Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles

A brief explanation on digital forensic techniques over mobile devices and systems

Guillermo Elías Jaramillo Cabrera[1]
guillermojaramillo.com

INTRODUCCIÓN

La disciplina del Análisis Forense Digital, es un campo de investigación excitante y dinámico, conocido hasta ahora sólo por especialistas, y tiene cada vez más un poderoso impacto en una variedad de situaciones, incluyendo ambientes corporativos, investigaciones internas, litigación civil, investigaciones criminales, investigaciones de inteligencia y asuntos de seguridad nacional. El Análisis Forense Digital Móvil, es sin duda, el de mayor crecimiento y desarrollo en la disciplina forense digital y ofrece ventajas significativas así como también muchos retos. Mientras que lo interesante de la investigación forense de dispositivos como los que usan el Sistema Operativo Móvil Android o simplemente dispositivo Android, implica la adquisición y análisis de datos; es importante tener una visión amplia tanto de la plataforma como de las herramientas que serán utilizadas a lo largo de la investigación. Un entendimiento minucioso asistirá al Ingeniero Examinador Forense o Ingeniero de Seguridad a través del análisis e investigación exitosos de dispositivos móviles, incluyendo los Smartphone basados en Android.

Buscando el por qué

Evidentemente existen razones para la investigación forense digital. La industria y el comercio actual, utilizan cada vez más, dispositivos tecnológicos para soportar su actividad económica; el giro de cada negocio actual se apoya en aparatos tecnológicos de una forma creciente (1). La información, como base del conocimiento de la inteligencia de negocios, reside entonces en estos aparatos y se manipula a través de software como por ejemplo, Android. Lo anteriormente dicho se traduce en miles de millones de dólares como inversión en tecnología (2).


Guillermo Jaramillo

Sin embargo se debe tener en cuenta aspectos como la seguridad de datos, privacidad y recuperación ante desastres, que hacen necesaria una examinación forense de modo

1 Ing. de Sistemas y Computación, Consultor en desarrollo, soporte y certificación de sistemas.

Recibido: 23-12-11 Aprobado: 18-01-12

de asegurar la calidad y la inversión en tecnología. Los Smartphone son quizá, en general, el único dispositivo electrónico con el que están más vinculadas las personas. Para la mayoría de la gente, su Smartphone se encuentra raras veces, a más de un metro de distancia de ellos, incluso mientras duermen. Tal dispositivo puede manejar a la vez información personal y corporativa con la capacidad de almacenar grandes cantidades de datos, incluyendo mensajes de texto, correos electrónicos, ubicaciones GPS, imágenes, videos y más. (3)

Vínculos digitales

Las personas tienden a desarrollar un mayor vínculo de honestidad con su Smartphone que con alguna otra persona o dispositivo. La razón es simple: "la gente siente que el dispositivo es seguro y los puede proveer de respuestas a las preguntas que puedan escoger no compartir con cualquier otra persona". Más de lo que un examinador forense ha dicho sarcásticamente, "Usted es lo que Usted busca en Google", esta aseveración esboza una percepción a priori de la honradez con la cual las personas usan sus Smartphone.

Como tal, los examinadores deben usar sumo juicio al examinar un dispositivo móvil y si el dispositivo ha sido alterado, deben poder explicar cómo y porqué se tomó esta decisión. Algunos forenses digitales hacen una excepción a este enfoque y los debates que se han suscitado. Sin embargo, las técnicas que pueden alterar un equipo de destino para el examen forense se han utilizado durante algún tiempo. Por ejemplo, a menudo un análisis de la memoria RAM en vivo es necesario en una investigación de un ataque de malware. Del mismo modo, si un disco duro está cifrado, el examinador debe obtener una imagen del dispositivo, mientras que el disco está encendido o se corre el riesgo de no poder acceder a los datos de la unidad. Otros buenos ejemplos, son los sistemas que deben permanecer en línea debido a entornos complejos y que se encuentran típicamente en los casos de grandes servidores corporativos. (5)

El análisis forense digital

Mientras que los examinadores deben esforzarse para no cambiar el dispositivo que están investigando, rara vez esto es

Figura 1: Almacenamiento secundario de un sistema computacional.
Fuente: http://www.sapphire.net/images/uploaded/6Sapphire09.jpg

posible en el mundo móvil. Así, si el dispositivo no se puede modificar, entonces la única opción sería no examinar el dispositivo. Es evidente que esta opción no es aceptable como evidencia de la ciencia forense móvil, componente crítico en muchas investigaciones que incluso ha resuelto muchos crímenes. Complican aún más investigación forense de Android la gran variedad de dispositivos, las versiones de Android y las aplicaciones existentes. Los cambios en los dispositivos y en las versiones de Android son únicos en los miles de dispositivos y en cada uno, sin embargo la plataforma tiene características únicas.

Mientras que un análisis lógico de todos los teléfonos Android se puede lograr, las grandes combinaciones de hardware de la totalidad física de cada dispositivo Android son probablemente inalcanzables. Incluso una pequeña diferencia en la versión de Android puede requerir de extensas pruebas y validación en casos de gran relevancia.

Privacidad y sistemas móviles

Hay un delicado equilibrio en ser a la vez un analista forense y un defensor de la privacidad. Si un dispositivo fuera 100%

seguro, entonces la investigación forense del mismo, no devolvería ninguna información. Por otro lado, si las medidas de seguridad del dispositivo están completamente ausentes, es necesaria una ardua pericia forense para extraer datos significativos desde el dispositivo (6).

Los principales consumidores de ciencia forense móvil son las fuerzas del orden y las agencias gubernamentales. Ambos utilizan y resguardan muchos tipos de datos confidenciales en dispositivos móviles bajo la orden y la autoridad de investigar crímenes. Se basan no sólo en el Análisis Forense Digital, sino también en ejercer su autoridad a través de sus mecanismos de persuasión como, órdenes de allanamiento y citaciones para obligar a las organizaciones a producir la información necesaria tal como registros financieros, correo electrónico, registros de proveedores de servicios de Internet y mucho más.

Del mismo modo, las empresas necesitan proteger datos sensibles y en ocasiones hacer investigaciones para garantizar la seguridad interna. Mientras que su autoridad no abarca más allá de los ámbitos de su empresa, también pueden ejercer una autoridad amplia relacionada con la búsqueda en los dispositivos que poseen.

Por último, las personas tienen derecho a acceder a sus propios datos. Ya sea que hagan uso de este derecho para fines civiles o judiciales, tienen autoridad para indagar en los dispositivos de su propiedad. En los casos de personas naturales o jurídicas, las partes generalmente no tienen necesidad de recuperar la información confidencial, como números de tarjetas de crédito, información bancaria o contraseñas en los dispositivos de su propiedad.

Los sistemas móviles como objetivo

Las empresas no buscan datos como por ejemplo, de tarjetas de crédito personales en una investigación interna, ellas tienen los medios para acceder a los sistemas de correo electrónico corporativo y cambiar contraseñas. En el caso de las personas naturales, ellas ya tienen acceso a sus propios registros financieros, correos y otros datos sensibles. En el caso de las fuerzas de la ley y las agencias gubernamentales, pueden utilizar su poder de persuasión y órdenes de allanamiento para obtener los datos que buscan. Por lo tanto, al final, las personas que probablemente sólo se beneficien de datos altamente sensibles que se almacenan de manera insegura en los dispositivos móviles son los criminales cibernéticos (7).

En el curso de muchas investigaciones ya sean individuales, empresariales o penales de dispositivos móviles, se encuentra información personal muy sensible la cual es fundamental para el caso. Sin embargo, si los cibercriminales tienen acceso a los dispositivos, ya sea en forma física o mediante exploits remotos, los datos que pueden reunir, representan un peligro significativo para el propietario (8).

Del mismo modo, las organizaciones son objeto de espionaje comercial, robo financiero, robo de propiedad intelectual y una amplia variedad de otros ataques. Como muchas empresas transfieren la propiedad de dispositivos a sus empleados, se pierde un mayor control y supervisión del dispositivo y se pone la propiedad de datos corporativos en un gran riesgo (9). Por último, las fuerzas de la ley y las agencias gubernamentales se ven afectadas negativamente por los problemas de seguridad móviles. Las agencias están compuestas por individuos que comparten los mismos riesgos de exposición de sus datos que los consumidores. Al igual que las corporaciones, las agencias en sí mismas pueden ser el blanco de ataques, los cuales buscan no sólo datos confidenciales que podrían poner en peligro investigaciones o perjudicar a la agencia, sino también motivos tan graves como el espionaje internacional (10).

Por estas razones, los temas de seguridad en dispositivos móviles son una preocupación creciente para las personas, corporaciones, fuerzas del orden y las agencias gubernamentales.

CONCLUSIONES

Hay una gran variedad de situaciones que pueden beneficiarse de los resultados de una investigación forense. Si bien la aplicación de la ciencia forense es un elemento común en todas las situaciones, cada una puede requerir diferentes procedimientos, documentación y enfoque general.

- La primera situación es probablemente las del grupo que serán utilizadas en un tribunal civil o penal. En estas situaciones, hay una serie de consideraciones importantes: cadenas de custodia, reportes detallados e informe final, posible validación de resultados utilizando diferentes herramientas informativas u otros investigadores, testimonio basado en hechos u opiniones.

- Otra situación común son las investigaciones internas en las empresas. Estas investigaciones pueden terminar litigando en los tribunales, pero a menudo se utilizan para determinar la causa raíz de un problema (en un sistema, ataques externos o internos) y pueden resultar en acciones disciplinarias contra algún empleado. Las investigaciones internas corporativas pueden cubrir muchas áreas, pero son las más comunes: robo de datos o de propiedad intelectual, uso inapropiado de recursos de la empresa, intento de ataque o ataque exitoso contra los sistemas informáticos, investigaciones relacionadas con el empleo como la discriminación, acoso sexual, etc., auditoría de seguridad (aleatoria o específica)

- También hay una necesidad de análisis forense en los casos de asuntos de familia. Los casos más comunes incluyen: divorcio, custodia de menores, litigio de bienes.

- Una última área donde la investigación forense puede generar un importante valor es en la seguridad y el funcionamiento de un gobierno. Los gobiernos suelen ser el mayor empleador en un país, entonces se hallan expuestos como empresa a los problemas antes citados. Más allá de las cuestiones relacionadas con el empleo, los países también son el blanco potencial de ataques extranjeros y la recopilación de datos de inteligencia de gobiernos extranjeros. La Investigación Forense puede desempeñar un papel clave en frustrar los ataques contra un país, la investigación de ataques realizados con éxito, los escenarios de contra inteligencia, y en el suministro de valiosa información de inteligencia necesaria para el gobierno del país.

REFERENCIAS BIBLIOGRAFICAS

1. Hoog A. Android Forensics - Investigation, Analysis, and Mobile Security for Google Android. Waltham: Syngress; 2011.

2. Daniel L, Daniel L. Forensics for Legal Professionals - Understanding Digital Evidence From the Warrant to the Courtroom. Waltham: Syngress; 2012.

3. Stark J, Jepson B. Building Android Apps with HTML, CSS, and JavaScript. 2da Edición. Sebastopol: O'Reilly; 2012.

4. Reyes A, Wiles J. The Best Damn Cybercrime and Digital Forensics Book Period. Burlington: Syngress; 2007.

5. Lillard T, Garrison CA, Steele J. Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Burlington: Syngress; 2010.

6. Steel C. Windows Forensics - The Field Guide for Conducting Corporate Computer Investigations. Indianapolis: Wiley Publishing, Inc.; 2006.

7. Jakobsson M, Ramzan Z. Crimeware: Understanding New Attacks and Defenses. Boston: Pearson Education Inc.; 2008.

8. Kipper G. Wireless crime and forensic investigation. Boca Ratón: Auerbach Publications; 2007.

9. Mohay G, Anderson A, Collie B, de Vel O, McKemmish R. Computer and Intrusion Forensics. Norwood: Artech House; 2003.

10. Barbara J. Handbook of Digital and Multimedia Forensic Evidence. Totowa: Humana Press Inc.; 2008.p

Correo electrónico:

gjaramillo@continental.edu.pe