ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SYMBIAN OS

C. Agualimpia y R. Hernández.
Maestría en Ingeniería Electrónica, Pontificia Universidad Javeriana

***Resumen*— El presente artículo describe algunos métodos de análisis forenses aplicados a dispositivos móviles. Adicionalmente se plantean diferentes alternativas de análisis en dispositivos móviles con el objetivo de evaluar el alcance que se puede tener con algunos de los software forenses más comunes del mercado. Finalmente se concluye con una lista de características deseables en programas forenses para el Sistema Operativo Symbian.**

***Palabras clave*— Computación forense (*computer forensic*), evidencia digital (*digital evidence*), herramientas forenses (*forensics toolkits*), ME (*Mobile Equipment*), SIM (*Subscriber Identity Module*), sistema operativo symbian (*symbian os*), teléfonos inteligentes (*SmartPhones*).**

I. Introducción

En la actualidad, la mayoría de personas tienen como prioridad poseer o utilizar un teléfono Celular con el fin inicial de saciar la necesidad de comunicarse, propia de todo ser humano; gracias a la convergencia en las telecomunicaciones, ese mismo dispositivo móvil que inicialmente se utilizaba básicamente para comunicaciones de voz, ya está brindando otra serie de servicios o funcionalidades que las mismas redes prestadoras del servicio, están promocionando masivamente con el objetivo de darle al usuario mayores ventajas de movilidad; quien se iba a imaginar que uno se lograra conectar a la Internet desde un teléfono móvil o acceder remotamente a su portal, correo corporativo, o mejor aún, poder manejar todo tipo de software contable, empresarial, administrativo, de gestión y hasta un ERP - Enterprise Resource Planning, tener relaciones con los clientes mediante estrategias de CRM - Customer Relationship Management, conectividad inalámbrica formando redes no solamente GSM – *Global System for Mobile Communications* y CDMA – *Code Division Multiple Accsess*, las cuales históricamente han sido las redes que masificaron la comunicación celular, sino también redes PAN – *Personal Area Network*, con tecnología Bluetooth IEEE 802.15x, WLAN – *Wireless Local Area Network*, con tecnología WI-FI - *Wireless Fidelity*, IEEE 802.11x y WMAN - *Wireless Metropolitan Area Network*, o WWAN - *Wireless Wide Area Network*, con tecnología WIMAX - *Worldwide Interoperability for Microwave Access*, IEEE 802.16x, y todo esto en un mismo dispositivo móvil; las funciones que anteriormente estaban solamente diseñadas para ser utilizadas en PC's o Mac's de escritorios y *laptops* sobre redes LAN - Local Area Network, alambradas privadas o corporativas, utilizando plataformas con sistemas operativos Windows o Unix y realizando conectividad remota por medio de módems telefónicos fijos (hasta 56Kbps), sistemas del tipo RADIUS - Remote Authentication Dial-In User Server, o VPN – Virtual Private Network, a través de la Internet, están prácticamente quedando atrás y olvidadas por la masiva penetración en el mercado de los teléfonos móviles, dentro de los cuales se está convergiendo a los llamados *SmartPhones*. Se estima que para el año 2009 las ventas de teléfonos móviles supere la cifra de un billón de ventas al año [20].

Bien es sabido que las nuevas tecnologías crean nuevas vulnerabilidades [1], y en los teléfonos móviles, de hecho, se tiene una arquitectura y software totalmente diferente al de los computadores que estamos tan acostumbrados. Aunque sus características pueden ser relativamente simples, los fabricantes de teléfonos móviles (NOKIA, MOTOROLA, SONY ERICSSON, PALM, BLACKBERRY, HP, SAMSUNG, LG, APPLE, entre otros importantes) emplean muy heterogéneos sistemas operativos y estructuras de almacenamiento [2] que además dependen del modelo en particular (por ejemplo: Nokia 3220, Nokia 6620, Nokia N95, Motorola V3, etc.). Dentro de esta diversidad, surge el Sistema operativo Symbian, como ente unificador para muchos dispositivos, en especial aquellos que tienen características asociadas a los *SmartPhones* (Symbian está presente en más del 60% de los teléfonos inteligentes del mercado actual [3]), los cuales son diseñados para adaptarse a ambientes de movilidad, siendo estos herederos de las PDA's - *Personal Digital Assistant*; en los trabajos de campo realizados para la evaluación de desempeño de los software forenses concerniente a este documento, se trabajó con dos teléfonos, el primero un Siemens C66 (un dispositivo que lleva en el mercado más de 5 años), el segundo un NOKIA N73 (un *SmartPhone* que lleva en el mercado menos de 2 años) el cual trabaja con el sistema operativo SYMBIAN, que es utilizado de manera general por los equipos NOKIA Serie 60, Serie E y Serie N y es muy aceptado a nivel general por los toolkits que se evaluaron.

Carlos Agualimpia es docente catedrático en el Departamento de Ingeniería Electrónica, de la Pontificia Universidad Javeriana, Kr 7 # 40-62, Bogotá (correo e.: cagualimpia@javeriana.edu.co).

Rodrigo Hernández es Ingeniero Consultor de proyectos móviles en *Quantum Data Systems Ltda.*, Kr 13 # 98-47, Bogotá (correo e.: rodrigo.hernandez@javeriana.edu.co).

En este orden de ideas, es preciso tener presente que el riesgo de la muy bien llamada inseguridad informática [4] es mucho más latente y como si fuera poco, más vulnerable gracias a la movilidad que puede poseer un atacante a la hora de violentar alguna plataforma bien sea esta del tipo móvil o fija por medio del uso de estos dispositivos móviles, tema que ya era de importancia en el año 2002 [1]. Adicionalmente también hay que tener muy en cuenta, que no únicamente se trata de los posibles riesgos que genera un atacante, sino de la importancia de poder examinar detalladamente la información que sea relevante y que pueda estar almacenada, escondida, cifrada o suprimida en un dispositivo móvil, como llamadas realizadas o perdidas, imágenes, videos, mensajes de texto, entre otros, ya que por medio de estos, muy seguramente se logrará encontrar evidencia y conectar al sospechoso de algo, con la o las personas afectadas.

Esta breve introducción, pretende mostrar la importancia, la relevancia y la necesidad de tener técnicas forenses de la más alta calidad desde el punto de vista científico y técnico, con el fin de poder interactuar de una manera más directa con una posible evidencia física del tipo digital, que con respecto a la triada del principio de intercambio de Locard [5], la cual plantea la necesidad de interactuar entre *la víctima, la escena del crimen y el sospechoso* se da la posibilidad que a partir de esa evidencia digital se puedan plantear hipótesis concretas que indaguen sobre respuestas a un acto delictivo que bien puede tocarnos directa o indirectamente a nosotros.

II. Recomendaciones para el análisis forense en móviles

En todo tipo de análisis forense, se deben realizar ciertos procedimientos que están enfocados a garantizar la integridad del proceso.

La recuperación de datos en móviles es usualmente realizada de forma lógica en lugar de una adquisición física, usando uno o más protocolos soportados por el dispositivo [2].

En este artículo al igual que en otros [2], se apoya la hipótesis de hacer análisis forense en teléfonos móviles diferenciando los dos módulos que conforman al dispositivo: por un lado el ME (Equipo Móvil) y por otro el módulo que identifica al suscriptor, el cual es llamado SIM - Subscriber Identity Module, en redes GSM [6], RUIM - Removable User Identity Module, en redes CDMA [7,18], y USIM - Universal Subscriber Identity Module o UICC - Universal Integrated Circuit Card, para redes UMTS - Universal Mobile Telecommunications System [8]. De ahora en adelante, por simplicidad independiente del tipo de red, se llamará SIM al módulo que identifica al suscriptor.

Análisis del SIM

El objetivo inicial del SIM es proporcionar un ambiente seguro y resistente al saboteo (extremadamente difícil de violar bajo una variedad de ataques) que identifique a un usuario móvil particular, lo cual se logra manejando claves digitales cifradas (de uso de los operadores de telefonía) que autentican a los usuarios en la conexión a la red y rastrean aquellas actividades que realizan una vez están "al aire". El SIM mantiene conexión permanente con la red desde que el ME se enciende; sin el SIM el ME no se conecta a la red [21].

El SIM, en la mayoría de los casos, se asocia a un chip o tarjeta inteligente (*Smart Card*) [22]. Las principales características del chip, desde el punto de vista forense, es su portabilidad y memoria [23], capaz de albergar datos con información del suscriptor en un espacio de almacenamiento que esta alrededor de los 64kB (existen de mayor capacidad hasta de 1MB no tan comerciales), allí el usuario puede almacenar información relevante como mensajes de texto y multimedia, directorios telefónicos, fechas de calendario, entre otros según la capacidad que se tenga.

Una segunda funcionalidad importante del SIM es su capacidad de albergar aplicaciones, normalmente conocidas como *Applets*, siendo de interés pericial aquellas aplicaciones que almacenan claves de cifrado o inclusive aquellas que potencian el uso del ME para aplicaciones en Internet [9], como por ejemplo aplicaciones de comercio electrónico.

El análisis forense de la SIM puede ser muy dispendioso y mostrar pocos avances, debido a las características de seguridad con las que se concibe este módulo. Sin embargo el análisis se facilita si el perito posee un conocimiento básico de la estructura de archivos, y si además el usuario, ha deshabilitado el uso del PIN o CHV1 [17], para acceder a los datos del chip (o en su defecto si se conoce el PIN).

Un primer acercamiento forense de la SIM debe procurar mostrar los siguientes datos:

- El Cell ID: identificador de dónde está el dispositivo actualmente situado (o dónde estuvo antes de apagarse el celular).
- IMSI (número serial que identifica al suscriptor)
- ICCID (número serial que identifica la SIM)
- Contactos telefónicos
- Mensajes de Texto (o multimedia, si es el caso) recibidos: Usualmente la SIM alcanza a guardar al menos 12 mensajes de texto.
- Mensajes de texto (o multimedia, si es el caso) Borrados
- Mensajes de texto enviados y guardados en la SIM.
- Números marcados (a veces este dato no se guarda en la SIM).

Vale la pena mencionar, que algunos de los datos anteriores pueden ser modificados, sin que el usuario se dé cuenta, mediante un ataque por Bluetooth [10]. Por esto el análisis forense puede tornarse un poco delicado.

La mayoría de datos mencionados anteriormente, son los que de forma clásica los distintos *forensics toolkits* se han encargado de encontrar en mayor o menor medida.

Un ciberatacante, con un mínimo de experiencia en dispositivos móviles, sabe que el lugar más "seguro" para almacenar datos de gran importancia es la SIM. Por tal razón puede crear (o pagar para que una tercera entidad lo haga) una aplicación que almacene dichos datos en la SIM. Es en este punto donde el análisis forense se ve gravemente limitado. Las herramientas forenses de la actualidad no están en la capacidad de detectar dichos Applets junto a la información que almacenan, y solamente un profundo análisis mediante software especializado en *Smart Cards* combinado con alguna pista encontrada en las comunicaciones del ME con el SIM podrían llevar a buen término la investigación.

ANÁLISIS DEL ME

El equipo móvil (ME) es el módulo en donde normalmente recae el grueso del análisis. Aunque el análisis del SIM puede complicarse si este tiene algún *Applet* distinto a los proporcionados por el operador, lo normal es que no lo tenga, el análisis en la mayoría de los casos se limita a buscar en 64KB de datos. Por otro lado el ME, dependiendo de la gama, puede almacenar hasta 8 GB de información como es el caso del *smartphone* Nokia N95 o inclusive más datos, si se trata por ejemplo de la última versión del *iPhone* de Apple.

Adicionalmente, se debe contar con el hecho de que el mercado posee una gran diversidad de MEs. Cada familia de dispositivos es diferente y tiene sus particularidades tanto en su estructura de datos, como en los protocolos que se deben utilizar para extraer su información.

Complicando las cosas, adicionalmente se presentan algunas variaciones en la estructura y ubicación de los datos y en el firmware de algunos modelos de teléfonos que son personalizados para los operadores por los fabricantes (por ejemplo teléfonos marca Movistar, O2, etc.).

Una vez el investigador forense a identificado la marca (o fabricante en la mayoría de los casos) y el modelo del ME, debe proceder a realizar el análisis. El análisis debe hacerse con varias herramientas y además se debe tener en cuenta que los nuevos modelos telefónicos a menudo tienen diferencias en sus funcionalidades con respecto a modelos anteriores, lo que hace que una herramienta forense a veces no pueda recuperar y reportar los datos apropiadamente. Cuando un nuevo teléfono es lanzado al mercado, un fabricante de herramientas forenses debe decidir si adaptar su herramienta al nuevo modelo, pagar los correspondientes estudios que se le hagan a dicho modelo, crear y probar una versión actualizada del *toolkit*, y finalmente distribuir la herramienta actualizada al investigador forense (los *forensics toolkits* necesitan ser distribuidos periódicamente para superar el inconveniente de los nuevos modelos telefónicos que van apareciendo). El tiempo requerido para que las actualizaciones de los *forensics toolkits* estén disponibles, puede ser muy amplio, colocando a los especialistas forenses en problemas. A veces la situación puede requerir maneras alternativas de adquirir los datos de modelos telefónicos muy recientes. Muchos especialistas forenses de móviles usan una colección de herramientas forenses y no-forenses (por ejemplo las *PC suites* proporcionados por los fabricantes del teléfono) junto con otros accesorios para formar sus "*toolbox*". Obviamente las herramientas no diseñadas específicamente para propósitos forenses utilizan conexiones USB o Bluetooth que tienen resultados, que con razón [11], son cuestionables.

Los pasos para realizar el análisis varían dependiendo de la gama del dispositivo. Esto se debe a que los teléfonos de gama baja se limitan simplemente a guardar información básica del usuario, tal como:

- Fecha y hora de llamadas realizadas, recibidas y perdidas.
- Fecha y hora de los Mensajes de texto recibidos, enviados y borrador.
- Registro de llamadas borradas.
- Contactos telefónicos
- Log de las páginas Wap y Web visitadas
- Ring tones
- Imágenes y fotos.

En cambio los teléfonos de gama alta pueden tener información comparable a la que tiene un computador de escritorio. Para este tipo de dispositivos, dentro de los cuales se encuentran los *SmartPhones*, se proponen de forma general los siguientes pasos, basados en [12], para realizar un análisis forense:

1. Creación del archivo de hallazgos (documento que permite llevar un historial de todas las actividades que se llevan a cabo durante el proceso y de los hallazgos encontrados)
2. Imagen de datos (o backup cuando no sea es posible realizar la imagen)
3. Verificación de integridad de la imagen
4. Creación de copias de la imagen suministrada
5. Aseguramiento de la imagen suministrada
6. Revisión antivirus y verificación de la integridad de la copia de la imagen.
7. Identificación de las particiones actuales y anteriores (las que sea posible recuperar). Esto se hace importante en los drives removibles (memorias flash removibles).
8. Detección de información en los espacios entre las particiones. Para no utilizar el ME de forma física, es muy útil el uso de los emuladores proporcionados por los fabricantes de teléfonos. De esta forma no se corrompe la evidencia [13].
9. Detección de las HPA - *Host Protected Areas*. Se deben utilizar emuladores hasta donde sea posible.
10. Identificación del sistema de archivos.

11. Recuperación de los archivos borrados.
12. Recuperación de información escondida.
13. Identificación de archivos existentes.
14. Identificación de archivos protegidos (quebrar la seguridad).
15. Consolidación de archivos potencialmente analizables
16. Determinación de la versión del sistema operativo, las aplicaciones instaladas y conexiones que han abierto las aplicaciones instaladas en el teléfono. Para analizar las aplicaciones instaladas se recomienda la utilización de los kits de desarrollo proporcionados por los fabricantes de teléfonos [13].
17. Filtrado basado en archivos buenos conocidos
18. Consolidación de archivos sospechosos
19. Primera Clasificación
20. Segunda Clasificación
21. Analizar los archivos
22. Archivos comprometidos con en el caso
23. Obtención de la línea de tiempo definitiva
24. Generación del informe

Para una explicación detallada de los anteriores pasos, por favor revisar [12].

Como se mencionó anteriormente, el análisis forense se debe hacer con varias herramientas, debido entre otros factores a que la prisa con que las nuevas versiones del *toolkit* son desarrolladas produce herramientas imperfectas (con *bugs* en la mayoría de los casos). Al utilizar varias herramientas se aumenta la confiabilidad de la investigación.

III. ANÁLISIS ESPECIALIZADO: SYMBIAN OS

Como se mencionó en la introducción, el sistema operativo Symbian está surgiendo como elemento unificador en los dispositivos móviles, tanto así que ya está consolidado en el mundo de los *SmartPhones*. Por esta razón, se plantea en este artículo la necesidad de una herramienta forense especializada en Symbian OS, así como se encuentran también para sistemas Windows o Unix.

Symbian, también tiene sus inconvenientes, al ser un sistema operativo que se está renovando continuamente, trae problemas o *bugs* que pueden ser aprovechados por los ciberatacantes. Además, aunque el software este bien hecho, muchas veces el mismo usuario se encarga de mover al mínimo el nivel de seguridad del software, con lo cual se abren muchas vulnerabilidades.

Es de especial interés la construcción de un emulador para análisis forense (los emuladores para desarrollar aplicaciones ya existen), de tal forma que se puedan emular y montar imágenes (o *backups*) de cualquier dispositivo con un sistema operativo Symbian, pudiéndose analizar el comportamiento del kernel, la memoria y los distintos sistemas de archivos que posee [14], a saber:

- El ROM file system que es usado para almacenar código sobre XIP. XIP se refiere a la capacidad de ejecutar código directamente fuera de la memoria.
- El Log Flash file system (LFFS) para almacenamiento de datos de usuario sobre memoria Flash NOR.
- El sistema de archivos FAT para almacenamiento de datos de usuario sobre memoria Flash NAND, drives de RAM interna y drives (media) removibles.
- El Read-Only file system (ROFS) para código almacenado sobre medios no-XIP tal como memoria Flash NAND. El código no-XIP tiene que ser copiado primero a la RAM para ser ejecutado.

La dificultad de la creación del emulador radica, en que se debe crear un software para PCs que imite las características de una arquitectura computacional distinta, empezando por el procesador de tipo ARM, un Kernel de tiempo real [14], y otras particularidades como el hecho de no manejar discos duros sino (en la mayoría de los casos) solo memoria de tipo FLASH. Adicionalmente a nivel del software, se debe empezar por crear la partición "Z" donde se encuentran los datos del sistema operativo y dejarla "visible" para un posible análisis forense. Finalmente, añadiendo un poco de complejidad, se tiene el hecho de que Symbian cuenta con tres distintas Interfaces (Series 60, UIQ y FOMA) que añaden ciertas particularidades a la versión del sistema operativo.

Una vez se tiene el emulador con propósitos forenses, los *forensics toolkits* deben perfeccionar sus diferentes técnicas (adaptar o crear nuevas técnicas si es necesario), que de acuerdo a las particularidades Hardware y Software, ayuden a la consecución de un buen análisis basado en diferentes pasos, como por ejemplo los propuestos en [12].

IV. DESEMPEÑO DE HERRAMIENTAS

Dentro de las variadas herramientas forenses para dispositivos móviles que se encuentran en el mercado, se decidió analizar tres de ellas: TULP2G, PARABEN y MOBILedit! FORENSIC. El objetivo final fue analizar su desempeño teniendo como punto de comparación las características [12] brindadas por herramientas forenses enfocadas a computadores tales como EnCase y The Sleuth kit, a saber:

- Recuperación de archivos borrados
- Verificación de firmas de tipo de archivo (identificar si el contenido de los archivos no corresponde a su extensión).
- Capacidad de buscar, filtrar y organizar los archivos según diferentes criterios, lo que permite alcanzar una visión más clara del caso.
- Reconstrucción temporal
- Recuperación de particiones.

- Apoyo en el análisis de Logs
- Toolkit de análisis para Internet
- Realización de la imagen en formato *raw* o *split*
- Facilitar la búsqueda de información en el slack space (*Data Carving*)
- Detección de información en los espacios entre las particiones.

TULP2G

Este es un framework de software forense para adquisición y decodificación de datos almacenados en dispositivos electrónicos [15]. Esta herramienta desarrollada por el *Netherlands Forensic Institute*, es *open source* y como tal brinda unas ventajas y otras desventajas con respecto a otras herramientas licenciadas.

Como se describió anteriormente las herramientas forenses móviles deben ser continuamente actualizadas, por lo que TULP2G presenta grandes deficiencias en este aspecto. Esto se evidenció al intentar analizar el dispositivo Nokia N73 del cual no se obtuvo ninguna información.

El proceso de investigación es modelado con cuatro diferentes categorías de plug-in: dos para adquisición de datos y dos para convertir y exportar los datos. Una quinta categoría de plug-in ha sido definida para tareas relacionadas a casos.

Las investigaciones pueden ser agrupadas en casos. Todos los datos relacionados a un caso son almacenados en un archivo con formato XML.

Con esta herramienta se analizó un Siemens C66, utilizando para ello una comunicación serial mediante un cable USB, y analizándolo con dos protocolos: el "AT-ETSI phone protocol" y el "AT-SIEMENS phone protocol", obteniéndose resultados diferentes.

Con el primer protocolo se obtuvieron: los contactos de la SIM, los SMS creados, los SMS recibidos, la respuesta de los Comandos AT más conocidos y el nivel de carga de la batería. Con el segundo se obtuvieron todos los datos obtenidos con el primero, más: algunas imágenes, algunos midis (archivos de sonido), información de los directorios del sistema de archivos y valores propietarios que solo se pueden ver en teléfonos Siemens.

Se puede concluir que este software es un poco limitado (sirve especialmente para hacer análisis del SIM), no recupera ningún dato que hayan sido borrado y si se lo compara con la información recopilada con la *PC Suite* del fabricante, se concluye que obtiene poca información.

PARABEN

Este software es bastante robusto y está dirigido a múltiples plataformas computacionales. La versión para dispositivos móviles se denomina "*Device Seizure*" y permite hacer análisis forense de un gran número de dispositivos. El análisis se organiza por casos, aunque para poder efectuarlo requiere un cierto conocimiento del dispositivo móvil a analizar.

Con este *toolkit* se analizó el *SmartPhone* Nokia N73, obteniéndose bastante información del mismo (inclusive se recuperaron datos que habían sido borrados). La información es organizada en múltiples logs (es bastante tedioso el análisis de la información) teniendo estos la mayoría de características [16] deseables en un análisis forense, a saber:

- Fecha, hora y recurso que se accedió
- Registro de todos los encabezados
- Registro de los parámetros de la petición realizadas.
- Identificador del log, de tal forma que sea posible identificar la falta de un registro.
- Comprobación de integridad (lo hace con MD5 y SHA1).

Además de los logs, se recuperan todos los archivos de usuario dentro del móvil, a saber: directorio telefónico, SMS, fotos, archivos de sonido, archivos de aplicaciones, etc. La única falencia detectada es que no encontró la HPA (*Host Protected Area*) de Symbian, es decir la partición "Z".

De este *toolkit* se puede concluir que recopila bastante información, mucha más que la que alguien podría recuperar haciendo uso de la PC Suite.

MOBILEDIT! FORENSIC

Esta herramienta es bastante robusta y actualizada. Permite hacer un análisis forense diferenciado del SIM y del ME. Con este *toolkit* se analizó el *SmartPhone* Nokia N73.

Una vez se efectúa la conexión (de forma casi automática, a diferencia de los dos *toolkits* analizados anteriormente), la herramienta muestra las principales características del teléfono: IMEI, revisión de Hardware, revisión de Software, red (GSM, para el caso de análisis), resolución de la pantalla, número de colores de la pantalla, soporte de Java, nivel de la batería y nivel de la señal.

Las principales evidencias digitales a analizar por parte de la herramienta son: el directorio telefónico, los archivos de todas y cada una de las particiones (a diferencia de PARABEN, si se encontró la partición Z), gestión de SMS (incluye inbox, items enviados, *drafts*), calendario, notas, tareas y Análisis del SIM.

Adicionalmente la herramienta permite exportar cualquier archivo o dato del teléfono. Finalmente se tuvo una dificultad, esta fue que los reportes forense en distintos formatos (xml, xls, *template* forense del teléfono y *template* forense del SIM) sólo se pueden realizar si se compra el *toolkit*, por lo que esta característica no pudo ser evaluada.

V. CONCLUSIONES

El presente artículo describe la forma idónea como se debe hacer el análisis forense en un dispositivo móvil, diferenciando entre el SIM y el ME.

También se menciona la dificultad que implica el análisis forense a un dispositivo móvil, dada las grandes diferencias que existen entre dispositivos de diferentes fabricantes así, como las numerosas diferencias entre modelos del mismo fabricante.

Adicionalmente se resalta la importancia de la creación a futuro de una herramienta forense especializada en el sistema operativo Symbian y que contemple mejoras sustanciales con respecto a las debilidades que presentan las herramientas forenses actuales.

Se presentaron diferentes características de desempeño en lo relacionado a ventajas y desventajas de los tres *forensic toolkits* aquí evaluados; estos, se encuentran actualmente en la Internet disponible para su evaluación y utilización.

El análisis en dispositivos móviles aparece como una necesidad latente y necesaria a nivel de las investigaciones actuales en cualquier país del mundo, por esta razón, no se deben descuidar los avances y la integración desde el punto de vista científico y tecnológico en este tipo de herramientas; por esto, se deben generar convenios a nivel de investigación que involucren a la academia y los entes de policía judicial.

La temática planteada en [19], pretende romper el paradigma del análisis forense local a un teléfono móvil, y abarca la posibilidad de la utilización de una plataforma móvil MFP - The Mobile Forensic Platform, con el fin de acceder remotamente al dispositivo bien sea este del tipo móvil o fijo, con la ayuda de la infraestructura de red asociada a cada dispositivo, esto para preservar el hardware y liberar de carga al investigador forense en situaciones geográficamente complicadas.

REFERENCIAS

[1] Debra Littlejohn Shinder. (2002). Scene of the Cybercrime: Computer Forensics Handbook. Ed. Syngress Publishing, Rockland - MA, p 62-90.

[2] W. Jansen & A. Delaitre & L. Moenner. (2008). Overcoming Impediments to Cell Phone Forensics. Proceedings of the 41st Hawaii International Conference on System Sciences.

[3] Symbian. (2007, Sep.). Symbian Fast Facts Q4 2007. Symbian. [Online]. Disponible: http://www.symbian.com/about/fastfacts/fastfacts.html

[4] Cano J., (2007),"Inseguridad Informática y Computación Anti-forense: Dos Conceptos Emergentes en Seguridad de la Información", Information Systems Control Journal, Volume 4, 2007.

[5] Cano J., (2008),"Computación Forense: Conceptos, Procedimientos y Reflexiones", Presentación en el curso de seguridad en redes PUJ.

[6] (Especificación Técnica) 3GPP 11.10 (1999). Mobile Station Conformity Specification [doc]. Disponible: http://www.3gpp.org/ftp/Specs/html-info/1110.htm

[7] (Especificación Técnica) 3GPP2 C.S0023-B_v1.0. Removable User Identity Module for Spread Spectrum Systems [pdf]. Disponible: http://www.3gpp2.org/Public_html/specs/C.S0023-B_v1.0_040426.pdf

[8] (Especificación Técnica) 3GPP 22.038 (2004). Technical Specification Group Services and System Aspects; USIM Application Toolkit (USAT) [doc]. Disponible en: http://www.3gpp.org/ftp/Specs/html-info/22038.htm

[9] F. Martínez, R. Hernández, J. Caicedo, O. Caicedo & J. Hurtado. (2007). Plataforma para el acceso a servicios desde dispositivos móviles utilizando parámetros de autenticación basados en SIM Card. Revista de Ingenieria #26. Universidad de los Andes. Bogotá, Colombia. p. 29-38.

[10] C. Castillo & J. Gómez-Casseres, & E. Torres (2007). Blue MAC Spoofing: El Backdoor de Bluetooth. Pontificia Universidad Javeriana. [Online]. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142c1.htm

[11] P. Peña & I. Vásquez (2007). Métodos de control y acceso a través de dispositivos de almacenamiento USB. Pontificia Universidad Javeriana. [Online]. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142b1.htm

[12] J. Cordoba & R. Laverde & D. Ortiz & D. Puentes (2005). Análisis de Datos: Una propuesta metodológica y su aplicación en The Sleuth Kit y EnCase. Universidad de los Andes. [Online]. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142y.htm

[13] M. Burnette. (2002). Forensic Examination of a RIM (BlackBerry) Wireless Device. Rogers & Hardin LLP. [Online]. Disponible en: http://www.rh-law.com/ediscovery/Blackberry.pdf

[14] Jane Sales (2005), Symbian OS Internals "Real-time Kernel Programming", ed. John Wiley & Sons, Ltd - England, p. 17-42 y 251-314.

[15] J. van den Bos & R. van der Knijff (2005). TULP2G – An Open Source Forensic Software Framework for Acquiring and Decoding Data Stored in Electronic Devices. Netherlands Forensic Institute. [Online]. Disponible en: http://tulp2g.sourceforge.net/

[16] J. Torres & R. García (2003). Control, administración e integridad de logs. Universidad de los Andes. [Online]. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m248h.htm

[17] NISTIR-7387 (2007). Cell Phone Forensic Tools: An Overview and Analysis Update, National Institute of Standards and Technology, March 2007.

[18] Hamid Jahankhani (2006). "Criminal Investigation and Forensic Analysis of SmartPhones", Technology & Services Section, Information Security.

[19] Frank Adelstein (2003). "MFP: The Mobile Forensic Platform," International Journal of Digital Evidence, Spring 2003, Volume 2. Issue 1.

[20] Rick Ayers, "An Overview of Cell Phone Forecsic Tools," NIST.

[21] Svein Yngvar Willassen (2003) "Forensics and the GSM mobile telephone system," International Journal of Digital Evidence, Spring 2003, Volume 2. Issue 1.

[22] Fabio Casadei, Antonio Savoldi, Paolo Gubian (2006). "Forensics and SIM cards: an Overview," International Journal of Digital Evidence, Fall 2006, Volume 5, Issue 1.

[23] Wayne Jansen, Rick Ayers (2006). "Forensic Software Tools for Cell Phone Subscriber Identity Modules" Conference on Digital Forensics, Security and Law.