Análisis Forense Orientado a Incidentes en Teléfonos Celulares GSM: Una Guía Metodológica

Carlos Castillo, Andrés Romero, y Jeimy Cano

Departamento de Ingenieria de Sistemas, Pontificia Universidad Javeriana,
Carrera 7 No. 40 – 62, Bogotá, Colombia
{carlos-castillo, romero.r, j.cano}@javeriana.edu.co

Resumen. El presente artículo propone una guía metodológica para realizar análisis forenses orientados a incidentes en dispositivos móviles GSM. Presenta la situación actual de la seguridad informática de dichos dispositivos, evidenciando su susceptibilidad frente a fallas de seguridad y los impactos en los mismos. Describe los modelos generales de un análisis forense, su aplicación sobre los dispositivos móviles particularmente GSM, especificando herramientas de software disponibles (licenciadas y de código abierto), así como los procedimientos y estándares utilizados a la fecha**.** Presenta algunas limitaciones que tienen los dispositivos móviles en la actualidad, que generan dificultades al practicar análisis forenses en dichos dispositivos. Finalmente propone la guía metodológica que permite obtener evidencias digitales de incidentes ocurridos en teléfonos celulares GSM.

Palabras clave: Informática forense, seguridad informática, procedimientos, estándares, GSM, teléfonos celulares, metodología, herramientas.

1 Introducción

Desde hace algunos años, se ha presentado un crecimiento importante en la utilización de dispositivos móviles en la vida diaria [1] dado que permiten llevar datos personales de forma práctica, fácil y cómoda. Estos datos son, en muchos casos, objetivo de personas mal intencionadas, que aprovechando las vulnerabilidades que presentan este tipo de dispositivos, son capaces de acciones no autorizadas, generalmente con fines ilegales**.**

El Instituto de Seguridad Informática CSI (*Computer Security Institute*) [2] publica cada año un reporte llamado "*CSI Computer Crime and Security Survey*" [3] que expone la situación actual de la seguridad informática y del crimen informático ofreciendo estadísticas basadas en la experiencia de múltiples organizaciones en los Estados Unidos. Dicho reporte proporciona una visión de los incidentes de seguridad más frecuentes en los EE.UU, los cuales representan un número importante a nivel mundial, sin considerar los que no son detectados por los expertos en seguridad de las distintas compañías [3]. Como dato importante del reporte es pertinente resaltar que el 61% de los encuestados intenta realizar la identificación del perpetrador, para ello se

hace necesario recurrir a los procedimientos dispuestos por la informática forense, para recuperar y recolectar la evidencia digital del sistema vulnerado e identificar la acción realizada y demás detalles del ataque efectuado. Por otra parte, el 29% de los encuestados reportó el incidente a las autoridades correspondientes, lo cual sugiere un procedimiento previo de identificación y recolección de evidencia digital de manera oportuna, dada la volatilidad de la misma [3].

Si lo anterior es correcto, la práctica de la informática forense, se convierte en una disciplina emergente en las ciencias forenses, como garante de la verdad en los procesos donde la administración de justicia valore elementos materiales probatorios de carácter tecnológico. Al ser los dispositivos móviles los elementos tecnológicos de mayor demanda en el mercado, particularmente los teléfonos celulares, se vuelven un objetivo claro de las mentes criminales para materializar sus acciones delictivas.

De acuerdo con estadísticas del sector de teléfonos móviles, para el 2005 el número de teléfonos celulares en el mundo era de 2.168'433.600 [4], para julio de 2006, el número ascendía a 2.4 billones de teléfonos, con un estimado de más de 1.000 nuevos clientes cada minuto según el Washington Post [5]. De otra parte, Nokia proyectaba que para finales de 2007 existirían más de tres billones de usuarios de telefonía celular [5]. Otros datos establecen que China tiene 461 millones de usuarios de telefonía celular lo cual representa el 35% de su población total mientras que, en comparación, Estados Unidos tiene 219 millones de usuarios de telefonía celular, lo cual representa el 73% de su población según Time [5]. Finalmente, 32% de la población de América Latina usan la telefonía celular según el Banco Mundial [5].

En cuanto a la proporción del mercado entre las diferentes marcas de teléfonos celulares y las mayores empresas de este gremio tecnológico [6], encontramos que el mayor fabricante de teléfonos celulares en el mundo, con 900 millones de dispositivos vendidos en el 2006 [5] es Nokia, además con el mayor margen de ganancias en el mercado actual, seguido en crecimiento a través de los años por Sony Ericsson, Samsung, LG y Motorola. Esto es en cuanto a margen de ganancias pero en cuanto a porcentaje del mercado en el 2007, Nokia controla el 36,2% del mercado, seguido por un 18% de Motorola, un 13,8 de Samsung y un 8,7% de Sony Ericsson Mobile Communications [7]. En éste escenario de masificación de las comunicaciones móviles con el uso intensivo de la telefonía celular en prácticamente todo el planeta, estamos ante una realidad emergente de la inseguridad de la información, la cual se manifiesta en un crecimiento exponencial de plagas informáticas que ahora se concentran en los dispositivos móviles [8]. Si bien las vulnerabilidades informáticas son frecuentes en la computación de oficina y las prácticas propias de los usuarios de los hogares; ahora el nuevo escenario de inseguridad informática que deben comprender todos los usuarios es el que sugiere la telefonía móvil y la integración de servicios que avanza rápidamente en este tipo de dispositivos. En consecuencia, los incidentes de seguridad que se presenten en este escenario "sin cables", requieren un entendimiento más detallado de dichas tecnologías y mayores esfuerzos de investigación para comprender las conductas de los atacantes en este tipo de comunicaciones inalámbricas.

2 Informática Forense

Es una rama de las ciencias forenses que pretende enfocar los estándares y

procedimientos establecidos para ser empleados en una investigación de crímenes e incidentes en el análisis de datos y evidencia digital, utilizando herramientas tecnológicas de extracción y análisis las cuales facilitan dicha labor [9]. El objetivo general de la misma es efectuar el estudio de cualquier tipo de evidencia digital que se encuentre involucrada en un incidente, con el fin de lograr que ésta cobre valor probatorio lo cual conlleva a que sea admisible en el momento de entablar procesos judiciales [9]. Actualmente, el campo de las ciencias forenses digitales se encuentra en un proceso de metamorfosis: está cambiando de una simple destreza a una verdadera ciencia forense [10]. Con este cambio, es imperante entender la base científica de la disciplina. Para realizarlo, los investigadores a través de los años, han construido varios modelos de investigación los cuales han reflejado una serie de observaciones que han contribuido con el proceso de metamorfosis antes mencionado.

Un buen modelo de investigación de informática forense debe ajustarse a una serie de principios entre los cuales se encuentran [11]: Considerar el sistema en su totalidad, conservar la información de registro a pesar de que el sistema falle totalmente, considerar los efectos de los eventos; no solo las acciones que los causan, tener en cuenta el contexto para ayudar a la interpretación y el entendimiento del significado de un evento y presentar los eventos de manera en que puedan ser analizados y entendidos por un analista forense.

Luego de comprender la base científica de la informática forense, se vislumbra la necesidad de conocer y entender los procedimientos y estándares a seguir para efectuar un análisis forense. En una investigación forense de carácter digital, se pueden seguir los patrones de una investigación forense de carácter estándar; sin embargo, dado lo sensible de la evidencia en esta rama de investigación, se hace necesaria la aplicación de procedimientos más cuidadosos, desde el momento en que se recolecta la evidencia, hasta que se obtienen resultados posteriores a la investigación [13]. A continuación se expone un procedimiento estándar que permite efectuar una investigación forense digital procurando fortalecer la admisibilidad y validez de las evidencias digitales encontradas en el contexto del incidente, con el fin de presentarlas como elementos materiales probatorios en un proceso jurídico.

2.1 Recolección de Evidencia

En esta fase del procedimiento, lo primero que se debe realizar es un análisis del sistema o periférico que posiblemente se encuentre involucrado en el incidente. Para ello, se deben tener en cuenta algunos pasos que pueden llevar a determinar si existió algún tipo de acción sobre el elemento implicado. Entre los más destacados y eficientes están [12]: La revisión de logs del sistema, la revisión de listados de usuarios conectados al sistema, la búsqueda de archivos faltantes o modificados, la revisión de las políticas de seguridad del sistema y la búsqueda de puertas traseras abiertas del sistema y vulnerabilidades del mismo. Para realizar las recolecciones es necesario tener en cuenta el estado en que se encuentra el dispositivo contenedor de la posible evidencia, es decir, si el dispositivo se encuentra encendido o apagado y, en lo posible, mantenerlo en ese estado con el fin de que no se produzcan cambios sobre las posibles evidencias del atacante que se puedan identificar sobre memoria volátil [14].

2.2 Preservación de la Evidencia

Este paso no es tan crucial como el paso inicial, sin embargo, de no hacer una preservación de los datos y dispositivos de una manera rigurosa, es posible que la evidencia pierda su carácter de admisibilidad desde el punto de vista legal [15]. Es importante resaltar que en el proceso de preservación se debe tener cierto rigor en el momento de manipulación de evidencia por parte de agentes externos. Para esto es necesario documentar y tener en cuenta los siguientes pasos a la hora de tener cualquier tipo de interacción con la evidencia [12]: Sin importar quién sea la persona que transporte o tenga a cargo la evidencia, se deben registrar los datos personales, los datos de la organización que lleva la investigación a cabo, el cargo que tiene la persona en la organización, las acciones que se realizaron con la evidencia, a qué hora se realizó la acción, etc. De igual manera se debe llevar a cabo el mismo proceso cuando se haga un cambio de custodia de la evidencia, es decir, un traspaso.

El anterior procedimiento se conoce como cadena de custodia. De esta manera, la evidencia puede mantenerse confiable y segura en un alto porcentaje, sin embargo, no está exenta de cambios sobre ella debido a sucesos que estén fuera de estas consideraciones tales como fenómenos climáticos y/o electromagnéticos [12], por lo cual también se debe considerar el medio en que se transporta y se preserva la información [9].

2.3 Análisis de la Evidencia

En esta fase de la investigación se puede encontrar un volumen importante de información lo cual puede consumir una cantidad considerable de tiempo en la realización de la misma, especialmente en procesos como la identificación de acciones puntuales. Seguramente en este paso del procedimiento se requerirá el uso de una herramienta forense especializada para evitar que se produzcan cambios en la evidencia original y, por otro lado, para facilitar el trabajo del investigador proporcionando agilidad y rapidez en el análisis de grandes cantidades de información. Antes de trabajar sobre el análisis de la evidencia, es importante tener en cuenta lo siguiente [12]: Saber por dónde se va a comenzar, en términos de ubicación física de archivos clave y establecer una línea de tiempo que debe comprender el posible instante en el cual ocurrió el incidente, así como el momento en que se tuvo conocimiento del mismo. También se debe trabajar en lo posible sobre copias exactas de la evidencia original, comprobadas a través de funciones hash como MD5 o SHA1.

Una vez realizado lo anterior, lo ideal sería que los análisis realizados sobre los datos de evidencia se llevaran a cabo en un sistema idéntico al original donde ocurrió el incidente. Lo anterior con el fin que no se produzcan alteraciones sobre la evidencia original y que el trabajo realizado sea confiable debido al entorno; esto se conoce como preparación del entorno de trabajo [12].

2.4 Presentación de un 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, etc. Debido al rigor que una investigación de este tipo requiere, 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 [12], entre los cuales se encuentran: El documento de custodia de la evidencia, 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.

3 Problemas de Seguridad en Teléfonos Celulares GSM

La mayoría de personas en la actualidad tiene un dispositivo móvil, sin embargo, numerosos virus han venido apareciendo especialmente para infectar teléfonos celulares. Estos se han venido convirtiendo en el objetivo preferido por los atacantes debido a las vulnerabilidades y a la poca protección con que cuentan [17]. Sin embargo, los 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 [16]. Entre los ataques de código malicioso se encuentra principalmente el *malware* tales como troyanos y gusanos [18]. El gusano Cabir fue la primera pieza notable de *malware* para teléfonos celulares. Dicho virus usa la tecnología *Bluetooth* para auto-enviarse a todos los contactos de la agenda del teléfono celular [17].

Por otro lado, una de las formas en las que un dispositivo móvil se puede vulnerar es realizando un ataque directo en el cual un *hacker* puede localizar el dispositivo y tomar acciones deliberadas para vulnerarlo [16]. Lo primero que se debe realizar es encontrar el teléfono celular que utiliza *Bluetooth*. Existe una gran cantidad de herramientas gratuitas están disponibles para realizar estos pasos entre las que se encuentran GhettoTooth [19], BTScanner [20] y BlueScan [21]. Seguidamente se procede a identificar el dispositivo utilizando las mismas herramientas nombradas en el paso anterior. A continuación se utiliza la herramienta para atacar el objetivo. Entre las técnicas que existen para vulnerar el dispositivo se encuentran BlueJacking [22], BlueSpam [23], BlueSnarfing [24], BlueBug [16], BlueSmac [16] y BackDoor [16]. No todos los dispositivos son vulnerables a estos ataques. Es por esto que existe una tabla que muestra varias marcas y modelos de teléfonos celulares y a qué tipo de ataques son susceptibles [25]. Finalmente se ejecuta un *exploit* o comando para obtener datos, cargar datos o cambiar la configuración del dispositivo.

Algunas veces la forma más fácil para atacar un dispositivo es hacerlo de forma indirecta. Una gran variedad de dispositivos actualmente son capaces de conectarse a otros dispositivos o redes a través de numerosos métodos. Es ésta comunicación la cual puede ser vulnerada y usada para propósitos malintencionados [16]. Uno de los ataques más famosos de interceptación de comunicación es llamado *Car Whisperer*

[26] y consiste en la interceptación de la comunicación que se produce entre un manos libres Bluetooth y el dispositivo vulnerado.

Finalmente existen ataques que atentan sobre los mecanismos de autentificación, entre ellos se encuentran el *spoofing* y el *sniffing* los cuales, combinados con la tecnología *Bluetooth*, pueden llegar a comprometer de manera importante la información que se encuentra en el dispositivo. *Blue MAC Spoofing* [27] 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. Desde luego este último escenario es uno de los más completos en cuanto a ataque a teléfonos celulares se refiere, debido a que reúne una gran variedad de técnicas y herramientas las cuales permiten el acceso no autorizado al dispositivo utilizando tecnología *Bluetooth*.

4 Informática Forense en Teléfonos Celulares GSM

La informática forense aplicada a dispositivos móviles es una ciencia relativamente nueva debido a la popularidad que han tenido estos dispositivos a nivel mundial. El objetivo de la misma, al igual que en la informática forense clásica, es la búsqueda y recolección de información relacionada con un incidente en el cual se pueda encontrar posible evidencia digital incriminatoria y sea utilizará como elemento material probatorio en un proceso judicial. Esta búsqueda y recolección de información, presenta algunas diferencias con relación a si ésta se realiza en dispositivos móviles o en otros sistemas. Si se tiene en cuenta que los dispositivos móviles GSM varían con relación a otros sistemas digitales, como por ejemplo, los computadores personales, tanto en su configuración de hardware, como en su sistema operativo y el tipo de aplicaciones que manejan [14]; se entiende la importancia de conservar los lineamientos definidos en el capítulo 2 del presente documento con relación a los procedimientos y estándares para realizar un análisis forense digital confiable, agregando brevemente algunos puntos específicos referentes al manejo de teléfonos celulares.

4.1 Recolección de Evidencia

Esta fase del procedimiento inicia con la búsqueda de componentes asociados al teléfono tales como módulos de memoria que se encuentren fuera del dispositivo, accesorios, etc. Como se mencionó en el procedimiento definido en la parte 2, es necesario tener en cuenta el estado del dispositivo, es decir, si se encuentra encendido o apagado, y en lo posible, mantenerlo de esa manera, a fin de que no se produzcan cambios en la evidencia digital y se conserve su carácter de admisibilidad. Otra razón del por qué se debe mantener el estado del dispositivo radica en que especialmente los teléfonos celulares GSM poseen mecanismos de seguridad al momento de iniciar el dispositivo, tales como el ingreso del código PIN de la SIM card, lo cual facilita el acceso al teléfono debido a que usualmente no se cuenta con dichos códigos de acceso y, por lo tanto, evita la labor de evadir dichos mecanismos [14].

Otro aspecto importante es el poder recolectar oportunamente la información acerca de las conexiones realizadas desde y hacia el dispositivo, mensajes de datos, etc., que por lo general, se mantiene en memoria no volátil, realizando un aislamiento de cualquier tipo de medio de comunicación que pueda alterar dicha información, como por ejemplo la red celular.

4.2 Preservación de Evidencia

Como se mencionó anteriormente, es imperante mantener la integridad de la evidencia digital procurando aislar el dispositivo de todas las conexiones entrantes y manteniendo el suministro de energía constante con el fin de evitar la pérdida de datos de la memoria volátil. [14]. Además es necesario tener en cuenta que es recomendable utilizar un medio físico para la adquisición de los datos, tales como un cable de conexión punto a punto, debido a que las comunicaciones inalámbricas pueden verse afectadas por interacciones externas que pueden conllevar a la modificación de la posible evidencia digital recolectada [14].

4.3 Análisis y Reportes de la Evidencia

En cuanto a la fase de análisis de la evidencia, se puede seguir como estándar los lineamientos proporcionados en la sección concerniente a la informática forense clásica en este mismo documento; sin embargo, se debe centrar la atención en información puntual como es [28]: IMEI, mensajes de texto, ajustes, idioma, fecha, tono, grabaciones de audio, archivos, llamadas entrantes y números marcados, listado de programas ejecutables iniciados recientemente, calendario, GPRS, WAP y ajustes de la conexión a Internet. En cuanto a la generación de reportes de investigación, lo expuesto en la parte 2.4 del presente documento aplica sin ningún cambio.

Para llevar a cabo con éxito y de forma eficiente las anteriores fases del proceso de análisis forense, es recomendable, en lo posible, utilizar un conjunto de herramientas forenses especialmente diseñadas para funcionar con dispositivos móviles. En la actualidad una gran variedad de herramientas forenses para un rango de dispositivos discriminado, típicamente, por las distintas plataformas del fabricante, por la familia del sistema operativo o por el tipo de arquitectura del hardware del dispositivo [9]. Entre las herramientas forenses comerciales se encuentran: Paraben's cell seizure [29], MOBILedit! Forensic [30], Oxygen Forensic Suite [31], .XRY [32], PhoneBase2 [33] y Secure View Kit for Forensics [34]. Finalmente existe una herramienta libre para realizar análisis forenses en dispositivos móviles, su nombre es TULP2G [35] aunque no está desarrollada por completo y se encuentra actualmente en una fase muy temprana como para ser utilizada en procedimientos rigurosos.

5 Guía metodológica para realizar análisis forense orientado a incidentes en teléfonos celulares GSM

5.1 Fase de Preparación

El propósito de ésta fase es planear y preparar todos los elementos necesarios para efectuar con éxito el proceso de análisis forense orientado a incidentes: personal, el

kit de herramientas forenses y el dispositivo en sí. Entre las actividades que se realizan en este momento de la investigación se encuentran: Definir el equipo de trabajo con el que se va a abordar el caso, establecer roles y responsabilidades para cada uno de los miembros del equipo de trabajo, identificar y documentar todos los componentes electrónicos que no se van a incautar, recolectar todos los elementos no electrónicos relacionados con el dispositivo, realizar una entrevista al propietario del dispositivo, identificar el dispositivo, aislar el dispositivo de la red GSM, crear el registro de la cadena de custodia, documentar toda interacción con el dispositivo, tomar una foto o un video que exhiba el estado inicial del dispositivo, determinar las herramientas forenses a utilizar y documentar la/las herramienta/s escogida/s. Los resultados esperados de la fase son: Obtener el equipo de trabajo capacitado, establecido con roles y responsabilidades asignados, asegurando la preservación de la evidencia. También se debe tener realizada la incautación y documentación de todos los elementos electrónicos y no electrónicos relacionados con el dispositivo, registro de identificación del teléfono celular y su estado inicial. Además de esto, se debe tener la documentación de toda interacción con el dispositivo en la cadena de custodia. Finalmente, se debe tener la definición y documentación del conjunto de herramientas escogidas para realizar el análisis forense.

5.2 Fase de recolección de datos

El propósito de la fase es recolectar la mayor cantidad de información posible del dispositivo conservando la integridad y, por tanto, admisibilidad de la posible evidencia digital encontrada en la fase siguiente de la metodología. Entre las actividades que se realizan en este momento del proceso se encuentran: Obtener la imagen de datos, verificar la integridad de la imagen de datos, crear una copia de la imagen de datos y asegurar la imagen suministrada. Finalmente el resultado de esta fase es la imagen de datos del dispositivo (copia bit a bit de memoria volátil y no volátil del dispositivo, incluyendo la SIM Card, si la adquisición es física. Si la adquisición es lógica, se debe obtener toda la información del dispositivo concerniente a lista de contactos, historial de mensajes, historial de llamadas etc..

5.3 Fase de análisis de datos

El propósito de la fase es identificar tanto datos lógicos (historial de llamadas y mensajes de texto entre otros) como físicos (procesos en memoria, logs entre otros) para construir una línea de tiempo en donde se correlacionen todos los hechos y se pueda obtener la mayor cantidad de detalles del incidente ocurrido. Entre las actividades que se realizan en este momento de la investigación se encuentran: Identificar el sistema de archivos, recuperar los datos borrados, recuperar la información escondida, realizar el análisis de datos lógicos, realizar el análisis de datos físico (identificar procesos en ejecución, revisar logs del sistema e identificar rastros de conexiones), analizar archivos obtenidos y construir la línea de tiempo definitiva. Finalmente el resultado de esta fase es la línea de tiempo definitiva con todos los hechos correlacionados junto con el conjunto de evidencias digitales obtenidas halladas durante el proceso.

5.4 Fase de reporte de hallazgos

El propósito de la fase es documentar todas las acciones, eventos y hallazgos obtenidos durante el proceso. La actividad general consiste en construir el reporte final (identidad de miembros del equipo de trabajo, cadena de custodia, hallazgos, herramientas utilizadas, descripción de pasos) y, finalmente, el resultado es el documento con toda la información concerniente al caso.

6 Conclusiones

La informática forense es un campo que poco a poco ha ido evolucionando, sin embargo, tiene aún muchas áreas por investigar y explotar [10]. Por tanto, este documento establece un conjunto de elementos conceptuales y aplicados sobre dispositivos móviles GSM como una respuesta a una de las áreas que requiere hoy por hoy más investigación y profundización, dado el crecimiento tecnológico que se presenta actualmente. La presente guía metodológica constituye la definición de un proceso especializado en la obtención de detalles de incidentes ocurridos en teléfonos celulares GSM. En la segunda fase de la investigación se probará a la luz de escenarios reales en incidentes de seguridad informática sobre teléfono celulares GSM y así afinar dicha guía basada en la experiencia práctica prevista.

Referencias

1. Barrie, M.: Forensic examination of mobile phones. http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf, Teddington United Kingdom (2004) 266-272
2. CSI Computer Security Institute; http://www.gocsi.com
3. CSI. Computer Crime and Security Survey. http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf (2007) 1-23
4. Infoplease.: Cell Phone Usage Worldwide, by Country. http://www.infoplease.com/ipa/A0933605.html (2007)
5. The Globalist.: Cell Phones and Globalization. http://www.theglobalist.com/globalicons/syndication/sample.htm
6. Mobile User Experience.: What happened to handset industry margins in Q307?. http://www.pmn.co. uk/images/q307marginsm.jpg
7. INFOBAE.: Nokia y Samsung le quitan porción de mercado a Motorola. http://tecnologia.infobaeprofesional.com/notas/44978-Nokia-y-Samsung-le-quitan-porcion-de-mercado-a-Motorola.html (2007)
8. Perry, C.: The Emerging Mobile Malware Threat. http://securityrenaissance.com/wordpress//wordpress/wp-content/uploads/2007/01/mobilemalware.pdf (2006)
9. Oscar, L., Haver, A., Ricardo, L., Beatriz, A.: Informática Forense: Generalidades, aspectos técnicos y herramientas. http://www.criptored.upm.es/guiateoria/gt_m180b.htm 1-16
10. Mark, P.: An Ad Hoc Review of Digital Forensic Models. National Center for Forensic Science, Department of Engineering Technology, University of Central Florida, 1 (2007)
11. Sean, P., Matt, B., Sidney, K., Keith, M.: Toward Models for Forensic Analysis. In Proceedings of the Second International International Workshop on Systematic approaches to digital forensic engineering.
12. Miguel, L.: Análisis Forense Digital. http://www.criptored.upm.es/guiateoria/gt_m335a.htm 10-24

13. Rian, A., Wayne, J.: Guidelines on CellPhone Forensics. National Institute of Standards and Technology Special Publication. http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
14. Amber, S.: Handheld Forensics. http://www.syngress.com/book_catalog/SAMPLE_1597491381.pdf
15. Christian, F.: An Analysis of the Integrity of Palm Images Acquired with PDD, School of Computer and Information Science, Edith Cowan University, Bradford Street, Mt Lawley, Western Australia. http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-2.pdf
16. Daniel, H.: Blackjacking. Wiley Publishing, USA, cap. 4 (2007)
17. Benny, R.: Mobile Phone Security. East Carolina University. http://www.infosecwriters.com/text_resources/pdf/Phones_BRayner.pdf 1-5
18. Shaharudin, I., Zahri, Y.: Worms and Trojans go mobile. National ICT Security and Emergency Response Centre. http://www.cybersecurity.org.my/data/content_files/13/91.pdf?.diff=11764168431-2
19. Dual. ghettotooth.pl. http://www.oldskoolphreak.com/tfiles/ ghettotooth.txt
20. PenTest: BTScanner. http://www.pentest.co.uk/cgi-bin/viewcat.cgi?cat=downloads
21. Devianizado: BlueScan. Scanner de dispositivos Bluetooth. http://debianizado.net/bluescan
22. BlueJackq: Mobile Phone BlueJacking. http://www.bluejackq.com
23. Collin, M.: BlueSpam. http://www.mulliner.org/palm/bluespam.php
24. Alighieri: Bluesnarfer. http://www.alighieri.org/project.html
25. The Bunker: Bluetooth. http://www.thebunker.net/resources/bluetooth
26. Alberto, M.: Car Whisperer. http://gospel.endorasoft.es/bluetooth/seguridad-bluetooth/car-whisperer. html (2007)
27. Carlos, C., Jose, G., Edgar, T.: Blue MAC Spoofing: El Backdoor de Bluetooth. http://www.criptored.upm.es/guiateoria/gt_m14 2c1.htm (2007)
28. Svein, Y.: Forensics and the GSM mobile telephone system. International Journal of Digital Evidence Volume 2 Issue 1. http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf 10-11 (2003)
29. Paraben Corporation: Device Seizure v2.0. http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=405 (2008)
30. COMPELSON LABORATORIES: MOBILEedit! Forensic. Revolutionary Forensic Software for Mobile Phone Investigation. http://www.mobiledit.com/forensic (2008)
31. OXYGEN SOFTWARE: Oxygen Forensic Suite - mobile phone forensic software. http://www.oxygensoftware.com/es/products/forensic (2008)
32. MICRO SYSTEMATION: .XYR Software. http://www.msab.com/en/Products/XRY--PROGRAMME -SOFTWARE (2008)
33. Envisage Systems: PhoneBase2. http://www.phonebase.info/html/information.html
34. DATAPILOT: Secure View Kit for Forensics. http://www.datapilot.com/productdetail/253/supphones/Notempty (2008)
35. Jeroen, van der B., Ronald van der K.: TULP2G – An Open Source Forensic Software Framework for Acquiring and Decoding Data Stored in Electronic Devices. Netherlands Forensic Institute. International Journal of Digital Evidence. http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A85456-BE75-87F8-E45EB9C6082FDF4E.pdf 2 (2005)