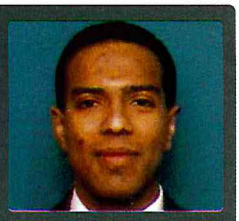
El presente artículo desarrolla una revisión conceptual y de la literatura sobre la informática forense en dispositivos móviles. Para ello presenta la situación actual de la seguridad informática de dichos dispositivos, evidenciando su susceptibilidad frente a fallas de seguridad y los impactos en los mismos. En este contexto, se describen 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) para esta labor, así como los procedimientos y estándares utilizados a la fecha.



POR: MSc. Jeimy Cano[1]

Departamento de Ingeniería de Sistemas
Pontifica Universidad Javeriana
Carrera 7 No. 40 – 62, Bogotá, Colombia
j.cano@javeriana.edu.co

Desde hace algunos años, se ha presentado un crecimiento importante en la utilización de dispositivos móviles en la vida diaria [1] .

El Instituto de Seguridad Informática CSI (Computer Security Institute) [2] publica cada año el reporte "CSI Computer Crime and Security Survey" [3] que expone la situación actual de la seguridad y crimen informático ofreciendo estadísticas basadas en la experiencia de múltiples organizaciones en los Estados Unidos. El reporte recoge los incidentes de seguridad más frecuentes en los EE.UU, pero no los que no son detectados por los expertos en seguridad de las distintas compañías [3].

En el reporte el 61% de los encuestados intenta realizar la identificación del perpetrador, y recurre a los procedimientos de informática forense. 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].

De acuerdo con estadísticas del sector de teléfonos móviles, para el 2005 el número de 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 para finales de 2007 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], el mayor fabricante con 900 millones de dispositivos vendidos en el 2006 [5] es Nokia, seguido por Sony Ericsson, Samsung, LG y Motorola. En el porcentaje del mercado en el 2007, Nokia controla el 36,2%, seguido por un 18% de Motorola, un 13,8 de Samsung y un 8,7% de Sony Ericsson Mobile Communications [7].

En la masificación de las comunicaciones móviles, hay un crecimiento exponencial de plagas informáticas concentradas en dispositivos móviles [8].

2. INFORMÁTICA FORENSE

La informática forense es una rama de las ciencias forenses que enfoca los estándares y procedimientos establecidos 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 es efectuar el estudio de cualquier tipo de evidencia digital involucrada en un incidente, para que ésta cobre valor probatorio y sea admisible en el momento de entablar procesos judiciales [9].

Actualmente, el campo de las ciencias forenses digitales se encuentra cambiando de una simple destreza a una verdadera ciencia forense [10].

El modelo de investigación de informática forense se ajusta a una serie de principios [11]: Considerar el sistema en su totalidad, la información de registro a pesar de que el sistema falle totalmente, los efectos de los eventos, el contexto para ayudar a la interpretación y el entendimiento del significado de un evento y presentar los eventos para ser entendidos por un analista forense.

En la actualidad hay una serie de herramientas para el análisis y recolección de evidencia digital. El uso de ellas es de gran utilidad debido a [9]: La cantidad de datos que se almacenan en un computador, la variedad de formatos de archivo existentes actualmente, la necesidad de recopilar información de manera exacta, la necesidad de verificar que la copia es exacta, las limitaciones de tiempo para analizar la información y la facilidad para borrar archivos de computadores.

Las herramientas forenses protegen la integridad y facilitan la disponibilidad de la información. Los análisis forenses se adelantan a [12]:

- Utilizar de manera correcta y efectiva las herramientas del sistema operativo que se está investigando
- Utilizar un conjunto de herramientas para el análisis de evidencias.

De acuerdo a estas herramientas hay 2 formas de clasificacion:

- Comerciales y no comerciales: En las herramientas comerciales no gratuitas (p.e EnCase [13] de la empresa Guideance Software [14], Access Data Forensic Toolkit 2.0 [15]) como herramientas de código abierto (open source), citamos (p.e The Forensic ToolKit [16], The Sleuth Kit y Autopsy [17], Helix CD [12], F.I.R.E (Forensics and Incident Response Bootable CD) [18])
- De acuerdo a su funcionalidad: hay 4 grupos principales [9]: Herramientas para la recolección de evidencia, para el monitoreo y/o control de computadores [19]), para el marcado de documentos [p.e WatermarkIt [20] o Sandmark [21]) y herramientas de hardware (p.e "Mobile Forensic Workstation" [22]).

En una investigación forense se hace necesaria la aplicación de procedimientos más cuidadosos, desde la recoleccion de la evidencia, hasta la obtencion de resultados posteriores a la investigación [23], a continuación se expone un procedimiento estándar:

[1](M'95, SM'03) es Ing. de Sistemas y Computación de la Universidad de los Andes, graduado del MSc. en Ingeniería de Sistemas y Computación de la misma universidad y Doctor en Filosofía (Ph.D) en la Administración de Negocios de Newport University, Calf. EE.UU. Profesor de Sistemas y Computación de la Universidad de los Andes, así como de la Facultad de Derecho de la misma universidad, donde hace parte del GECTI (Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática). Actualmente, es profesor de cátedra del Dpto. de Ingeniería de Sistemas de la Pontificia Universidad Javeriana en Sg. informática y Comp. Forense. Es miembro de la Red Iberoamericana de Criptología y Seguridad de la Información – CriptoRED.

FOTO: img.alibaba.com/.../Sell_Mobile_N99i.jpg

2.1 Recolección de evidencia

En esta fase del procedimiento, lo primero que se debe realizar es un análisis del sistema o periférico involucrado en el incidente. Para ello, se deben tener en cuenta algunos pasos, entre los más destacados y eficientes están [12]: Revisión de logs del sistema, revisión de listados de usuarios conectados al sistema, búsqueda de archivos faltantes o modificados revisión de las políticas de seguridad del sistema y búsqueda de puertas traseras abiertas del sistema y vulnerabilidades del mismo.

Para realizar las recolecciones es necesario tener en cuenta 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 [24].

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 [25].

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,sin embargo, no está exenta de cambios sobre ella debido a sucesos que estén fuera de estas consideraciones 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 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.
- Establecer una línea de tiempo delinstante en el cual ocurrió el incidente, así como el momento en que se tuvo conocimiento del mismo. 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, los datos de evidencia se llevaran a cabo en un sistema idéntico al original donde ocurrió el incidente, para 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

Es decir lo que se encontró en la fase de análisis de la evidencia, así como información puntual de los hechos y posibles responsables, etc.

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 [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

Un teléfono ya no es más un teléfono y un BlackBerry ya no es más un BlackBerry. Todos estos dispositivos deben ser considerados ahora como "estaciones de trabajo empresariales móviles" [26]. Estos elementos se encuentran en cualquier lugar: en aeropuertos, restaurantes, centros comerciales etc. Cada vez más personas los utilizan, entre ellas empresarios que, gracias a dichos aparatos, pueden mantenerse en contacto con su negocio.

A pesar de que estos dispositivos son, a su vez, teléfonos celulares, en el fondo son realmente computadoras móviles, quecontienen información corporativa sensible que puede ser guardada fácilmente en un bolsillo [26]. Esto, sumado a que la comunicación de estos aparatos es inalámbrica, plantea un gran interrogante en cuanto a seguridad de la información se refiere.

Para entender los problemas y amenazas a las cuales están expuestos los teléfonos celulares, es necesario conocer de forma general las características y funcionalidades de los mismos [27]:

- Los teléfonos móviles están compuestos por un microprocesador, una memoria de sólo lectura (ROM), una memoria de acceso aleatorio (RAM), un modulo de radio, un procesador de señales digitales, un micrófono y un parlante, un teclado y una pantalla de cristal liquido (LCD).
- El sistema operativo del dispositivo se encuentra en la memoria ROM la cual puede ser borrada y re programada electrónicamente con las herramientas apropiadas.
- La memoria RAM, la cual es usada para guardar datos del usuario, es soportada por la batería. Si la batería falla, la información se pierde.
- Los dispositivos más recientes están equipados con varios microprocesadores que reducen el número de chips requeridos para operar el teléfono e incluyen una capacidad de memoria considerable. Otras funcionalidades que tienen es que soportan slots de memorias extraíbles o periféricos especializados tales como wireless (tecnología incluida en el teléfono).
- Los teléfonos móviles se clasifican en : teléfonos básicos los cuales tienen funcionalidades simples como comunicación por voz y mensajes de texto, teléfonos avanzados los cuales tienen funcionalidades adicionales de multimedia y los smarth phones los cuales combinan las capacidades de los teléfonos avanzados con los PDA.

Symbian OS es el más avanzado sistema operativo en la industria de teléfonos móviles de última generación [28]. Fue diseñado para cumplir con los requerimientos de teléfonos que soportan tecnología 2.5G y 3G. Este es el sistema operativo licenciado utilizado por los grandes en telefonia movil como Nokia, Motorola y Sony Ericsson [30].

Con gran variedad de funcionalidades, es un sistema que brinda un buen nivel de desempeño en procesamiento, servicios multimedia, y lo más importante, en seguridad como [28]: El encapsulamiento de datos por parte de las aplicaciones, el uso de algoritmos criptográficos como DES, 3DES, RC2, RC4, RC5 y AES, el soporte para IPSec y clientes VPN, las limitaciones según permisos de usuario, la persistencia de datos a través de una base de datos SQL embebida, el soporte para MIDP 2.0 (Mobile Information Device Profile), el uso de protocolos seguros como HTTPS, SSL y TLS y la capacidad de monitoreo por aplicación.

La mayoría de personas en la actualidad tiene un dispositivo móvil, sin embargo, numerosos virus han venido apareciendo para infectar teléfonos celulares. Estos se han convirtido en el objetivo preferido por los atacantes debido a las vulnerabilidades y a la poca protección con que cuentan [29].

Sin embargo, los dispositivos móviles no están expuestos solamente a ataques de "código malicioso"; considerando lo expuesto, se utilizará el sistema de clasificación de vulnerabilidades en dispositivos móviles propuesto por Hoffman [26]. Hoffman clasifica las diferentes fallas de seguridad identificadas en dispositivos móviles en las siguientes categorías definidas: código malicioso, ataques directos, intercepción de la comunicación, ataques de autenticación y los incidentes en las instalaciones físicas, las cuales son mutuamente excluyentes y convenientes para la presentación de los análisis a continuación.

3.1 Ataques de "código malicioso"

El malware es la amenaza de seguridad mejor conocida actualmente, debido a que incluso los usuarios casuales saben que un programa antivirus es necesario para proteger el computador [26].

Los teléfonos celulares, así como los computadores de escritorio, son vulnerables a amenazas de seguridad tales como troyanos y gusanos [30], los cuales son tipos de malware.

El gusano Cabir está dirigido a dispositivos que tienen el sistema operativo Symbian, entre ellos la serie 60 de Nokia y, en especial, su interfaz de usuario. Una vez el dispositivo se encuentra infectado con el virus, Cabir usa la tecnología Bluetooth para autoenviarse a todos los contactos de la agenda del teléfono celular. El virus se presenta a sí mismo ante los usuarios como "Caribe Security Manager" y se instala mediante el archivo CARIBE.SIS [29].

Al momento de la infección, cuando se ejecuta el archivo de instalación, la pantalla del teléfono celular muestra la palabra "Caribe". Además de esto, el gusano modifica el sistema operativo Symbian del teléfono para que Cabir sea lanzado cada vez que el teléfono celular sea encendido. Luego de realizar la búsqueda de objetivos a infectar mediante Bluetooth, el teléfono envía el archivo "Velasco.sis" el cual contiene el gusano listo para instalar [30].

3.2 Ataques directos

Un hacker localiza el dispositivo y toma acciones para vulnerarlo [26].

Para este tipo de ataque es necesario encontrar el dispositivo e identificarlo. Luego el hacker determinara qué tipo de exploit utilizar contra dicho dispositivo [26].

Uno de los métodos más utilizados para encontrar dispositivos es identificando las señales que son emitidas por éstos [26]. Bluetooth es un buen ejemplo de esta técnica. Si el dispositivo tiene encendido el Bluetooth, con una herramienta que realice sniffing se puede encontrar e identificar dicha señal.

El ataque a un teléfono celular que utiliza Bluetooth involucra los mismos pasos estos son [26]:

1. Encontrar el teléfono celular que utiliza Bluetooth.
2. Identificar el dispositivo.
3. Utilizar la herramienta para atacar el objetivo.
4. Ejecutar un exploit o comando para obtener datos, cargar datos o cambiar la configuración del dispositivo.

Una gran cantidad de herramientas gratuitas están disponibles, GhettoTooth [34] es un script diseñado para ser utilizado en sistemas operativos Linux. El código fuente puede ser descargado desde Internet y compilado para ser utilizado mediante la instrucción perl ghettotooth.pl <hciX> en donde hci es la interfaz de comunicaciones del dispositivo Bluetooth.

BTScanner [35] es también una herramienta basada en Linux aunque, a diferencia de GhettoTooth, no sólo se limita a proporcionar la BD_ADDR y el nombre del dispositivo sino que suministra otros datos importantes como la clase del dispositivo (p.e: Phone/Mobile), los protocolos habilitados, el canal por el que éstos protocolos funcionan, entre otros.

Finalmente, BlueScan [36] es una herramienta muy parecida a BTScanner con la diferencia que se encuentra en español y que tiene una funcionalidad adicional la cual es exportar los resultados de la búsqueda a un archivo.

Luego de encontrar e identificar el dispositivo que se desea vulnerar, el paso siguiente consiste en atacarlo utilizando de serie de técnicas entre los cuales se encuentran [26]: BlueJacking [38], BlueSpam [39], Bluesnarfing [26], BlueBug [26], BlueSmac [26] y BackDoor [26].

No todos los dispositivos son vulnerables a estos ataques, una tabla muestra varias marcas y modelos de teléfonos celulares y a qué tipo de ataques son susceptibles [41].

3.3 Intercepción de la comunicación

Algunas veces la forma más fácil para atacar un dispositivo es hacerlo de forma indirecta. Es ésta comunicación la cual puede ser vulnerada y usada para propósitos malintencionados [26]. Uno de los ataques más famosos es llamado Car Whisperer [26].

La aplicación Car Whisperer [42] fue desarrollada con el objetivo de sensibilizar a los fabricantes de manos libres Bluetooth para automóvil sobre la amenaza de seguridad del emparejamiento automático anteriormente descrito [43]. Ésta herramienta realiza una búsqueda de manos libres Bluetooth. Cuando encuentra el dispositivo, Car Whisperer intenta conectarse y autenticarse utilizando el conocido PIN del fabricante el cual es identificado por los seis primeros caracteres de la dirección MAC del dispositivo [26]. Luego de realizar la conexión, el atacante puede acceder a las funciones de audio implementadas en el terminal y llevar a cabo las siguientes acciones con fines maliciosos [43]:

- Capturar el audio recogido por el micrófono del dispositivo, para escuchar conversaciones privadas en el interior del vehículo.
- Inyectar audio que sería reproducido por los altavoces del dispositivo, lo cual permitiria proyectar mensajes de voz a los ocupantes del vehículo o transporte.

3.3 Intercepción de la comunicación

A veces la forma más fácil de atacar un dispositivo es de forma indirecta. Una gran variedad de dispositivos actualmente son capaces de conectarse a otros dispositivos o redes a través de numerosos métodos. Esta comunicación es la que es vulnerada y usada para propósitos malintencionados [26]. Uno de los ataques más famosos de interceptación de comunicación es el Car Whisperer [26].

La aplicación Car Whisperer [42] se desarrolló con el objetivo de sensibilizar a los fabricantes de manos libres Bluetooth para automóvil sobre la amenaza de seguridad del emparejamiento automático anteriormente descrito [43]. Ésta herramienta realiza una búsqueda de manos libres Bluetooth. Cuando encuentra el dispositivo, Car Whisperer se conecta y autentica con el conocido PIN del fabricante el cual es identificado por los seis primeros caracteres de la dirección MAC del dispositivo [26]. Realizada la conexión, el atacante accede a las funciones de audio implementadas en el terminal y lleva a cabo las siguientes acciones con fines maliciosos [43]:

- Capturar el audio recogido por el micrófono del dispositivo, para escuchar conversaciones privadas en el interior del vehículo.
- Inyectar audio para reproducir por los altavoces del dispositivo, proyectando mensajes de voz a los ocupantes del vehículo.

La aplicación se compone de varios programas los cuales se encargan de [43]: Identificar dispositivos manos libres Bluetooth, utilizar claves PIN estándares para emparejarse con el dispositivo y crear una pasarela de audio estableciendo enlaces SCO para la transmisión de audio en ambas direcciones.

Esta es una vulnerabilidad pero no existe una forma de prevenir este ataque, sólo acudir a la educación y sensibilización de los usuarios.

Existen ataques que atentan sobre los mecanismos de autentificación, como el spoofing y sniffing, los cuales, combinados con la tecnología Bluetooth, comprometen la información en el dispositivo.

Blue MAC Spoofing [44] es el nombre de uno de los ataques que realizan suplantación de identidad en Bluetooth. Este escenario combina varias de las técnicas nombradas en los ataques directos debido a que involucra varias fases [44]:

1. Fase de emparejamiento: El resultado es que los dispositivos poseen una clave común para la conexión, que permite al atacante, realizar conexiones sin autorización del otro dispositivo.
2. Fase de descubrimiento de dispositivos: Consiste en el descubrimiento de dispositivos Bluetooth con cualquiera de las herramientas mencionadas en la sección 3.2.
3. Fase de suplantación de identidad de un dispositivo de confianza: Esta consiste en cambiar la BD_ADDR del dispositivo Bluetooth conectado a un computador portátil con sistema operativo Linux y la pila de protocolos Bluez, utilizando la herramienta bdaddr [45] a la cual se le envían como parámetros la nueva BD_ADDR y el puerto de Bluetooth que usualmente es el hci0.
4. Fase de transferencia del archivo sin necesidad de confirmación: Es el envío de un archivo a través del protocolo OBEX sin necesidad de confirmación o autorización del otro usuario ya que se realizó la suplantación de identidad de un dispositivo Bluetooth de confianza.

"El ataque Blue MAC Spoofing es una vulnerabilidad que explota el estándar mismo y por eso preocupa que se realice ya que al corregirlo se modificar el estándar completo cambiando el firmware de los dispositivos que usen esta tecnología para que no cambie la BD_ADDR."[44]. Este escenario es uno de los más completos en cuanto a ataque a teléfonos celulares, 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 nueva ciencia debido a la popularidad que han tenido estos dispositivos en el mundo. Su objetivo, es la búsqueda y recolección de información vinculada con un incidente en el que se encuentre posible evidencia digital que será prueba en un proceso judicial, y que se mantenga intacta y sea legalmente admisible en esta instancia.

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, por ejemplo, los computadores personales, tanto en su configuración de hardware, como en su sistema operativo y el tipo de aplicaciones que manejan [24]; se entiende la importancia de conservar los lineamientos definidos en la parte 2 con relación a los procedimientos y estándares para un análisis forense digital confiable, agregando algunos puntos específicos al manejo de teléfonos celulares.

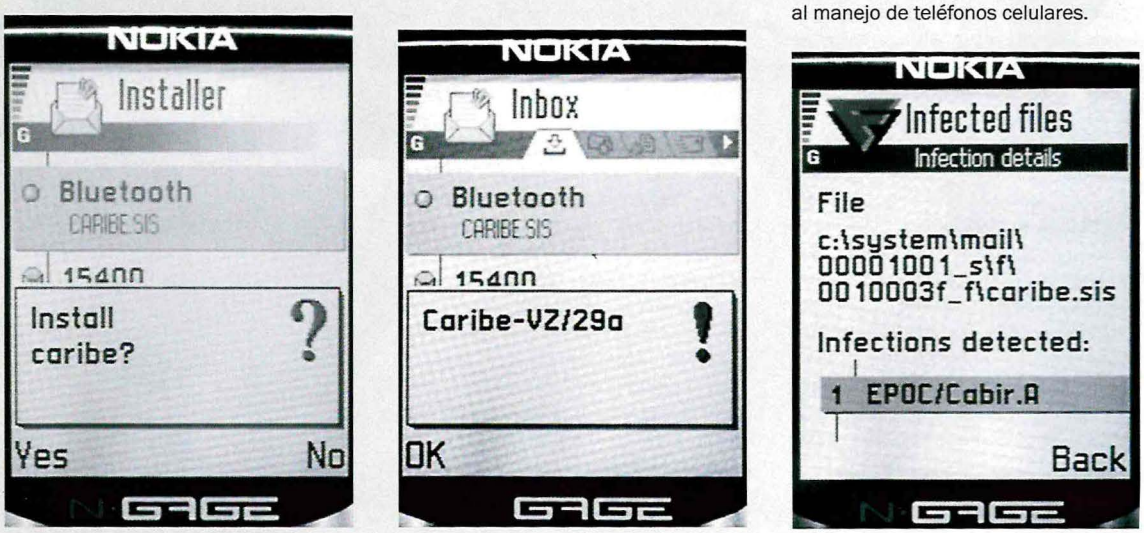


Figura 1. Infección y desinfección del gusano Cabir [31],[32],[33].

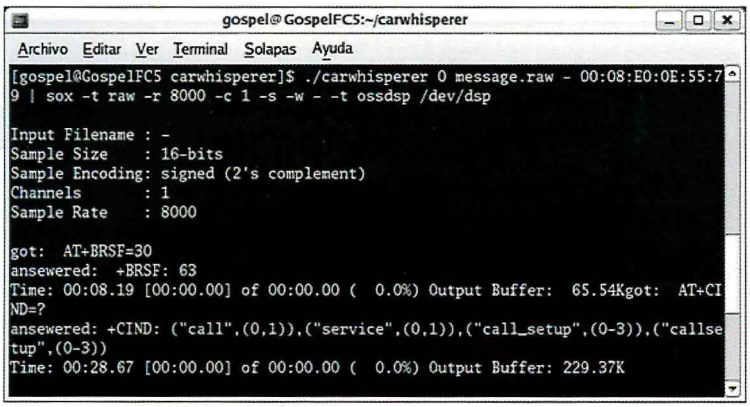


Figura 3. Car Whisperer [43]

4.1 Recolección de evidencia

Se inicia con la búsqueda de componentes asociados al teléfono, como módulos de memoria fuera del dispositivo, accesorios, etc.

Saber el estado del dispositivo, si se encuentra encendido o apagado, en lo posible, mantenerlo apagado a fin de que no se produzcan cambios en la evidencia digital y se conserve su admisibilidad. Por ejemplo los teléfonos celulares GSM poseen mecanismos de seguridad al momento de iniciar el dispositivo, como el ingreso del código PIN de la SIM card, facilitando el acceso al teléfono debido a que no cuenta con dichos códigos de acceso y, por tanto, evita la labor de evadir dichos mecanismos. [24].

Recolectar oportunamente la información de las conexiones realizadas desde y hacia el dispositivo, mensajes de datos, etc., que está en la memoria no volátil, realizando un aislamiento de cualquier tipo de medio de comunicación que no altere dicha información, ejemplo: la red celular.

4.2 Preservación de evidencia

Figura 2. BTScanner [37].

Hay que mantener la integridad de la evidencia digital aislando el dispositivo de todas las conexiones entrantes y manteniendo el suministro de energía constante para evitar la pérdida de datos de la memoria volátil. [24], y usar un medio físico para la adquisición de los datos, como un cable de conexión punto a punto, debido a que las comunicaciones inalámbricas son afectadas por interacciones externas que conllevan a la modificación de la posible evidencia digital recolectada [24].

4.3 Análisis y reportes de la evidencia

La fase de análisis de la evidencia se centra en atención a información puntual como es [46]: IMEI, mensajes de texto, ajustes, idioma, fecha, tono, GPRS, WAP, ajustes de la conexión a Internet, etc.

Las anteriores fases del proceso de análisis forense se realizan, utilizando un conjunto de herramientas forenses diseñadas para funcionar con dispositivos móviles, por la familia del sistema operativo o por el tipo de arquitectura del hardware del dispositivo [9].

Entre las herramientas forenses comerciales tenemos: Paraben's cell seizure [47], MOBILedit! Forensic [48], Oxygen Forensic Suite [49], .XRY [50],

PhoneBase2 [51] y Secure View Kit for Forensics [52].

Estas herramientas requieren un conocimiento detallado para su uso [53], exigen que el investigador tenga completo acceso al dispositivo, que no esté protegido por ningún mecanismo de autenticación [54]. Finalmente la herramienta para realizar análisis forenses en dispositivos móviles, el TULP2G [55], se encuentra en una fase temprana.

5. CONCLUSIONES

La informática forense ha ido evolucionando, tiene aún muchas áreas por investigar y explotar [10]. Este documento establece un conjunto de elementos conceptuales y aplicados sobre dispositivos móviles GSM, y es la base para proponer una guía metodológica para realizar análisis forenses orientados a incidentes en teléfonos celulares GSM.

▼ Referencias bibliográficas

[1] Mellar, B., (2004), "Forensic examination of mobile phones", Digital Investigation – Elsevier, pp. 266-272. Disponible en: http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf

[2] CSI Computer Security Institute; http://www.gocsi. com

[3] CSI. (2007). Computer Crime and Security Survey. pp. 1-23. Disponible en: http://i.cmpnet.com/v2.gocsi. com/pdf/CSISurvey2007. pdf

[4] Infoplease, "Cell Phone Usage Worldwide, by Country",2007; http://www.infoplease.com/ipa/ A0933605.html

[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 Q3077"; http://www.pmn.co.uk/images/q307marginsm.jpg

[7] INFOBAE, "Nokia y Samsung le quitan porción de mercado a Motorola", Abr. 2007; http://tecnologia. infobaeprofesional.com/notas/44978-Nokia-y-Samsung-le-quitan-porBE75-87F8-E45EB9C6082FDF4E.pdf

[8] Carpenter, P., (2006, Nov.), "The Emerging Mobile Malware Threat", pp. 1. Disponible en: http://securityrenaissance.com/wordpress//wordpress/wpcontent/uploads/2007/01/mobilemalware.pdf

[9] López, O., Amaya, H., León, H., Acosta, B., (2002, Feb.), "Informática Forense: Generalidades, aspectos técnicos y herramientas", pp. 1-16. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m180b. htm

[10] Pollit, M., "An Ad Hoc Review of Digital Forensic Models". National Center for Forensic Science, Department of Engineering Technology, University of Central Florida, pp. 1, 2007.

[11] Peisert, S., Bishop, M., Karin, S., Marzullo, K., "Toward Models for Forensic Analysis", In Proceedings of the Second International International Workshopon Systematic approaches to digital forensic engineering (SADFE'07), pp. 2, 2007.

[12] López, M., (2006, Jun.), "Análisis Forense Digital", pp. 10-24. Disponible en: http://www. criptored.upm.es/guiateoria/gt_m335a.htm

[13] "How EnCase Forensic Works", 2007; http:// www.encase.com/products/ef_works.aspx

[14] "EnCase Forensic. Guideance Software", 2007; http://www.guidancesoftware.com/products/ef_index .asp

[15] "Forensic ToolKit 2.0. Access Data", 2007; http:// www.accessdata.com/Products/ftk2test.aspx

[16] "The Forensic Toolkit. Foundstone Network Security",2007; http://www.foundstone.com/us/ resources/proddesc/forensictoolkit.htm

[17] Carrier, B., "The Sleuthkit & Autopsy"; http:// www.sleuthkit.org

[18] Salusky, M., F.I.R.E, 2008; http://fire.dmzs.com

[19] BlazingTools Software, "Perfect Keylogger"; http://www.blazingtools.com

[20] Salo Storm Software, "WatermarkIt"; http:// www.watermarksoft.com/index.htm

[21] Collberg, C., "Sandmark"; http://sandmark.cs. arizona.edu/ index.html

[22] DIBS USA INC, "DIBS Mobile Forensic Workstation"; http:// www.dibsusa.com/products/mws. asp

[23] Ayers, R., Jansen, W., (2007, May.), "Guidelines on CellPhone Forensics", National Institute of Standards and Technology Special Publication, pp. 24-25. Disponible en: http://csrc.nist.gov/publications/ nistpubs/800-101/SP800-101.pdf

[24] Schroader, A., "Handheld Forensics", pp. 125-140. Disponible en: http://www.syngress.com/ book_catalog/SAMPLE_159749138 1.PDF

[25] Frichot, C., "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 6050. pp 1-2; http://scissec.scis.ecu.edu.au/publications/ forensics04/Frichot-2.pdf

[26] Hoffman, D., "Blackjacking", Wiley Publishing, USA, cap. 4, 2007.

[27] Radack, S., "Forensic Techniques for Cell Phones", Information Technology Laboratory–NIST, USA, pp. 2, jun. 2007. Disponible en: http://csrc.nist.gov/publications/nistbul/b-June2007.pdf

[28] Symbian, "Symbian OS 9.5", pp. 1-2. Disponible en: http://www.symbian.com/files/rx/file8929.pdf

[29] Rayner, B., "Mobile Phone Security", East Carolina University, pp. 1-5. Disponible en: http://www.infosecwriters.com/text_resources/pdf/Phones_BRayner.pdf

[30] Ismail, S., Yunos, Z., (2005), "Worms and Trojans go mobile", National ICT Security and Emergency Response Centre, pp. 1-2. Disponible en: http://www.cybersecurity.org.my/data/content_files/13/91.pdf?.diff=1 176416843

[31] F-Secure, "Cabir Install Question"; http://www.f-secure.com/weblog/archives/cabir_install_question.jpg

[32] K Saavedra, "Cabir"; http://microasist.com.mx/ gifs/CABIR03.jpg.

[33] F-Secure, "Cabir Desinfect"; http://www.fsecure. com/virus-info/v-pics/cabir_disinfect.jpg

[34] Dual, "ghettotooth.pl"; http://www. oldskoolphreak.com/tfiles/ ghettotooth.txt

[35] PenTest, "BTScanner"; http://www.pentest. co.uk/cgi-bin/viewcat.cgi?cat=downloads

[36] Devianzado, "BlueScan - Scanner de dispositivos Bluetooth"; http://debianizado.net/bluescan

[37] CHW, "btscanner 0.1", 2004; http://www. wardriving.ch/hpneu/ blue/soft.htm

[38] BlueJackq, "Mobile Phone BlueJacking"; http:// www.bluejackq.com

[39] Mulliner, C., "BlueSpam"; http://www. mulliner.org/palm/bluespam.php

[41] The Bunker, "Bluetooth"; http://www. thebunker.net/resources/bluetooth

[42] Trifinite Group, "Car Whisperer"; http://trifinite.org/trifinite_stuff_carwhisperer.html

[43] Moreno, A., "Car Whisperer", 2007; http://gospel.endorasoft.es/bluetooth/seguridad-bluetooth/car-whisperer.html

[44] Castillo, C., Gomez, J., Torres, E., "Blue MAC Spoofing: El Backdoor de Bluetooth"; Nov. 2007; http://www.criptored.upm.es/guiateoria/gt_m142c1.htm

[45] Holtman, M., "bdaddr.c"; http://csourcesearch. net/data/package/bluez-utils/bluez-utils-2.17/test/ bdaddr.c

[46] Yngvar, S., (2003), "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence Volume 2 Issue 1, pp. 10-11. Disponible en: http://www.utica.edu/academic/ institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A2FDF4E.pdf pdf

[47] Paraben Corporation, "Device Seizure v2.0", 2008; http://www.paraben-forensics.com/catalog/ product_info.php?cPath= 25&products_id=405

[48] COMPELSON LABORATORIES, "MOBILEedit! Forensic, "Revolutionary Forensic Software for Mobile Phone Investigation", 2008; http://www.mobiledit.com/forensic.

[49] OXYGEN SOFTWARE, "Oxygen Forensic Suite - mobile phone forensic software", 2008; http://www. oxygensoftware.com/es/products/ forensic

[50] MICRO SYSTEMATION, ".XYR Software", 2008; http://www.msab.com/en/Products/XRY-PROGRAMME-SOFTWARE

[51] Envisage Systems, "PhoneBase2"; http:// www.phonebase.info/html/information.html.

[52] DATAPILOT, "Secure View Kit for Forensics", 2008; http://www.datapilot.com/productdetail/253/supphones/Notempty

[53] Casadei, F., Savoldi, A., Gubian, P., (2006), "Forensics and SIM cards: an Overview", International Journal of Digital Evidence Volume 5 Issue, University of Brescia, pp. 1. Disponible en: http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE3ED05-0AD75-87F8-E45EB9C6082FDF4E.pdf

[54] Ayers, A., Jansen, W., Cilleros, N., Daniellou, R., "Cell Phone Forensic Tools An Overview and Analysis", National Institute of Standards and Technology NIST, Disponible en: http://csrc.nist. gov/publications/nistir/nistir-7250.pdf

[55] Van der Bos, J., Van der Knijff, R., (2005), "TULP2G – An Open Source Forensic Software Framework for Acquiring and Decoding Data Stored in Electronic Devices", Netherlands Forensic Institute, International Journal of Digital Evidence, pp 2. Disponible en: http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A85456-BE75-87F8-E45EB96082FDF4E.pdf