apoyadas en conocimientos que adquirieron históricamente por otras tareas técnicas que realizaban para las empresas de telefonía, comenzaron a desarrollar suites de análisis forense para dispositivos móviles. Aún hoy prácticamente no existen soluciones de código abierto para realizar estas tareas periciales[2], por lo que el forense está obligado a aceptar las condiciones que imponen las empresas que han desarrollado estos productos.

Formalmente se define a la Informática Forense como la rama de las ciencias forenses que trabaja sobre datos que han sido procesados electrónicamente y se almacenan en un medio computacional. La forensia en dispositivos móviles es la parte específica de la Informática Forense que trabaja con los llamados "dispositivos móviles", es decir, smarphones, tablets, GPS's, entre otros. Si bien no hay una clasificación definida, usualmente se considera como dispositivo móvil a aquellos dispositivos que utilizan como sistema operativo Android, iOS, BlackBerry, Windows Phone u otros sistemas operativos similares, ya que si utilizan Windows, Linux o Mac OS, pueden utilizar los métodos y herramientas de la informática forense "clásica". Alguna de las actividades propias de esta subrama son la extracción de información del equipo, obtención de listado de contactos, registros de llamadas entrantes y salientes, reporte de mensajes enviados y recibidos (SMS), redes inalámbricas a las que se conectó, reportes de navegación (acceso a la información georeferenciada), cuentas de usuario, extracción de archivos (audio, imágenes, video, bases de datos, etc) y análisis de aplicaciones específicas, como pueden ser Facebook, WhatsApp, Twitter, Line, entre otras.

Actualmente el software de análisis para dispositivos móviles se concentra en los aspectos técnicos de la tarea de los peritos informáticos y gira alrededor de las capacidades que se van agregando sobre las nuevas ediciones de cada herramienta. En general, todos los entornos de análisis forense en dispositivos móviles proveen las mismas características[3]: todos pueden acceder de una u otra forma a la información almacenada en un teléfono (con una variabilidad en las marcas y modelos dependiendo de los distintos productos), tanto física como lógicamente, y todos proveen capacidades de análisis para la agenda de contactos, listados de llamadas, mensajes de texto y funcionalidades básicas. Para el caso de los *smartphones* se ofrecen funcionalidades más específicas, orientadas a las características que los distinguen de los teléfonos más simples que existían antes: el análisis del historial de navegación, la búsqueda de fotografías, datos de información geográfica y también el análisis de distintas aplicaciones que pueden instalarse en los mismos. Además, dependiendo del sistema operativo en particular que utilice el teléfono, pueden consultarse

logs específicos con información que no estaría accesible de otra forma.

En el Ministerio Público de la Provincia de Buenos Aires, República Argentina, surge la necesidad de complementar las capacidades disponibles por las soluciones comerciales para el análisis de dispositivos móviles modernos, razón por la que se encomienda el desarrollo del proyecto FOMO, Forensia en Equipos Móviles, al InFo-Lab: Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense.

El InFo-Lab es una iniciativa conjunta de la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón[4] que reúne en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores, profesionales y técnicos altamente calificados, con el objeto de desarrollar soluciones a las demandas en el campo de la Informática Forense y su aplicación. Es, a su vez, la sede del Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA. El InFo-Lab en este momento está trabajando sobre tres proyectos:

- INVESTIGA, un proyecto para desarrollar un ambiente integrado para la visualización y análisis de datos.
- PAIF-PURI, un protocolo para de actuación en informática forense.
- FOMO, el proyecto que se presenta en éste trabajo, un sistema informático para el análisis forense de dispositivos móviles.

Actualmente para las tareas de análisis forense sobre dispositivos móviles en el Ministerio Público se trabaja con un esquema de solicitud de pericias al experto en informática forense. Esto impone procesos, tiempos y documentación que debe respetarse, y un ritmo propio del proceso que hace lento el paso de información del equipo analizado a los investigadores judiciales, a través del perito y su tarea. Para presentar la información, es necesario que se redacten puntos de pericia, luego el perito trabaje sobre éstos, y se devuelva el informe. Hasta ese momento, todo lo que se vaya extrayendo y trabajando no puede ser consultado por los *stakeholders* del proceso judicial. Como se explicará más adelante, con FOMO se trata de permitir un cambio en el proceso de trabajo, que permita incorporar en forma temprana a los instructores al entorno de análisis y que puedan acceder a la información a través de medios informáticos, con el respaldo del informe final del perito para garantizar la información sobre la que trabajan.

II. Desarrollo

El proyecto FOMO se focaliza en resolver algunas cuestiones y desafíos con los que hoy se encuentra el Ministerio Público de la Provincia de Buenos Aires al momento de realizar el análisis forense de dispositivos móviles. Del estudio y análisis de los softwares que se comercializan, se hace evidente que hay aspectos que pueden mejorarse, y de esta forma, mejorar tanto la capacidad de trabajo como la calidad del resultado que se puede obtener.

Algunos de los aspectos que se han identificado para mejorar son:

- Importación de adquisiciones desde distintas fuentes.
- Entorno de análisis mejorado y compartido a través de la red interna.
- Asistencia en la generación de reportes específicos.

La importación de adquisiciones desde distintas fuentes permite que se integre información al Entorno de Análisis FOMO tanto desde el propio software de extracción que se está desarrollando, como desde otros productos de análisis forense de móviles, como UFED o XRY. Esto permite que se realice la adquisición con las herramientas que pueden manejar de mejor forma cada caso: aquellos equipos que pueden conectarse a la computadora a través del cable USB se puede extraer su información por medio del Extractor FOMO, dejando disponible los equipos UFED y XRY para los modelos de teléfonos que cuentan con conectores especiales (incorporados en estos productos) que solo pueden adquirirse utilizando estas herramientas. Luego el módulo de importación de información interpreta los archivos generados por cualquiera de los extractores soportados, e incorpora la información en el servidor FOMO de la red local para comenzar a trabajar con el Entorno de Análisis.

El Entorno de Análisis de FOMO va a ser una aplicación web que se aloja en un servidor de la red interna de la institución (puede ser LAN o una VLAN o VPN de alcance regional) y brindará una interfaz que permite iniciar procesos de análisis sobre los datos, ver los resultados de estos procesos, analizar los datos desde distintas vistas (ya sea como tablas de una base de datos, representaciones afines a la información que representan, o vistas que faciliten algún tipo de análisis determinado), explorar la información contenida en el dispositivo, y seleccionar la representación más adecuada para incluir en un informe específico. Además, al ser una aplicación que se accede a través del navegador, el Entorno de Análisis podrá ser accedido cómodamente por los fiscales, instructores e investigadores del ministerio público para que puedan ir accediendo a la información del informe pericial de una forma más cómoda e intuitiva. Esto permitirá que las personas que necesitan acceder a la información puedan hacerlo de forma más cómoda que un informe estático en papel, en el que resulta difícil buscar datos específicos o relacionarlos entre si.

Los reportes específicos son una herramienta más en esta dirección, ya que permiten condensar información relevante a un aspecto de la investigación o pericia en unas pocas páginas, que acompañan al reporte completo pero son mucho más cortos. Usualmente un informe completo

de los contenidos de un *smartphone* estan ocupando entre 500 y 1000 páginas (en PDF o papel), y la información más relevante para la investigación puede encontrarse en unas 20 o 30 páginas que se encuentran dispersas a lo largo de todo el contenido. Dado que el Entorno de Análisis permitirá seleccionar la información y "etiquetarla" de acuerdo a cada informe específico que se quiera realizar, se podrá optimizar algunos procesos internos de la institución. De esta forma, el informe específico confiere rápidamente la información, y se puede ampliar el análisis tanto con el Entorno de Análisis como con el informe completo.

El proyecto se está llevando a cabo con una metodología de trabajo basada en las metodologías ágiles que se utilizan en muchas empresas de desarrollo de software. Esto permite organizar el grupo de trabajo, donde participan expertos de Ministerio Público que brindan su experiencia en la utilización de este tipo de herramientas, pero cuentan con tiempo reducido y de quienes es necesario extraer los requerimientos e ir adaptando el software a sus necesidades. También se está tomando un enfoque basado en prototipos funcionales, sobre los que se va construyendo las aplicaciones finales. Esto permite que rápidamente entren en contacto con lo que será la interfaz, y puedan sugerir cambios y mejoras para que la herramienta se adapte mejor a su actividad y sus necesidades.

A nivel de diseño, se plantea una jerarquía de clases modular, que soporte la integración al proyecto de distintos plugins para manejar la recolección, análisis y muestra de información proveniente de distintas fuentes de datos dentro del dispositivo. De esta forma se puede trabajar en la incorporación de módulos de análisis para aplicaciones en forma específica. Esto es prácticamente una necesidad si se tiene en cuenta que las aplicaciones de *smartphones* se actualizan en forma regular y pueden cambiar configuraciones de una versión a otra. Esto es transparente para los usuarios, pero puede si se cambia la forma en que se almacena la información, los scripts de análisis que no se actualicen al cambio dejan de funcionar. Una complicación adicional es que no se pueden reemplazar los módulos de análisis por versiones más modernas, sino que debe tenerse módulos para cada versión que sea necesario analizar, ya que muchas veces se deben realizar pericias sobre equipos que no están actualizados y tienen versiones anteriores de las aplicaciones.

La arquitectura del sistema consiste en cliente-servidor, con clientes específicos que cargan información sobre el sistema (el programa Extractor, o los módulos de importación) y clientes que acceden a la información a través del Entorno de Análisis. El servidor donde corren los servicios y aplicaciones FOMO coordina las tareas de importación de información, procesamiento y acceso a los datos, y lleva los registros necesarios para brindar trazabilidad y replicabilidad.

En su versión inicial, se está contemplando un análisis en profundidad del sistema operativo Android, dado que cuenta con un altísimo procentaje del mercado de celulares inteligentes actualmente, superior al 80%. De esta forma se puede lograr un gran impacto, concentrando el equipo de trabajo en un sistema operativo específico. Para reforzar el trabajo sobre Android, además del desarrollo principal de FOMO, que supone el desarrollo de los servicios, jerarquías de clases, bases de datos, estructuras y programas de soporte, tres alumnos avanzados de la carrera de Ingeniería en Informática complementan con el Proyecto Final de Graduación “FOMO en Android”, en el que investigan cuestiones específicas de la arquitectura y aplicaciones que forman parte de dicho sistema operativo, y aportan módulos específicos para el análisis del mismo al desarrollo principal de FOMO.

III. Conclusiones y Trabajo Futuro

El desarrollo de las aplicaciones y sistemas necesarios para soportar una plataforma de análisis forense de dispositivos móviles es desafiante y complejo, ya que debe cumplirse con todos los requisitos para brindar las funcionalidades de análisis, pero también deben darse garantías sobre el tratamiento de los datos para no modificarlos, y llevar registros de las acciones realizadas para facilitar las eventuales tareas de auditoría sobre cada caso o investigación.

Si bien al momento el proyecto se encuentra en desarrollo, ya se han realizado tareas de relevamiento de requerimientos funcionales, no funcionales, diseño y algunas tareas de desarrollo.

El Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA ha trabajado durante más de 8 años en investigación aplicada, entendiendo las demandas concretas de la sociedad, en este caso del Ministerio Público, y asumiendo el desafío de generar soluciones ingeniería a problemas concretos de las instituciones del país. Sumado a su capacidad técnica, el compromiso profesional, la vocación de servicio y la calidad humana de estos jóvenes investigadores argentinos, que trabajan en silencio, fortalecen la capacidad y potencial del InFo-Lab en particular y de la ingeniería argentina en su conjunto.

Este laboratorio y sus proyectos son un aporte concreto de la Universidad al Estado, en pro de la mejora de la sociedad toda. La conjunción multidisciplinaria de actores académicos con los del poder judicial y ejecutivo, tanto en el plano provincial como municipal, demuestra que la colaboración Universidad-Estado, que tanto se promueve, es posible.

El InFo-Lab, inédito en su diseño y conformación mixta, es un ejemplo más, de los tantos que hay en el país, que honran la verdadera misión de la ingeniería: crear, con ingenio y compromiso, para mejorar la calidad de vida de la gente.

IV. Reconocimientos

Los autores agradecemos a la Universidad Fasta, el Ministerio Público Fiscal de la Provincia de Buenos Aires y el Municipio de General Pueyrredón por el apoyo brindado al grupo de Investigación en Informática Forense y Sistemas Operativos y el InFo-Lab. Sin el apoyo de las tres instituciones, este trabajo no habría sido posible.

V. REFERENCIAS

Libros:

[1] http://source.android.com/
[2] Rizwan Ahmed, Dr. Rajiv V. Dharaskar, Dr. Vilas M. Thakare, "Digital evidence extraction and documentation from mobile devices", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1, January 2013.
[3] Manual de Usuario de UFED, Cellebrite.
[4] Ana H. Di Iorio, "InFo-Lab: Investigando y desarrollando tecnología nacional en Informática Forense", Revista Argentina de Ingeniería, Año 3, Vol. 5, Abril de 2015.