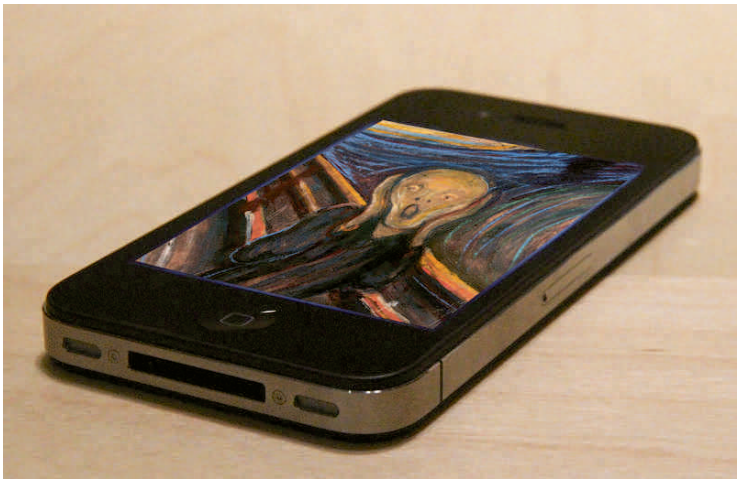
# SEGURIDAD DE DISPOSITIVOS MOVILES

**Riesgos de pérdida de datos en el Apple iPhone y smartphones de otras marcas**

**Francisco Lázaro**

## Smartphones: pasaporte al siglo XXI



Un teléfono móvil no es ni de lejos comparable a la experiencia de poseer un smartphone. En los comienzos de la telefonía móvil estar conectado en todo momento generaba en el usuario una sensación de seguridad y libertad. Lo pudieron comprobar viajantes de comercio, excursionistas, geólogos e innumerables familias expuestas al riesgo de secuestro en las grandes ciudades latinoamericanas. Los smartphones -teléfono, ordenador, agenda electrónica, reproductor de medios y GPS todo en uno-, heredan las servidumbres de la telefonía móvil (mal servicio de las compañías telefónicas, cláusulas abusivas, dispositivos bloqueados), pero la vivencia subjetiva no es la misma. En un iPhone, *Samsung Galaxy* o *HTC*, el usuario literalmente *toca* los datos con los dedos sobre una pantalla que pese a su reducido tamaño comienza ya a tener la definición de un televisor HD. Si el teléfono móvil supuso la culminación de toda la tecnología de telecomunicaciones del siglo XX, los nuevos smartphones, pequeños, compactos, visualmente atractivos y cómodos de manejar, son la tarjeta de presentación para el siglo XXI.

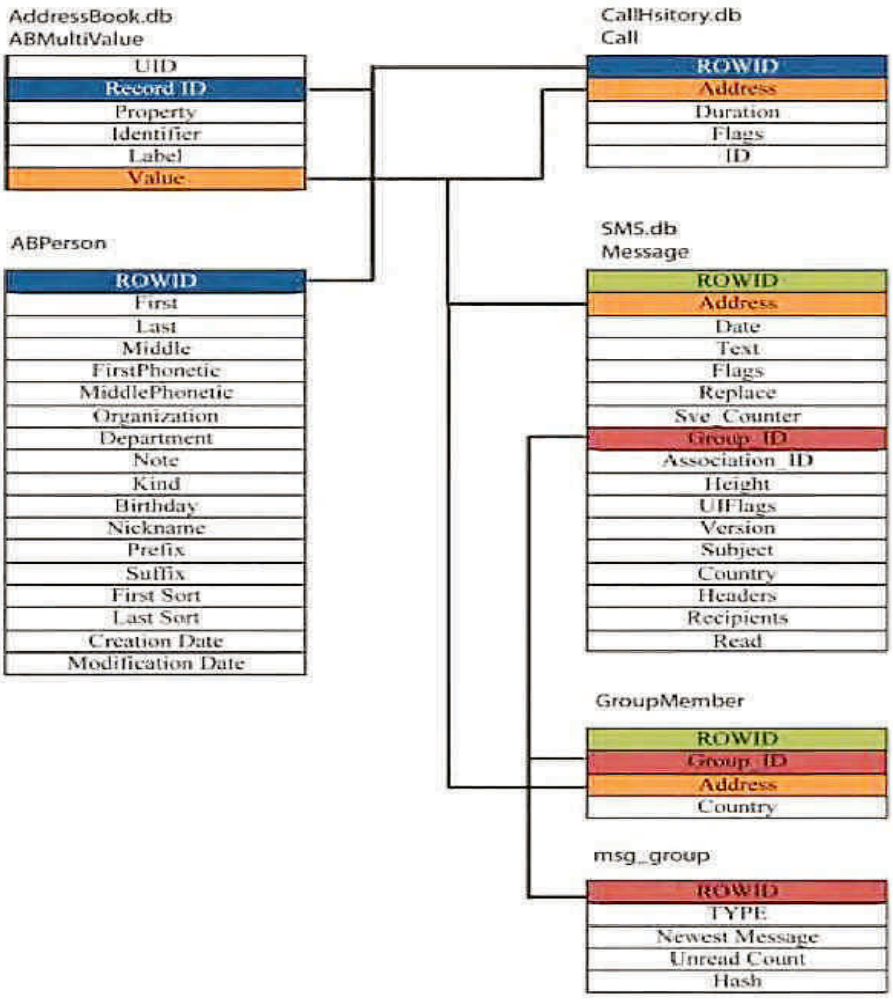
Intuitividad, sencillez y frescura en el manejo seducen a las masas sin transmitir una idea de lo que sucede bajo la pantalla de estos dispositivos de apenas un centímetro de espesor. Subsistemas miniaturizados de enorme complejidad trabajan en perfecta sincronía bajo las órdenes de un sistema operativo iOS o Android. Un potente gestor de bases de datos (*SQLite*), que no funciona en el contexto habitual del modelo servidor-cliente de las redes informáticas sino implementado en una librería que se adosa a los programas para aumentar la velocidad de respuesta, recopila datos y los introduce en tablas: números de teléfono, contactos, direcciones de correo electrónico, mensajes SMS, llamadas entrantes y salientes, archivos de audio, fotografías, anotaciones en el calendario e incluso posiciones geográficas.

Con la localización activa el iPhone no solo sabe dónde se encuentra el lector sino también dónde ha estado. Recuerda los lugares en los que se detuvo para hacer fotos y, al igual que en las novelas de Marcel Proust, recupera tanto el tiempo como el camino perdido. Además debe saber que usted ya no es el dueño exclusivo de esa información. Ahora está en poder de Apple, Google y varias compañías de marketing por Internet. Asi que prepárese a recibir publicidad personalizada.

Si trabaja para una empresa importante y tiene acceso a datos vitales, no está de más que reflexione sobre las consecuencias de extraviar un smartphone. Su terminal acumula de manera automática gran cantidad de información que escapa al control directo del usuario y resulta difícil de proteger mediante cifrado. La substracción de un iPhone tiene los mismos efectos que el robo de un portátil o una estación de trabajo: daños de imagen, pérdida de ventas, responsabilidades civiles, riesgo de intrusión en la red y brechas en la seguridad corporativa.

Este artículo no pretende ser un recetario de seguridad ni una guía de productos software para proteger su smartphone. La informática móvil, con su gran variedad de marcas, aparatos, sistemas operativos e interfaces, dificulta la búsqueda de soluciones simples. Quizá el tiempo y la estandarización hagan que

esto cambie. Pero por el momento valga decir que toda precaución es poca a la hora de proteger sus datos. Cuando termine de leer las páginas que siguen sabrá por qué.




**Dependencias de tablas *SQLIte* en el iPhone 4**

## Hardware

El iPhone 4 o el Samsung Galaxy S que la compañía telefónica nos acaba de regalar por puntos, con procesador Apple A4 a 800 MH o ARM Cortex A8 de 1 gigahertzio, 512 MB de RAM, 16 GB de memoria flash -en el iPhone: 32 GB- (equivalente a discos duros de la misma capacidad), tiene una potencia muy superior a la de un ordenador de sobremesa de finales del siglo XX. Aquellas máquinas podían gestionar ya con total soltura una pila de protocolos TCP/IP y por tanto conexiones de banda ancha a Internet. Los smartphones van aun más lejos. No necesitan ser conectados a ningún modem, pues vienen provistos de serie con interfaces inalámbricos, y por si fuera poco se manejan con un solo dedo. En las páginas que siguen se habla preferentemente del iPhone por tratarse del aparato que marcó la pauta. Gran parte de lo que se va a leer –en cuanto a funcionalidad, forma de uso y bases de datos *SQLite*- también es aplicable a productos de la competencia que funcionan con el sistema operativo Android. Estos dispositivos nuevos están quitando cuota de mercado al iPhone, ya que ofrecen prestaciones similares e incluso superiores a un precio más económico.

Apple sacó a la venta su primer iPhone en el verano de 2007. Desde entonces se han sucedido varias generaciones hasta llegar al iPhone 4, liberado en junio de 2010. El iPhone 4 funciona con el sistema operativo iOS, versión especial de OSX -instalado en macs portátiles y de sobremesa- adaptada para

dispositivos móviles. Su diseño innovador lo distingue de los modelos anteriores 2, 3G y 3GS. Lleva un lateral metálico que al mismo tiempo actúa como antena. Dispone de una pantalla con 89 mm de diagonal y resolución de 640 x 960 a 326 puntos por pulgada, dos cámaras -una trasera para tomas fotográficas y video y otra frontal para teleconferencia-, giróscopo de 3 ejes, acelerómetro, indicador de contacto con líquidos, flash LED, adaptadores WiFi 802.11 b/g/n, Bluetooth y GPS.


**Jailbreaking: liberando el iPhone de su prisión**

**Software**

El sistema operativo y el software incluyen lo necesario para trabajar incluso en entornos de productividad. Las aplicaciones adicionales se instalan mediante el *App Store* de Apple, bien directamente desde el iPhone bien a través del software *iTunes*, utilizado para sincronizar el dispositivo con el ordenador de sobremesa y otras funciones como actualizar el firmware, realizar copias de seguridad, convertir formatos de audio y video, etc. Apple, aunque da a conocer las APIs del sistema y distribuye un kit de programación para desarrolladores, no quiere saber nada sobre instalación de software de terceros. El usuario que desea utilizar programas al margen de la *App Store* se ve obligado a "liberar" su iPhone ("*jailbreaking*") por medio de suites especiales de hacking como *Ultrasn0w* o *Pwnage*. Estas operaciones comportan su riesgo: inutilización ("enladrillado" o *bricking* del terminal), pérdidas de rendimiento y anulación de la garantía. Por no hablar de una mayor exposición a incidentes de seguridad.

No solo los hackers recurren al *jailbreaking*: también la policía se sirve de él para extraer datos de dispositivos incautados en el transcurso de sus investigaciones. Apple se muestra tan reservada en lo referente a la tecnología del iPhone que ni siquiera ha puesto a disposición de las autoridades, ni tiene previsto hacerlo en el futuro, un método adecuado para recuperación de archivos borrados con fines forenses. La compañía de Cupertino (California) no hace esto por codicia, sino para mantener la seguridad en sus productos y redes de datos. No hace falta decir que en un entorno empresarial respetable está de sobra el *jailbreaking* . A ningún miembro de la plantilla se le debería permitir el uso de un iPhone liberado en su puesto de trabajo.

**Recursos de seguridad básicos**

Perder el hardware no es ninguna tragedia. Un iPhone cuesta 600 euros, pero la información personal o de la empresa vale mucho más y hay que protegerla por todos los medios. Una primera línea de defensa la constituye el bloqueo del dispositivo mediante código. Esta opción se halla en *Ajustes / General / Bloqueo con código*. Aparte del acceso restringido ofrece diversas posibilidades, por ejemplo un borrado de todos los datos del iPhone después de varios intentos fallidos de averiguar la contraseña.

*MobileMe* es un servicio tecnológico de Apple a través del cual se puede conocer la posición de un iPhone extraviado. También permite mandar un mensaje al propio terminal para advertir de la pérdida, facilitar señas o números de teléfono para que quien lo encuentre se pueda poner en contacto con el propietario, establecer contraseñas para proteger los contenidos del dispositivo y forzar un borrado remoto. Para utilizar *MobileMe* hace falta descargar una aplicación gratuita de la página web de Apple e instalarla en el ordenador empleado para sincronizar el iPhone, que por supuesto deberá tener acceso a Internet.

Estas soluciones, pese a su carácter innovador, distan de ser la panacea. Están pensadas para evitar el

acceso oportunista a los datos del dispositivo. En el caso más frecuente el iPhone pasa a poder de un carterista o de un individuo que lo encuentra por casualidad en el aeropuerto o en el asiento de un taxi. El nuevo propietario estaría más interesado en utilizarlo para sus propios fines. Sin embargo, lo que interesa a un espía industrial es la información. Para llegar a ella dispone de numerosas posibilidades.

Para el caso de que un usuario no quiera seguir utilizando su terminal y vaya a dejárselo a otra persona el iPhone incluye también una utilidad de borrado seguro. Se encuentra en *Ajustes / General / Restablecer / Borrar contenidos y ajustes*. Tras haber borrado los archivos se sobreescribe el espacio vacío con ceros o datos aleatorios para hacer imposible una recuperación con técnicas forenses. El proceso de borrado seguro dura varias horas en un iPhone de 32 GB, pero deja el dispositivo prácticamente en el mismo estado en que salió de fábrica.

**En las catacumbas del iPhone**

Si el lector es ejecutivo de una gran empresa, líder de un partido político o activista comprometido con movimientos cívicos en países con gobiernos dictatoriales, conviene que tenga una idea de todo lo que el iPhone esconde. Existen técnicas para puentear contraseñas y otras protecciones. La recepción telefónica puede ser anulada introduciendo el aparato en una jaula de Faraday (receptáculo con mallas de metal que impide el paso de las ondas electromagnéticas) o simplemente -según dicen- en una bolsa de patatas fritas que tenga el interior forrado de con papel de plata. De esta manera se impide el borrado remoto a través de *MobileMe*. Aun más fácil: basta poner el iPhone en modo avión (Ajustes), con lo cual el teléfono y la conectividad WiFi quedan inmediatamente desactivados.

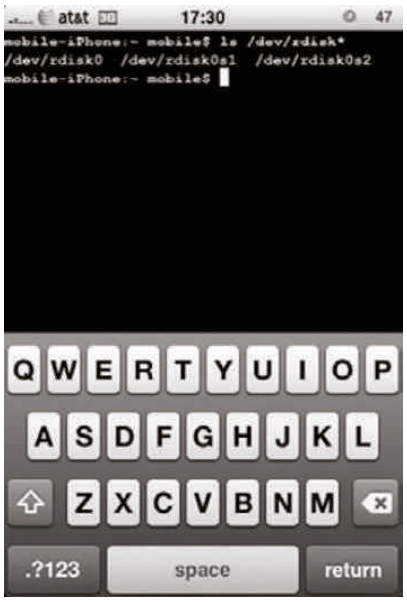
El examen de las propiedades básicas -número de serie, IMEI del teléfono móvil, compañía telefónica, etc.-, asi como de la lista de contactos, agenda, fotografías, documentos y demás, resulta trivial. Con un visor de bases de datos (por ejemplo *SQLite Database Browser* o *Froq*) se puede explorar todo el entramado de tablas en las que el iPhone almacena la información generada en el transcurso de su interacción con el usuario:

- ✓ Libro de direcciones (*AddressBook*): base de datos principal y más voluminosa del sistema iOS, con informaciones de contacto e imágenes, incluyendo grupos y sus miembros, números de teléfono, direcciones postales y de correo electrónico.
- ✓ Cachés del navegador *Safari*: información referente a aplicaciones, servicios y fechas de uso de los programas. Dentro de las bases de datos gestionadas por la caché se incluyen datos de antenas de telefonía móvil y puntos de acceso WiFi con los que interacciona el dispositivo, lo que resulta de gran ayuda para reconstruir itinerarios. Estos datos son imprescindibles para el funcionamiento de *Maps* y otras herramientas de geolocalización.
- ✓ Historial de las últimas 100 llamadas telefónicas, incluyendo fecha y hora, duración y números contactados tanto entrantes como salientes.
- ✓ Perfiles de configuración creados por el usuario.
- ✓ *Cookies:* efectivamente, se trata de esos pequeños archivos de texto almacenados por los navegadores que delatan la actividad del usuario en la red. Como pueden ver no es fácil librarse de las famosas galletitas de Internet, ni siquiera en algo tan pequeño como el iPhone.
- ✓ Historial del teclado: guardado en el archivo *dynamic-text.dat*, que funciona como *keylogger* del iPhone y se abre con un simple editor de texto. Información sensible a más no poder. A partir de ella se pueden reconstruir mensajes SMS e incluso correos electrónicos confidenciales *almacenados en un servidor remoto*.
- ✓ Logs y archivos de registro: información referente al uso de aplicaciones del iPhone.
- ✓ Mapas: esta aplicación del iPhone se sirve del motor de Google Maps para localizar y marcar lugares. Combinado con informaciones adicionales -por ejemplo los metadatos EXIF de las imágenes tomadas por la cámara fotográfica-, permite conocer la posición geográfica y los trayectos seguidos por el usuario. Requiere tener activa la localización.

- ✓ Notas: texto escrito a través de Notes App, con las fechas de creación y modificación de los archivos correspondientes.
- ✓ Preferencias: hay datos que aisladamente resultan poco expresivos, pero estudiados en conjunto pueden llegar a transmitir un retrato fiel de la personalidad, nivel de ingresos, ideas políticas, modo de vida e incluso estado de salud del usuario. Ajustes y cuentas del correo electrónico, código de país, App Store, códigos ICCID, IMSI y ajustes de roaming internacional para el teléfono móvil, norte magnético o real, números para *forwarding* de llamadas, búsquedas recientes en Internet, ajustes de zonas horarias, estado de redes WiFi y Bluetooth, lista de aplicaciones standard e instaladas por el usuario, cotizaciones favoritas de acciones, lista de ciudades para las cuales se hacen consultas meteorológicas, videos buscados en YouTube y parámetros de todas las redes a las que el iPhone ha estado conectado, incluyendo identificadores SSID asi como fecha y hora de la última conexión WiFi.
- ✓ Historial de Internet y *bookmarks* del navegador Safari: URLs de páginas visitadas junto con la fecha y hora de acceso. Especial interés posee la funcionalidad de Estado Suspendido, que permite pasar rápidamente de unas páginas a otras hasta un total de ocho que permanecen guardadas en un caché especial.
- ✓ SMS y MMS: base de datos con mensajes de texto y multimedia enviados y recibidos por el usuario. No solamente se guarda el contenido de los mensajes sino también los números de teléfono, fechas, horas y borradores sin mandar.
- ✓ *Voicemails* (iPhone OS 3.0 y superior): los mensajes de voz se guardan en archivos con extensión .amr que pueden escucharse con *QuickTime*.
- ✓ *WebClips* y *WebKits*: las aplicaciones de Internet suelen volcar gran cantidad de información a las bases de datos *SQLite* (URLs, nombres de aplicaciones, direcciones de correo electrónico, fechas, etc.).
- ✓ Configuración del sistema: en este apartado se incluyen las preferencias del sistema y de la red, junto con las direcciones IP y *hotspots* que el dispositivo va encontrando por el camino.
- ✓ Medios audiovisuales: imágenes tomadas con la cámara fotográfica, archivos de sonido MP3, videos, grabaciones y recordatorios de voz. En lo que respecta a las fotografías es importante mencionar la información contenida en los metadatos EXIF, típicos del formato JPEG y que indican, entre otras cosas, la fecha y hora en que fue tomada la fotografía, modelo de cámara, ajustes, si se disparó el flash, software de retoque utilizado, etc. Con la localización activa los metadatos EXIF incluyen las coordenadas GPS: latitud, longitud, altura y dirección de la brújula.
- ✓ Documentos: archivos PDF, Word y de otros formatos: si han sido cargados desde ordenadores portátiles y de sobremesa incluirán metadatos con información referente a otros usuarios, máquinas, impresoras, grupos de trabajo, modificaciones realizadas en el documento junto con los autores y los nombres de las máquinas por las que el documento ha pasado, tiempos trabajados, objetos incrustados como hojas de cálculo Excel, configuraciones de redes, etc.
- ✓ Y para terminar –pese a que estamos lejos de tener una lista completa- el gran protagonista de la revolución 2.0: las redes sociales, *Facebook*, *LinkedIn*, *MySpace*, *Twitter* y *Skype*. El iPhone guarda artefactos con información relevante para la seguridad: identidades, cuentas, registros VoIP, nombres de usuario en F*acebook*, direcciones de correo electrónico, cualificación profesional, cargos y funciones, posición en el organigrama, etc.

**Extracción de datos**

El espacio de almacenamiento del iPhone está dividido en dos particiones: una de 500 MB para el sistema operativo y los ajustes de fábrica, a la que el usuario no tiene acceso -a no ser que emplee técnicas de *jailbreaking*-; y otra que ocupa el volumen restante (hasta 8, 16 o 32 GB según el tipo) con datos y aplicaciones del usuario. El método más simple para llegar hasta este espacio, también llamado partición del usuario, consiste en conectar el iPhone a un ordenador mediante *iTunes* y realizar una copia de seguridad. Se pueden emplear técnicas más complejas como conectar el dispositivo a un ordenador MacIntosh -físico o virtualizado- con el fin de montar las particiones y acceder directamente a directorios y archivos; por último el volcado NAND, solo al alcance de expertos en electrónica, que consiste en desmantelar el dispositivo, extraer el chip de memoria y copiar su contenido mediante un terminal de programación conectado a un ordenador portátil. Asimismo podemos recurrir al *jailbreaking* para instalar herramientas hacker que le permitan utilizar las mismas técnicas forenses aplicadas por la policía en el análisis de ordenadores incautados: establecimiento de conexiones TCP vía *Netcat*, realización de imágenes en *bitstream*[1] con *dd* incluyendo el espacio de no asignado por el sistema y transferencia de las mismas a una estación de trabajo para proceder a un análisis con *EnCase* o *FTK ,* herramientas forenses de código libre como *TSK* o editores hexadecimales. Tales métodos también permiten recuperar archivos borrados.




**Acceso a las particiones del iPhone mediante herramientas de Jailbreaking**

**UFED**

Conectando el iPhone a un *UFED*, aparato de tecnología israelí distribuido por la empresa Cellebrite, puede realizar un duplicado en *bitstream* de la partición de usuario, incluyendo los archivos borrados. Originariamente el *UFED* (*Universal Forensic Extraction Device: Dispositivo Universal para Adquisiciones Forenses*) fue desarrollado para el sector de la electrónica de consumo, siendo sus principales clientes empresas de telefonía móvil que se servían de él para hacer duplicados de tarjetas y pasar datos de unos terminales a otros. En la actualidad lo utilizan departamentos de policía y agencias de seguridad. Viene acompañado de un maletín con cables para conectarlo a casi todos los terminales disponibles en el mercado (teléfonos, agendas electrónicas, smartphones, tabletas, etc.). El *UFED* también permite realizar volcados de datos a llaves USB, tarjetas SD y otros medios de almacenamiento.

En el ámbito de la seguridad empresarial el UFED, suponiendo que el espía haya podido hacerse con uno de estos aparatos de venta reservada a departamentos de policía y agencias de seguridad, representa el peor de los casos posibles. Se trata de un aparato portátil, del mismo tamaño que los terminales que utilizan los empleados de la compañía eléctrica para leer los contadores, y no requiere más que conocimientos básicos para su manejo. Es verdad que el duplicado de un iPhone lleva demasiado tiempo para poder realizarlo en un descuido de la víctima –al fin y al cabo es necesario copiar más de 8 GB-. Pero tras habérselo sustraído al propietario y una vez terminado el trabajo se puede escenificar un hallazgo casual del dispositivo y la devolución desinteresada del mismo, en perfecto estado de funcionamiento y sin que se noten indicios de que ha tenido lugar un *data leak*[2].

[1] Bitstream: "flujo de bits". Se refiere a la copia forense de un medio de datos que a diferencia del *backup* o la copia de respaldo convencional incluye no solamente los archivos listados en carpetas y/o directorios sino también todos los sectores de la partición con datos procedentes de archivos anteriores o volcados de memoria del sistema.

[2] *Data Leak*: fuga de datos o información vital para la empresa.


**UFED copiando un smartphone**

**Análisis**

El análisis de los datos robados se lleva a cabo por diversos métodos, algunos ya comentados: extracción de archivos mediante *data carving*[3], con software de recuperación de archivos, herramientas forenses o examinando los datos directamente a través de un editor hexadecimal. Teniendo en cuenta que se trata de un dispositivo iOS con particiones HFS, lo más práctico es tratar de montarlas en un ordenador *Apple*. La base de datos *SQLite*, en cuyas tablas almacena toda su información el iPhone, puede examinarse cómodamente a través de *SQLite Data Browser* o *Froq*. Si la categoría del objetivo justifica la inversión, el espía puede adquirir una suite del tipo *Oxygen Forensic Suite 2010* (al precio aproximado de 1.500 dólares, aunque existen versiones de prueba gratuita en la página web del desarrollador: http://www.oxygen-forensic.com). Esto facilita la extracción de datos a través del software de sincronización *iTunes*.

**Recomendaciones**

Si pensaba que este artículo iba a ser una guía fácil de estrategias y productos software para asegurar su iPhone lamento haberle decepcionado. Tampoco es mucho lo que hay al respecto. La gran variedad de sistemas, dispositivos y diseños hace imposible establecer conceptos de seguridad válidos para todo tipo de situaciones. La escena del smartphone se encuentra en plena explosión cámbrica y todavía no existen estándares ni entornos unificados como en el mundo del PC de sobremesa. Lo único que puede hacer es utilizar las herramientas software de *Apple* (bloqueo del dispositivo, *MobileMe*) y ser consciente del peligro de pérdida de datos para empresas, partidos políticos, ONGs, administraciones públicas y otras entidades que manejan datos valiosos. Por no hablar de su propia información personal.

La pérdida de un iPhone -de cualquier smartphone- supone el mismo riesgo potencial que el robo de un ordenador de sobremesa repleto de documentos y bases de datos con información de acceso reservado. El riesgo va más allá de la seguridad corporativa. El entorno legal europeo es cada vez menos permisivo en lo referente a la privacidad y el tratamiento de informaciones personales. Aparte de la pérdida de competitividad y los daños de imagen hay que tener en consideración el riesgo jurídico: en los tiempos que corren llueven demandas y sanciones por doquier.

No quiero que el lector se quede con la impresión de que soy una especie de pesimista cultural. No hay por qué renunciar a las ventajas de las nuevas tecnologías solo por el riesgo que implica utilizarlas. Siguiendo la misma lógica no deberíamos encender la cocina de gas ni subirnos a un avión. Lo único que digo es que hay que estar alerta, desconfiar y mantener en todo momento una actitud de prudencia e incluso de sano escepticismo. Guíese por la madurez y el sentido comun. Quizá un universitario pueda permitirse matar el rato con un iPhone. Resulta satisfactorio utilizarlo como medio de interacción social intuitiva y desestructurada: mandar mensajes, twittear y subir fotografías a *Facebook* o *Flickr*. Incluso es beneficioso, según se ha podido comprobar, para reforzar la autoestima de los adolescentes. Los smartphones se hicieron para abastecer segmentos de mercado muy influidos

[3] *Data Carving*: "tallado de archivos" o búsqueda de archivos borrados en un medio a través de cadenas de caracteres características.

por las nuevas tendencias sociales y la cultura de la movilidad. Pero si tiene intención de emplearlos con fines profesionales piénselo dos veces antes de sacar el suyo del bolsillo. Lo que lleva encima no es un juguete, sino el dispositivo informático más potente fabricado hasta la fecha en términos de prestaciones y tamaño.

Finalmente no olvide que existe un lado oscuro. Hay que ser realistas: vivimos una época dorada para espías industriales, spammers, traficantes de datos, acosadores, pederastas, intrigantes, empleados desleales, traidores y sinvergüenzas de todo tipo. No hay dispositivo informático que no pueda usarse no ya para algún ardid de picaresca digital, sino en actividades definitivamente criminales. Incluso a las herramientas de seguridad desarrolladas para combatir el delito se les puede dar la vuelta y emplearlas con fines espúreos. Caso típico es el del individuo celoso que regala a su compañera un iPhone con *MobileMe* activo para tener vigilados sus movimientos.

**Bibliografía**


- ✓ Sean Morrissey: *iOS Forensic Analysis for iPhone, iPad and iPod touch.* Apress 2010
- ✓ Jonathan Zdziarski: *iPhone Forensics.* O'Reilly Media 2008.
- ✓ David Jurick, Adam & Damien Stolarz: *iPhone Hacks. Tips & Tools for Unlocking the Power of your iPhone & iPod touch.* O'Reilly 2009 (Versión en español: iPhone 3G. Los mejores trucos. Anaya Multimedia).
- ✓ Ryan R. Kubasiak, Sean Morrissey: *Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit.* Syngress Publishing 2009.