iPhone 3G: Un Nuevo Reto para la Informática Forense

Andrea Ariza, Juan Ruíz y Jeimy Cano

Departamento de Ingeniería de Sistemas, Pontificia Universidad Javeriana,
Carrera 7 No. 40 – 62, Bogotá, Colombia
{a-ariza, jc.ruiz, j.cano}@javeriana.edu.co

Resumen. El presente artículo reúne y expone el estado actual de la informática forense en el dispositivo móvil iPhone 3G. Se presenta un panorama general de la seguridad en dispositivos móviles. Describe el iPhone 3G, su funcionamiento, características principales y las vulnerabilidades identificadas hasta la fecha, a las cuales puede estar expuesto. Presenta los modelos generales de un análisis forense, su aplicación sobre los dispositivos móviles, especificando herramientas y procedimientos utilizados en la actualidad para llevar a cabo dicho proceso sobre el iPhone 3G. Finalmente detalla por qué es importante contar con un procedimiento estándar para realizar un análisis forense sobre éste dispositivo.

Palabras Clave: Informática forense, seguridad informática, procedimientos, estándares, teléfonos celulares, iPhone 3G, metodología, herramientas.

1 Introducción

Según [1], en la actualidad y desde hace aproximadamente diez años, el empleo de dispositivos móviles se ha incrementado notablemente principalmente por su facilidad de uso y la propiedad de mantener en contacto permanente a sus usuarios. A partir de esto, se ha generado un cambio significativo en la forma en que las personas se comunican, pero también por su proliferación, se ha incrementado su uso en actividades de orden delictivo.

Existe gran variedad de gamas de dispositivos móviles, dentro de los cuales el mayor crecimiento en popularidad y uso se presenta en los dispositivos móviles inteligentes, debido a su capacidad tanto para realizar llamadas como para navegar por Internet, y además porque permiten desarrollar y ejecutar aplicaciones que no necesariamente son incluidas por el fabricante [2]. Canalys, empresa que realiza análisis expertos de la industria de alta tecnología, realiza anualmente una investigación acerca del estado del mercado de los dispositivos móviles inteligentes. En los dos últimos años (2007-2008) se ha presentado el mayor crecimiento en el uso de estos dispositivos comparándolo con años anteriores. De los resultados obtenidos cabe rescatar que Apple[1] se introdujo en el mercado en tercer lugar con el dispositivo

[1] Formalmente Apple Computer Inc., empresa norte americana que se caracteriza por producir computadores, portátiles, impresoras, cámaras y sistemas operativos con tecnología innovadora por más de 30 años [9].

móvil iPhone, esto gracias a la innovación en cuanto a diseño e interfaz de usuario que soporta [3]. Además, Canalys estimó que Apple en el 2007 tomó el 28% del mercado de dispositivos móviles de EE.UU [3] y posteriormente en el 2008, con la llegada del iPhone 3G al mercado, Apple se posicionó en el segundo lugar de ventas de dispositivos móviles inteligentes [4], convirtiéndose rápidamente en líder en el mercado de dispositivos móviles.

Al alcanzar tanta popularidad en el mercado mundial de dispositivos móviles y por la variedad de funcionalidades que ofrecen los teléfonos inteligentes, también se han incrementado notablemente los ataques a las vulnerabilidades que presentan ellos. Los ataques fuertes son más fáciles de realizar y son más lucrativos para quienes los desarrollan y llevan a cabo no solo a nivel de dispositivos móviles sino a nivel de cualquier otro sistema informático dentro de una organización [7].

Anualmente el Instituto de Seguridad Informática CSI (Computer Security Institute) [6] publica un reporte llamado "CSI Computer Crime and Security Survey" [5] en el cual se realiza un análisis de la situación actual de la seguridad informática y del crimen informático de las organizaciones participantes, y cuyo objetivo principal es conocer si las mejores prácticas de seguridad informática implantadas producen resultados. Dicha encuesta arrojó que por la necesidad de movilidad y disponibilidad de la información en las organizaciones, el uso de dispositivos móviles inteligentes dentro de estas se ha incrementado notablemente (una de las razones por las cuales su popularidad ha aumentado), al igual que los incidentes de inseguridad (robo de información de propietarios y pérdida de datos de clientes) que ocurren sobre ellos [8]. Cuando un incidente se presenta, es más fácil y debe ser más importante para lograr la identificación de los perpetradores, monitorear los terminales de comunicación que la comunicación en sí misma. Por ejemplo si un criminal utiliza un iPhone para llevar a cabo algún tipo de ataque su operación estará comprometida en cierto nivel [5], pues el hecho que haya utilizado este dispositivo para cometer el ataque implicará que se siga un procedimiento estándar establecido para la realizar la investigación.

En la actualidad existen gran cantidad de proveedores y fabricantes de dispositivos móviles inteligentes, lo que produce heterogeneidad en todo sentido en el campo de la informática forense, especialmente en las herramientas que se utilizan para obtener evidencia de estos dispositivos en una investigación, de tal manera que los fabricantes crean sus propios protocolos para este propósito [2].

A diferencia de la informática forense clásica, el análisis forense sobre dispositivos móviles inteligentes y específicamente sobre iPhone, que es en esencia un computador [5], es un campo relativamente nuevo y los procedimientos y normas para su análisis aún se encuentran en desarrollo [9]. Un análisis forense que se lleve a cabo sobre un dispositivo como éste en una corte, puede ser admitido o no dependiendo de lo que considere el juez que lleve dicho caso y la formalidad con que se desarrolle el procedimiento de recolección, control, análisis y presentación de las evidencias.

2 ¿Qué es el iPhone?

El iPhone es un dispositivo móvil creado por Apple, caracterizado principalmente por combinar tres productos en uno: un teléfono revolucionario, un iPod[2] de pantalla ancha y un innovador dispositivo de internet que permite navegar en la web, recibir correos electrónicos con HTML enriquecido y navegación web completa [18] [27].

2.1 Conociendo el iPhone

Desde hace mucho tiempo, diferentes dispositivos móviles, incluyendo teléfonos celulares, han podido hacer lo que el iPhone es capaz de hacer. Según [9] lo que diferencia al iPhone de los demás, y ha logrado hacerlo tan popular en el mercado de la tecnología móvil, es su diseño de pantalla táctil con un teclado virtual, que permite que el tamaño de la pantalla sea superior a cualquier otro dispositivo de forma tal que se puedan visualizar películas, fotos y navegar por la web de manera sencilla y cómoda [24] [17].

Actualmente, existen dos generaciones de iPhone. De la primera generación se lanzaron modelos con capacidad de almacenamiento de 4 GB y 8 GB, el modelo de 4 GB fue descontinuado del mercado dos meses después de su lanzamiento, por lo cual se lanzó el modelo de 16 GB de capacidad de almacenamiento. De la segunda generación se lanzaron modelos con las mismas capacidades (8GB y 16 GB), la diferencia radica en que el iPhone de segunda generación utiliza tecnología 3G (tercera generación de telefonía móvil), y añade más funcionalidades [9] [16] [29].

2.2 Estructura lógica y física del iPhone

Como ya se ha mencionado anteriormente el iPhone es un teléfono inteligente que integra funcionalidades de iPod y teléfono celular [26]. Es en esencia un computador ejecutando una versión del sistema operativo Leopard UNIX OS de Apple, diseñado principalmente para minimizar las escrituras sobre la memoria flash, de forma tal que se puede conservar y preservar datos por periodos largos de tiempo, incluso por mucho más tiempo que lo que un computador de escritorio podría hacerlo [5] [19].

Aunque los primeros modelos del iPhone tuvieron variaciones, como cualquier dispositivo electrónico complejo, el iPhone es una colección de módulos, chips y otros componentes electrónicos de diferentes fabricantes [21] [23], que ejecuta una versión móvil de MAC OS X 10.5 (Leopard) que es similar a la versión del sistema operativo MAC para computadores de escritorio [5]. Los componentes que se muestran en la siguiente tabla pertenecen al modelo del iPhone 3G.

Tabla 1. Hardware iPhone 3G. Tomado de [23], traducción libre de los autores

Función	Fabricante	Modelo
Unidad central de	Samsung	S5L8900B01 – 412 MHz ARM1176Z(F)-

[2] Reproductor de música creado por Apple Inc., caracterizado por ser una biblioteca multimedia digital [28].

procesamiento (CPU)		S RISC, 128 Mbytes of stacked, package-on-package, DDR SDRAM
Aceleración Gráfica 3D	Tecnologías Imagination	Power VR MBX Lite
Amplificador de potencia UMTS	TriQuint	TQM676031 – Band 1 – HSUPA TQM666032 – Band 2 – HSUPA TQM616035 – Band 5/6 WCDMA/HSUPA PA-duplexer
Transceptor UMTS	Infineon	PMB 6272 GSM/EDGE and WCDMA PMB 5701
Procesador Base	Infineon	X-Gold 608 (PMB 8878)
Memoria base de apoyo	Numonyx	PF38F3050M0Y0CE - 16 Mbytes of NOR flash y 8 Mbytes of pseudo-SRAM
Amplificador de cuatro bandas GSM / EDGE	Skyworks	SKY77340 (824- to 915-MHz)
Antena GPS, Wi-fi y BT	NXP	OM3805, a variant of PCF50635/33
Gestor de comunicaciones	Infineon	SMARTi Power 3i (SMP3i)
Gestor a nivel de sistema	NXP	PCF50633
Cargador de batería / controlador USB	Tecnología Linear	LTC4088-2
GPS	Infineon	PMB2525 Hammerhead II
Flash NAND	Toshiba	TH58G6D1DTG80 (8 GB NAND Flash)
Chip flash serial	SST	SST25VF080B (1 MB)
Acelerómetro	ST Microelectronics	LIS331 DL
Wi-Fi	Marvell	88W8686
Bluetooth	CSR	BlueCore6-ROM
Codec de audio	Wolfson	WM6180C
Controlador de la pantalla táctil	Broadcom	BCM5974
Interfaz de enlace con la pantalla	National Semiconductor	LM2512AA Mobile Pixel Link
Controlador de línea de pantalla táctil	Texas Instruments	CD3239

Dos de los componentes más importantes del iPhone son:

- *Unidad central de procesamiento (CPU):* es una unidad de procesamiento RISC[3] (Conjunto de Instrucciones Reducidas) que ejecuta el núcleo de los procesos del iPhone y trabaja conjuntamente con el coprocesador PowerVR para la aceleración de gráficos. La CPU ejecuta a una tasa de reloj más baja que la especificada por el fabricante, se ejecuta a 412 MHz de 667 MHz posibles, esto para extender la vida útil de la batería [23].
- *Procesador Base:* es el componente del iPhone que gestiona todas las funciones que requieren la antena (servicios celulares). El procesador base

[3] Es un tipo de microprocesador con las siguientes características fundamentales: Instrucciones de tamaño fijo y presentadas en un reducido número de formatos. Sólo las instrucciones de carga y almacenamiento acceden a la memoria por datos.

tiene su propia memoria RAM[4] y firmware en flash NOR[5], como recurso de la CPU principal. El Wi-Fi y el Bluetooth son gestionados por la CPU principal a pesar que el procesador base almacena su dirección MAC en su NVRAM[6] [23].

El esquema de partición del disco de un iPhone se asemeja a un Apple TV[7]. Por defecto el iPhone está configurado con dos particiones de disco que no residen en una unidad de disco física, debido a que utiliza una NAND flash[8] de estado sólido que es tratada como un disco de almacenamiento. Allí se almacenan una tabla de particiones y un formato de sistema de archivos [5] [9]. La primera partición se conoce como Master Boot Record[9] (MRB), responsable de cargar el sistema operativo. Esta partición es de solo lectura para conservar el estado de fábrica durante todo el ciclo de vida del iPhone, y es donde se encuentran todas las aplicaciones que vienen por defecto en el iPhone. A continuación existe un área libre conocida como Apple_Free area, seguida de la segunda partición que se divide en dos: una parte HFSX[10] que en un principio almacena el sistema operativo, otra área libre Apple_Free area y la segunda parte HFSX que contiene todos los datos de usuario, donde se almacena música, videos, fotos, información de contactos, entre otros [5] [9].

Los orígenes del iPhone provienen del iPod y del Apple TV, que cuentan con dos particiones: una únicamente para operación y otra únicamente para almacenamiento. Aunque el esquema de partición es diferente, los sistemas de archivos son similares en su estructura [9]. El tamaño de la primera partición esta generalmente entre los 300MB y los 500MB, y usa el sistema de archivos HFSX. Esta partición es la encargada de cargar el sistema operativo del iPhone, el iPhone OS, el cual es una variante del núcleo del sistema operativo OS X de Apple. Basado en el mismo núcleo MACH y compartiendo algunos elementos básicos con el sistema operativo OS X 10.5 (Leopard), el iPhone se compone de 4 capas, incluyendo el sistema operativo básico, el núcleo API de servicios, los medios de comunicación y una capa de cacao resistente [23].

El tamaño de la segunda partición, en un iPhone de 16GB es de 14.1GB, en uno de 8GB es de 7.07GB. Dicha partición, contiene el sistema de archivos HFSX y un volumen llamado “Data”, donde la mayoría de la información y de datos de valor se aloja y puede ser localizada [9].

---

[4] Memoria de acceso aleatorio desde donde el procesador recibe las instrucciones y guarda los resultados.

[5] Memoria que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos.

[6] La memoria de acceso aleatorio no volátiles un tipo de memoria que no pierde la información almacenada al cortar la alimentación eléctrica.

[7] El Apple TV permite escuchar los temas de iTunes, visualizar fotos en HD y visualizar podcasts gratuitos. http://www.apple.com/es/appletv/whatis.html [22]

[8] Memorias que usan un túnel de inyección para la escritura y para el borrado un túnel de ‘soltado’. Permiten acceso secuencial (más orientado a dispositivos de almacenamiento masivo).

[9] Sector de almacenamiento de datos que contiene código de arranque de un sistema operativo almacenado en otros sectores del disco.

[10] Es un sistema de archivos desarrollado por Apple Inc [25].

3 Problemas de seguridad en el iPhone 3G

Como se mencionó en la sección anterior, el iPhone 3G es un dispositivo móvil celular que presenta múltiples funcionalidades, por tal razón, está sujeto a sufrir ataques que cualquier otro tipo de teléfono celular puede recibir. Pero, el limitado conocimiento sobre el aseguramiento del dispositivo es el que abre la posibilidad a vulnerabilidades conocidas o desconocidas, las cuales pueden ser aprovechadas por los intrusos. En la actualidad no existe una taxonomía detallada que especifique que tipo de ataques puede sufrir un iPhone 3G, sin embargo, se han identificado algunos ataques, los cuales se describirán a continuación.

Según [14], "*este tipo de dispositivos móviles no están expuestos solamente a ataques de "código malicioso"; existen otros tipos de amenazas como son los ataques directos, la intercepción de la comunicación y los ataques de autentificación*". Los ataques de código malicioso o malware son algún tipo de software que se ejecuta en el dispositivo sin que el usuario se de cuenta, algunos ejemplos son los troyanos y gusanos. Los ataques directos, los cuales no son efectivos para todos los dispositivos móviles, consisten en que el perpetrador es capaz de localizar el dispositivo para vulnerarlo [20]. Generalmente este tipo de ataques se realiza utilizando Bluetooth y una serie de herramientas, como GhettoTooth, BTScanner y BlueScan, que identifican el dispositivo, ejecutan el ataque mediante una serie de técnicas como BlueJacking, BlueSpam, BlueSnarfing, BlueBug, BlueSmac y BackDoor, y por último ejecuta algún comando para obtener datos, cargar datos o cambiar la configuración del dispositivo. La intercepción de la comunicación consiste en que el perpetrador se conecta a los dispositivos o redes para obtener información. Por último, están los ataques de autenticación como el spoofing (suplantación de identidad) y sniffing (captura de tramas de la red) [11]. "*Blue MAC Spoofing es el nombre de uno de los ataques que realizan suplantación de identidad en Bluetooth. Este escenario combina varias de las técnicas nombradas anteriormente en los ataques directos debido a que involucra varias fases tales como emparejamiento, descubrimiento de dispositivos, suplantación de identidad (BlueSmac) y transferencia de archivos sin confirmación"*. [14]

Además de los ataques comunes para dispositivos móviles, el iPhone 3G esta sujeto a ser víctima de otro tipo de ataques por contar con un sistema operativo similar al de un computador [41]. Actualmente se han identificado otros tipos de ataque sobre este dispositivo. Uno es conocido como 'Jailbreak', es decir, el firmware original del dispositivo es reemplazado con un firmware alternativo o "hackeado" que libera el dispositivo evitando las restricciones puestas por el fabricante. Este firmware contiene paquetes de instalación que permiten instalar herramientas para manejar el dispositivo de acuerdo a las necesidades [9]. Para ello existen herramientas que realizan el 'Jailbreak' como Pwnage Tool [30] y Quickpwn [10].

"Un experto en seguridad ha descubierto que la técnica denominada "URL Spoofing" puede ser utilizada en las aplicaciones de correo y navegación web del iPhone, lo que puede provocar ataques de phishing en este dispositivo." [31]. Esto es que un atacante puede simular que una página web maliciosa tenga el aspecto y funcionalidades de una web válida, y así aprovecharse instalando algún tipo de malware.

Considerando lo anterior y entendiendo la estructura lógica del iPhone los rastros de un ataque se pueden obtener en la segunda partición. Según [5] otro tipo de datos que se almacenan en esta partición además de la música, videos, fotos y contactos, y que pueden llegar a ser evidencia en una investigación dada son:

- Caches de teclado, nombres de usuario, contraseñas, términos de búsqueda y fragmentos de documentación tecleada.
- Pantallazos del último estado de una aplicación son preservados cuando el botón Home es presionado o cuando se cierra alguna aplicación.
- Fotos eliminadas de la librería y de la memoria.
- Direcciones, contactos, eventos de calendario y otros datos personales.
- Historial de llamadas, además de las que se despliegan, las ultimas 100 llamadas y entradas eliminadas.
- Imágenes de mapas de Google Maps y búsquedas por longitud/latitud de coordenadas.
- Cache del buscador y objetos eliminados del buscador que identifican que sitios web fueron visitados.
- Correos electrónicos eliminados, mensajes de texto, marcas de tiempo y banderas de comunicación (con quien y en que dirección la comunicación tuvo lugar).
- Grabaciones de correo de voz eliminadas.
- Información entre el dispositivo y el computador relacionado.

4 Informática forense en Teléfonos Inteligentes

La informática forense aplicada a dispositivos móviles y especialmente a teléfonos inteligentes, es un área de investigación relativamente nueva. Es por esto que existe poca literatura sobre el tema, y más aún en lo relacionado con la atención de incidentes [14]. A continuación explicaremos que es la informática forense y la importancia de su aplicación en dispositivos móviles como el iPhone 3G.

4.1 Informática forense clásica

El constante aprovechamiento de fallas sobre los sistemas de computación por parte de agentes mal intencionados, ofrece un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos [32], estos agentes malintencionados varían según sus estrategias y motivaciones, que abarcan desde lucro monetario hasta satisfacción personal, y en algunos casos es un estilo de vida [33].

Con respecto a lo citado anteriormente, según [32], la criminalística ofrece un espacio de análisis y estudio sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones criminales, por lo tanto, es necesario establecer un conjunto de herramientas, estrategias y acciones que ayuden a identificar estos hechos y evidencias dentro del contexto informático [42].

La informática forense es una rama de las ciencias forenses, que involucra la aplicación de la metodología y la ciencia para identificar, preservar, recuperar, extraer, documentar e interpretar [5] pruebas o evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos encontrados en la escena del crimen [36], para luego usar dichas evidencias como elemento material probatorio en un proceso judicial [34] [14].

Con respecto a lo anterior según [32] podemos considerar la evidencia como "cualquier información, que sujeta a la intervención humana u otra semejante, ha sido extraída de un medio informático". La evidencia digital tiene como características principales el hecho de ser volátil, anónima, duplicable, alterable y eliminable, en consecuencia, a diferencia de la evidencia física en un crimen clásico, la evidencia digital es un desafío para aquellas personas que la identifican y analizan debido a que se encuentran en un ambiente cambiante y dinámico [43] [46].

Por consiguiente, se hace necesaria la aplicación de procedimientos estrictos y cuidadosos, desde el momento en que se realiza la recolección de la evidencia, hasta que se obtienen los resultados posteriores a la investigación [14] [38], por tal razón a continuación se muestra un modelo generalizado para realizar este tipo de investigaciones.

1. *Identificación de la escena del crimen:* en esta fase se hace el reconocimiento del incidente con el objetivo de identificar el tipo de crimen [36]. Es primordial tener precauciones para evitar la contaminación de la escena de esta fase en adelante [39].
2. *Preparación:* en esta fase se realiza la preparación de herramientas, técnicas, órdenes de registro y autorizaciones para acceder a la escena del crimen [36].
3. *Preservación de la escena del crimen:* en esta fase se realiza el aislamiento de la evidencia física y digital del mundo externo, es decir, de personas no autorizadas y dispositivos electromagnéticos [36].
4. *Recolección de la evidencia:* en esta fase se realiza la recolección de toda la evidencia encontrada en la escena del crimen, empezando por la más volátil hasta la menos volátil, es importante que al momento de realizar la inspección de (los) equipo (s) evitar alterar cualquier variable ya que un cambio a la vista insignificante podría invalidar todo el proceso de investigación en un proceso judicial. Por otro la recolección debe ser realizada mediante herramientas especializadas y certificadas con el objetivo de evitar modificaciones en las fechas de acceso y en la información del registro del sistema [35] [38] [40].
5. *Preservación de la evidencia:* es importante que durante todo el proceso de investigación forense la evidencia conserve sus propiedades con las que fue recolectada para evitar que pierda su valor de carácter legal, por lo tanto, es primordial realizar toda la investigación sobre copias exactas de la evidencia obtenida en la escena del crimen, comprobando periódicamente la integridad de dicha copia [35]. Por otro lado es necesario actualizar la cadena de custodia de la evidencia cada vez que esta cambie de responsable, este documento debe contar con la información de donde, cuando y quien manejo la evidencia, quien la custodia y en donde esta almacenada [37] [38] [40].
6. *Análisis de la evidencia:* el objetivo de esta fase es lograr identificar como fue efectuado el ataque, cual fue la vulnerabilidad explotada y en lo posible identificar al atacante [40], para lograr lo anterior es necesario reconstruir la

secuencia temporal del ataque, para lo cual se debe recolectar la información de los archivos asociados, marcas de tiempo, permisos de acceso y estado de los archivos.

7. *Presentación del informe forense:* Finalmente culmina la investigación y en este paso se presentan los resultados por parte del investigador sobre su búsqueda y análisis de los medios, lo que se encontró en la fase de análisis de la evidencia, así como información puntual de los hechos y posibles responsables [44]. Debido al rigor que requiere una investigación de este tipo, cada movimiento por parte del investigador o su equipo de trabajo se debe documentar hasta que se resuelva o se dé por concluido el caso. Esta documentación se debe llevar a cabo por medio de formularios que hacen parte del proceso estándar de investigación, entre los cuales se encuentran el documento de custodia de la evidencia nombrado en el numeral 5 de esta sección, el formulario de identificación de equipos y componentes, el formulario de incidencias tipificadas, el formulario de recogida de evidencias y el formulario de medios de almacenamiento [14].

Luego de realizar las fases del modelo anterior según [5] y [35], para que la evidencia digital pueda ser usada en procesos judiciales debe cumplir con las siguientes características:

- *Admisibilidad:* toda evidencia recolectada debe ajustarse a ciertas normas jurídicas para presentarlas ante un tribunal.
- *Autenticidad:* la evidencia debe ser relevante al caso, y el investigador forense debe estar en capacidad de representar el origen de la misma.
- *Completitud:* la evidencia debe contar todo en la escena del crimen y no una perspectiva en particular.
- *Fiabilidad:* las técnicas usadas para obtener la evidencia deben gozar de credibilidad y aceptadas en el campo en cuestión, evitando dudas sobre la autenticidad y veracidad de las evidencias.
- *Entendimiento y Credibilidad:* se debe explicar con claridad y pleno consentimiento, que proceso se siguió en la investigación y como la integridad de la evidencia fue preservada, para que esta sea comprensible y creíble en el tribunal.

4.2 Informática forense en iPhone 3G

El objetivo principal de la informática forense aplicada a dispositivos móviles, al igual que el objetivo de la informática forense clásica como se mencionó anteriormente, es la búsqueda y recolección de información relacionada con un incidente en el cual se pueda encontrar posible evidencia digital incriminatoria, y esta sea utilizada como elemento material probatorio en un proceso judicial [14]. Actualmente, el 80% de los casos en procesos judiciales contienen algún tipo de evidencia digital [2], razón por la cual el proceso de recolección y el valor de la evidencia resulta ser de vital importancia.

Sin embargo, y debido a que el mercado de la telefonía móvil inteligente se ha incrementado primordialmente por la variedad de fabricantes y modelos de teléfonos que existen, la heterogeneidad que se presenta tanto en su configuración de hardware,

su sistema operativo y tipo de aplicaciones que manejan, como en las herramientas adoptadas para recuperar contenidos que se puedan utilizar en una investigación forense, es bastante significativa [12] [47]. En la mayoría de los casos, los fabricantes de dispositivos móviles optan por crear y aplicar sus propios protocolos para uso de sus sistemas operativos y cables, ocasionando que para los analistas forenses sea más difícil realizar una investigación por la variedad de herramientas que existen para cada tipo de dispositivo [2] [14].

Es por esto que para que se logre un análisis forense digital confiable, y la evidencia que se recoja logre ser admisible, auténtica, completa, fiable, entendible y creíble, es importante conservar los lineamientos presentados en la sección 4.1, añadiendo parámetros concernientes a la manipulación de teléfonos móviles celulares, y los puntos que pueden variar dependiendo del fabricante y modelo [13].

Hoy en día, como ya se ha mencionado, existe poca literatura sobre el análisis forense en dispositivos móviles y específicamente sobre el iPhone. Sin embargo, se han desarrollado herramientas y algunas técnicas forenses no formales para llevar a cabo dicho proceso.

Como en cualquier investigación forense, existen variedad de enfoques que se pueden utilizar para la recolección y análisis de información [13]. Un aspecto clave para ello, por no decir el más importante, es que el procedimiento que se siga, no modifique la fuente de información de ninguna manera, o que de ser esto absolutamente necesario, el analista esté en la capacidad de justificar por qué realizó esta acción [23]. Según [23], existen tres técnicas diferentes para la recolección de evidencia sobre un iPhone:

1. *Obtener datos directamente del iPhone*: este enfoque es preferible a la recuperación archivos desde el computador con el que el iPhone se sincronizó. Sin embargo, el analista forense debe entender cómo ocurrió la adquisición de información, si el iPhone fue modificado en algún aspecto y qué tipo de información no se logró adquirir.
2. *Obtener una copia de respaldo o una copia lógica del sistema de archivos del iPhone utilizando el protocolo de Apple*: esta aproximación consiste en la lectura de archivos del iPhone, mediante el protocolo de sincronización de Apple, el cual solo es capaz de obtener archivos explícitamente sincronizados a través de el. Piezas claves de información son almacenadas en bases de datos de tipo SQLite, las cuales son soportadas por el protocolo. Hacer consultas sobre estas bases de datos generará la recuperación de información como mensajes de texto y correos electrónicos eliminados del dispositivo.
3. *Una copia física bit a bit*: este proceso crea una copia física bit a bit del sistema de archivos del iPhone, de manera similar al procedimiento que se sigue sobre computadores personales. Este proceso, de todos los anteriores, es el que más potencial tiene para recuperar información, incluyendo los datos eliminados, pero resulta ser complicado pues requiere que se modifique la partición del sistema del iPhone.

Según [5], el proceso técnico que se debe seguir para realizar un análisis forense sobre un iPhone, debe seguir fuertemente los lineamientos nombrados en la sección 4.1, y consta de cuatro pasos que se describen a continuación:

1. *Manipulación física*: Es el paso más importante antes de examinar el dispositivo, ya que se debe contar con el equipo adecuado para mantener el

dispositivo cargado y conectado. Se debe retirar la tarjeta SIM o bloquear cualquier tipo de comunicación o alteración que pueda sufrir el dispositivo mediante una jaula de Faraday que bloquee los campos eléctricos alrededor de él, incluyendo las transmisiones celulares [12].

2. *Establecer comunicación*: este paso consiste en organizar las conexiones físicas y de red apropiadas para instalar una herramienta forense y realizar la recuperación de información.
3. *Recuperación forense*: extraer la información original para crear una copia y trabajar sobre ella. Esto requiere revisiones de integridad para evitar alteraciones de datos.
4. *Descubrimiento electrónico*: es el proceso en el cual toda la información extraída es procesada y analizada. Durante esta etapa, los archivos eliminados son recuperados y el sistema de archivos es analizado, para la recolección de evidencia.

Para llevar a cabo el proceso anteriormente descrito, se han desarrollado de igual manera herramientas que permiten la extracción de información del dispositivo, y se ha hecho un enfoque del equipo necesario que se requiere para ello [15]:

- Un computador ejecutando el sistema operativo Mac OS X Leopard ó Windows XP. Algunas de las herramientas que existen hasta el momento funcionan sobre Mac OS Tiger y Windows Vista pero no han sido probadas en su totalidad sobre estos sistemas, por lo cual no se garantiza que la extracción de datos sea completa.
- Un cable de tipo USB para instalar las herramientas de recuperación, y mantener el dispositivo cargado.
- Una implementación de SSH en el computador incluyendo ssh y scp, para establecer comunicación con el dispositivo.
- Una instalación en el computador de iTunes 7.6 o 7.7 dependiendo del firmware del iPhone en cuestión. De igual manera versiones superiores deberían funcionar correctamente.
- Espacio adecuado en el computador, para almacenar las copias del sistema de archivos del iPhone. Se recomienda reservar un espacio de mínimo tres veces la capacidad del iPhone en cuestión.

Una vez se cree un ambiente más confiable que limite la contaminación cruzada sobre las copias del sistema de archivos obtenidas, se debe contar con una herramienta para su análisis. Existen variedad de herramientas para este propósito cada una con características y propiedades diferentes. A continuación describiremos algunas de las que existen en la actualidad según [23] [45].

1. *WOLF de Sixth Legion*: Es una herramienta forense diseñada específicamente para el iPhone. Soporta todos los modelos, 2G y 3G, que ejecutan cualquier versión de firmware desde la 1.0 hasta la 2.2. Este software solo se puede ejecutar sobre el sistema operativo Mac OS X, y es capaz de eludir el código de seguridad tanto del dispositivo como el de la tarjeta SIM, si se tiene acceso al computador en el que fue usado el iPhone, sin necesidad de realizar el "Jailbreak" (descrito en la sección 3). WOLF no modifica el iPhone para realizar la adquisición de información ya que usa una copia de la lógica de datos, sin embargo una desventaja es que no recuperar contenido suprimido del dispositivo.

2. *Cellebrite UFED*: El sistema forense Cellebrite UFED es un dispositivo autónomo (stand-alone), capaz de adquirir datos desde dispositivos móviles y almacenar la información en una unidad USB, tarjeta SD[11] o PC. UFED incorpora un lector y generador de copias de tarjetas SIM. La posibilidad de clonar una tarjeta SIM es una potente característica que puede crear e insertar un clon de la tarjeta SIM original y el teléfono funcionará con normalidad. Sin embargo, no se registrará con el operador de telefonía móvil de la red, eliminando la necesidad de bolsas de Faraday y la posibilidad de que los datos del teléfono sean actualizados o eliminados. El paquete viene con alrededor de 70 cables para conectar a la mayoría de los dispositivos móviles disponibles en la actualidad. Incluyen protocolos de conexión serial, USB, infrarrojos y Bluetooth. Permite extraer información de contactos, mensajes de texto, historial de llamadas, mensajes de texto eliminados, grabaciones, video, fotos y detalles del teléfono entre otros.
3. *MacLockPick II (MLP)*: Esta herramienta tiene un enfoque único para la adquisición forense. El objetivo de MLP es proporcionar una solución de plataforma cruzada forense que realiza una adquisición en vivo de una máquina sospechosa. La información se almacena en un dispositivo USB y el software se proporciona para analizar los resultados. MLP no funciona directamente en el iPhone, en su lugar se centra en el directorio de copia de seguridad MDBACKUP donde se almacenan la gran mayoría de los archivos. Entre los datos que son recuperables se encuentran el historial de llamadas, mensajes de texto, contactos, notas, fotos, cuentas de correo sincronizadas, entradas rápidas de marcación, estado, historial y bookmarks del navegador y detalles del teléfono, entre otros.

5 Conclusiones

Se ha evidenciado que si bien el investigador forense tiende a seguir una metodología para realizar un análisis, frecuentemente la aparición de nuevas tecnologías y la heterogeneidad que estas presentan, no permiten que el seguimiento sea estricto y que varíen los procedimientos que se utilizan. Por otra parte, la variedad de herramientas de análisis de datos que existen y sus diferentes niveles de confiabilidad, presentan características particulares que facilitan o dificultan algunas actividades necesarias en el proceso de análisis de datos.

Este documento establece un conjunto de elementos conceptuales y aplicados sobre el dispositivo móvil iPhone 3G, perteneciente a una de las áreas que requiere hoy en día más investigación y profundización [14], debido a que los procedimientos y las normas para su análisis aún se encuentran en desarrollo, y al crecimiento tecnológico y popularidad alcanzada. En la segunda fase de la investigación se propondrá una guía metodológica que defina el proceso especializado en la obtención de detalles de incidentes ocurridos en un iPhone 3G, además de probar escenarios reales en incidentes de seguridad informática sobre el dispositivo.

[11] Es un formato de tarjeta de memoria flash utilizado en dispositivos portátiles.

6 Referencias

1. Mellar, B.; Forensic Examination of Mobile Phones. Digital Investigation – Elsevier. United Kingdom. (2004), http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf
2. Rossi, M.: Internal Forensic Acquisition for Mobile Equipments. Dipartimento di Informatica, Sistemi e Produzione, Università di Roma "Tor Vergata". (2008).
3. Canalys, Expert Analysis for High-tech Industry.: Smart Mobile Device Shipments hit 118 Million in 2007, up 53% on 2006. Singapore and Reading (UK) (2008). http://www.canalys.com/pr/2008/r2008021.htm.
4. Canalys, Expert Analysis for High-tech Industry.: Global Smart Phone Shipments Rise 28%". Reading (UK) (2008). http://www.canalys.com/pr/2008/r2008112.htm.
5. Zdziarski, J.: iPhone Forensics, Recovering Evidence, Personal Data & Corporate Assets. O'Reilly Media, Inc. (2008)
6. CSI, Computer Security Institute, http://www.gocsi.com/
7. CSI.: Computer Crime and Security Survey: The latest results from the longest-running project of its kind. (2008). http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
8. Castillo, C., Romero, A.: Guía Metodológica Para el Análisis Forense Orientado a Incidentes en Dispositivos Móviles GSM. Pontificia Universidad Javeriana. (2008).
9. Varsalone, J., Kubasiak, R.: Mac Os X, iPod and iPhone Forensic Analysis DVD Toolkit. Syngress Publishing, Inc, pp. 355-475. (2009)
10. Jailbreak iPhone and iPod Touch Games and More.: www.quickpwn.com
11. Bluetooth SIG.: Funcionamiento de la Tecnología Bluetooth. http://spanish.bluetooth.com/Bluetooth/Technology/Works/Default.htm
12. Willassen, S.: Forensic analysis of mobile phone internal memory. Norwegian University of Science and Technology. http://digitalcorpora.org/corpora/bibliography_files/Mobile%20Memory%20Forensics.pdf
13. Agualimpia, C., Hernández, R.: Análisis Forense en Dispositivos Móviles con Symbian OS. Documento de maestría, Dept. Ingeniería electrónica, Pontifica Universidad Javeriana. http://www.criptored.upm.es/guiateoria/gt_m142e1.htm.
14. Castillo, C., Romero, A., Cano, J.: Análisis Forense Orientado a Incidentes en Teléfonos Celulares GSM: Una Guía Metodológica. Conf. XXXIV Conferencia Latinoamericana de Informática, Centro Latinoamericano de Estudios en Informática (CLEI). (2008). http://www.clei2008.org.ar/
15. Baggilo, I., Milan, R., Rogers, M.: Mobile Phone Forensics Tool Testing: A Database Driven Approach". International Journal of Digital Evidence. Purdue University, Volume 6 Issue 2. (2007). http://www.utica.edu/academic/institutes/ecii/publications/articles/1C33DF76-D8D3-EFF5-47AE3681FD948D68.pdf
16. Vogelstein, F.: The Untold Story: How the iPhone Blew Up the Wireless Industry. WIRED, Wired Magazine: Issue 16.02. (2008). http://www.wired.com/gadgets/wireless/magazine/16-02/ff_iphone?currentPage=all
17. Penalva, J.: Historia del iPhone. Xataca, (2008). http://www.xataka.com/moviles/historia-del-iphone
18. Product Reviews.: The Apple iPhone Story: 1999 to 2008. (2008). http://www.product-reviews.net/2008/08/01/the-apple-iphone-story-1999-to-2008/
19. Dumas, D.: iPhone Timeline Highlights the Handset Through The Ages. WIRED. (2008). http://blog.wired.com/gadgets/2008/07/iphone-timeline.html,
20. Hackers pueden entrar a tu iphone mediante OpenSSH. Crackea tu iPhone. (2008). http://crackeatuiphone.com/2008/09/19/hackers-pueden-entrar-a-tu-iphone-mediante-openssh/#more-1523

21. Apple Inc.: Especificaciones iPhone 3G. (2009). http://www.apple.com/es/iphone/specs.html
22. Apple Inc.: Qué es iTunes. (2009). http://www.apple.com/es/itunes/whatis/
23. Hoog, A.: iPhone Forensics: Annual Report on iPhone Forensic Industry. Chicago Electronic Discovery. (2009).
24. Apple Inc.: iPhone 3G: Gallery. (2009). http://www.apple.com/iphone/gallery/
25. Macedonia, M.: iPhones Target the Tech Elite. Entertainment Computing, pp. 94-95. (2007).
26. Grossman, L.: Invention Of the Year: The iPhone. TIME in partnership with CNN. http://www.time.com/time/specials/2007/article/0,28804,1677329_1678542,00.html
27. Apple Inc.: iPhone 3G: Caracteristicas. (2009). http://www.apple.com/la/iphone/features/
28. Apple Inc.: iPod Classic. (2009). http://www.apple.com/la/ipodclassic/features.html
29. Apple Inc.: Apple introduce el Nuevo iPhone 3G: dos veces más rápido y a mitad de precio. Sala de prensa. (2009). http://latam.apple.com/pr/articulo/?id=1486
30. Spiner, T.: Crackers Claim iPhone 3G Hack, A group of developers has claimed to have cracked the iPhone 3G. ZDNet. (2008). http://news.zdnet.co.uk/security/0,1000000189,39446756,00.htm
31. Pastor, J.: El iPhone Vulnerable al Phishing. The Inquirer. http://www.theinquirer.es/2008/07/25/el_iphone_vulnerable_al_phishing.html
32. Cano, J.: Introducción a la informática forense: Una disciplina técnico-legal. Revista Sistemas, Asociación Colombiana de Ingenieros de Sistemas (ACIS). Vol.96, pp. 64-73. (2006). http://www.acis.org.co/fileadmin/Revista_96/dos.pdf
33. Cano, J.: Computación Forense: Conceptos Básicos.
34. Del Pino, S.: Introducción a la informática forense. Pontificia Universidad Católica del Ecuador. (2007). http://www.criptored.upm.es/guiateoria/gt_m592b.htm.
35. Brezinski, D., Killalea, T.: Guidelines for Evidence Collection and Archiving. IETF RFC 3227. (2002). http://www.ietf.org/rfc/rfc3227.txt
36. Reith, M., Clint, C., Gunsch G.: An Examination of Digital Forensic Models. International Journal of Digital Evidence, Air Force Institute of Technology, Volume 1 Issue 3. (2002). www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.
37. Baryamureeba, V., Tushabe, F.: The Enhanced Digital Investigation Process Model. Institute of Computer Science, Makerere University. (2004).
38. Meyers, M., Rogers, M.: Computer Forensics: The Need for Standardization and Certification. International Journal of Digital Evidence, CERIAS, Purdue University, Volume 3 Issue 2. (2004). www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.
39. International Organization on Computer Evidence.: Guidelines for best practice in the forensic examination of digital technology. IOCE Best Practice Guide V1.0. (2002). http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html
40. Delgado, M.: Análisis Forense Digital. Hackers y Seguridad, 2nd ed. (2007) http://www.criptored.upm.es/guiateoria/gt_m335a.htm
41. Sher, M., Magedanz, T.: 3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model. (2007).
42. Leigland, R.: A Formalization of Digital Forensics. International Journal of Digital Evidence. University of Idaho. Volume 3, Issue 2. (2004). http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2-8F98-8F7597844CF74DF8.pdf
43. DFRWS.: A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS). (2001). http://www.dfrws.org/2001/dfrws-rm-final.pdf

44. Bem, D., Huebner. E.: Computer Forensic Analysis in a Virtual Environment. International Journal of Digital Evidence. Volume 6, Issue 2. (2007). http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf
45. Geiger, M.: Evaluating Commercial Counter-Forensic Tools. Carnegie Mellon University. Digital Forensic Research Workshop (DFRWS). (2005). http://dfrws.org/2005/proceedings/geiger_couterforensics.pdf
46. IOCE: Guidelines For Best Practice in the Forensic Examination of Digital Technology. http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html
47. Adelstein. F.: MFP: The Mobile Forensic Platform. International Journal of Digital Evidence. Volume 2. Issue 1. (2003). http://www.utica.edu/academic/institutes/ecii/publications/articles/A066554D-DCDD-75EE-BE7275064C961B5D.pdf