

Seguridad en sistemas y servicios móviles

## 2

### Seguridad en los terminales móviles y las comunicaciones



## ÍNDICE

<b>MOTIVACIÓN .....</b>	<b>5</b>
<b>PROPÓSITOS .....</b>	<b>6</b>
<b>PREPARACIÓN PARA LA UNIDAD .....</b>	<b>7</b>
<b>1. INTRODUCCIÓN Y EVOLUCIÓN DE LAS COMUNICACIONES MÓVILES .....</b>	<b>9</b>
1.1. INTRODUCCIÓN .....	9
1.2. EL PRINCIPIO DE LOS TIEMPOS (0G) .....	10
1.3. PRIMERA GENERACIÓN (1G) .....	11
1.4. SEGUNDA GENERACIÓN (2G) .....	12
1.5. TERCERA GENERACIÓN (3G) - AÑOS 2000 .....	15
1.6. CUARTA GENERACIÓN (4G) .....	16
<b>2. INTERCEPTACIÓN LEGAL DE LAS COMUNICACIONES (ILT) .....</b>	<b>19</b>
2.1. CONCEPTO DE ILT .....	19
2.2. PROBLEMÁTICA Y EVOLUCIÓN. ....	21
2.3. EL CASO PARTICULAR DE LA TELEFONÍA IP .....	23
<b>3. INTERCEPTACIÓN MALICIOSA DE LLAMADAS Y SMS .....</b>	<b>25</b>
3.1. TELEFONÍA 2G .....	25
3.2. MAN IN THE MIDDLE .....	25
3.3. CAPTURA Y DES-ENCRIPCIÓN 2G / 3G .....	28
3.3.1. INTRODUCCIÓN .....	28
3.3.2. ATAQUES 1G/2G: .....	30
3.3.3. ATAQUES 3G .....	34

<b>4. CASO PRACTICO DE ANÁLISIS PARA LA DETECCIÓN DE TELÉFONOS INTERVENIDOS/INTERCEPTADOS .....</b>	<b>37</b>
4.1. INTRODUCCIÓN .....	37
4.2. EJEMPLO FLEXISPY .....	38
4.3. OTROS SOFTWARE ESPÍA.....	40
4.3.1. MSpY.....	40
4.3.2. HIGHSTER MOBILE.....	40
4.4. EJEMPLO DE DETECCIÓN.....	41
4.5. EJEMPLO ANÁLISIS IMSI CATCHER.....	42
<b>5. TÉCNICAS DE INFECCIÓN DE TERMINALES .....</b>	<b>45</b>
5.1. TÉCNICAS DE INFECCIÓN.....	45
5.2. INFECCIÓN EN IOS.....	46
<b>6. ESTRUCTURA DE CARPETAS PARA EL ANÁLISIS DE DISPOSITIVOS.....</b>	<b>49</b>
6.1. INTRODUCCIÓN .....	49
6.2. ANDROID .....	50
6.3. IOS.....	51
<b>7. HERRAMIENTAS PARA ANÁLISIS DE TERMINALES.....</b>	<b>55</b>
7.1. INFORMACIÓN PROPORCIONADA.....	55
7.2. HERRAMIENTAS.....	56
7.2.1. IPHONE .....	56
7.2.2. BLACKBERRY .....	57
7.2.3. ANDROID.....	57
<b>8. POSICIONAMIENTO Y LOCALIZACIÓN DE PERSONAS MEDIANTE TECNOLOGÍA GSM .....</b>	<b>58</b>
8.1. INTRODUCCIÓN .....	58
8.2. PROBLEMÁTICA.....	59
<b>9. CASO PRÁCTICO DE INTERCEPTACIÓN DE COMUNICACIONES DE APLICACIONES DE SMARTPHONES.....</b>	<b>62</b>
9.1. ESTUDIO DE CASO PRÁCTICO: WHATSAPP.....	62
9.2. CAPTURA DE DATOS EN EL PROCESO DE COMUNICACIÓN .....	65
9.3. ANÁLISIS DE DATOS CAPTURADOS.....	66
9.4. ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS DATOS ALMACENADOS .....	71
9.5. CONCLUSIONES GENERALES SOBRE EL CIFRADO DE LOS MENSAJES.....	73
9.6. CONCLUSIONES GENERALES SOBRE EL ALMACENAMIENTO DE DATOS EN DISPOSITIVO .....	73



<b>9.7. CONCLUSIONES GENERALES SOBRE EL USO DE LA APLICACIÓN WHATSAPP 2.8.3 PARA ENTORNO</b>	
<b>LABORAL .....</b>	<b>73</b>
<b>CONCLUSIONES .....</b>	<b>75</b>
<b>RECAPITULACIÓN .....</b>	<b>76</b>
<b>AUTOCOMPROBACIÓN .....</b>	<b>77</b>
<b>SOLUCIONARIO .....</b>	<b>81</b>
<b>PROPUESTAS DE AMPLIACIÓN .....</b>	<b>82</b>
<b>BIBLIOGRAFÍA .....</b>	<b>84</b>



## MOTIVACIÓN

---

Las comunicaciones móviles han experimentado un alto crecimiento en los últimos años. Desde los primeros terminales, cuya función no era otra que la de replicar a los teléfonos fijos, hemos saltado a un mundo en el que los terminales son un ordenador, donde la voz no es más que otra aplicación más, y donde se pueden ejecutar las más variadas aplicaciones, con una potencia de procesamiento equivalente a la de ordenadores tipo PC de hace unos pocos años.

Es por esto que no debe extrañarnos que la seguridad en estos terminales haya seguido la misma ruta que en su día siguió en los PC: La aparición de malware que permite a extraños tomar el control de nuestros equipos y poder ejecutar acciones sin nuestro consentimiento.

A todo esto hay que añadir la cuestión que estos terminales están permanentemente conectados a redes públicas de telecomunicaciones, con contratos de comunicación establecidos, y por tanto, con la posibilidad de poder ganar dinero con acciones no legítimas: Llamadas a números de tarificación adicional, llamadas internacionales Premium, etc.

Si quieres entender la Seguridad de las Comunicaciones móviles en toda su extensión, esta unidad te va a permitir iniciarte en este tipo de temas.

## PROPÓSITOS

---

Al finalizar el estudio de esta unidad deberías ser capaz de poder explicar las siguientes cuestiones:

- Tener claro la evolución seguida en las comunicaciones móviles y la seguridad en estos terminales.
- Conocer cómo se lleva a cabo un análisis de un malware de Android.
- Conocer qué posibilidades existen de interceptación en comunicaciones móviles.
- Conocer las técnicas y procedimientos para la geo-posición usando terminales móviles

Pero sobre todo, el alumno deberá tener claro al final de esta unidad que la Seguridad en las Comunicaciones móviles es un aspecto cada vez más esencial de las mismas, con grandes expectativas de negocio para las mafias implicadas.



## PREPARACIÓN PARA LA UNIDAD

---

En esta unidad vamos a tratar los siguientes temas:

1. Introduciremos las comunicaciones móviles así como entenderemos la evolución que ha sufrido estos terminales.
2. Veremos las posibilidades y técnicas para poder realizar interceptaciones de llamadas de terminales móviles y SMS con tecnología GSM.
3. Estudiaremos un caso práctico de análisis para la detección de teléfonos intervenidos/interceptados.
4. Veremos cómo se hace el posicionamiento GPS y la localización de personas mediante tecnología GSM, sus limitaciones y técnicas.
5. Veremos cómo se hace la interceptación de comunicaciones de las aplicaciones de Smartphones, así como un caso práctico con Whatsapp.



# 1. INTRODUCCIÓN Y EVOLUCIÓN DE LAS COMUNICACIONES MÓVILES

## 1.1. INTRODUCCIÓN

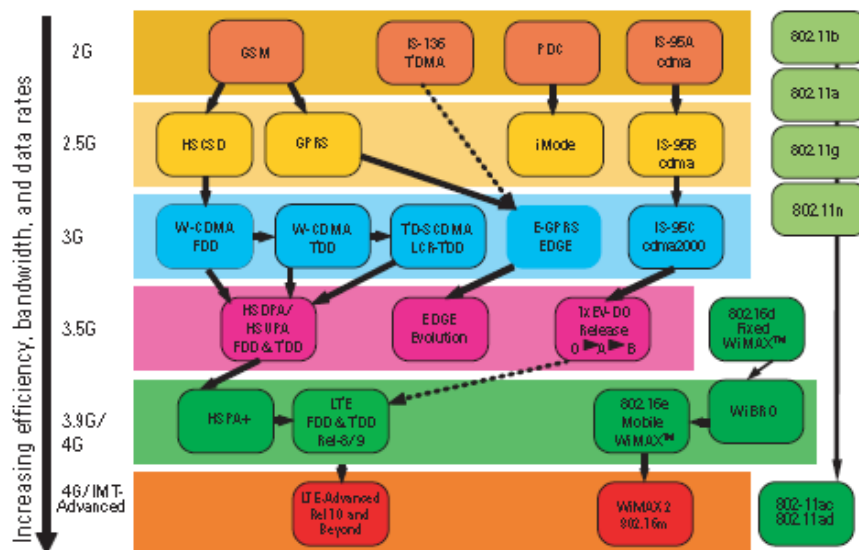
Las comunicaciones inalámbricas han evolucionado a partir de la llamada segunda generación (2G) sistemas de la década de 1990, que introdujo por primera vez la tecnología celular digital, a través del despliegue de la tercera generación (3G) sistemas con sus redes de datos de velocidad superiores hasta la cuarta generación con su tecnología de acceso IP de alta velocidad que se está desarrollando en la actualidad. Esta evolución se ilustra en la figura 1, lo que demuestra que se están proponiendo un menor número de normas para 4G que en generaciones anteriores, con sólo dos candidatos 4G están desarrollando activamente hoy: 3GPP LTE-Advanced y IEEE 802.16m, que es la evolución del estándar WiMAX conocida como Mobile WiMAX <sup>TM</sup>.

Las comunicaciones en movilidad permiten que un usuario pueda utilizar servicios de telecomunicaciones mientras se desplaza a lo largo de un territorio.

La clasificación más comúnmente usada para referirse a los sistemas de comunicaciones móviles es la siguiente:

- Primera Generación 1G o analógicos.
- Segunda Generación 2G o digitales.
- Segunda Generación y Media 2,5G.
- Tercera Generación 3G o de banda ancha.
- Beyond 3G: con este término se agrupan a todos los sistemas y generaciones posteriores a 3G. Se habla por tanto de 3,5G, 4G, etc.

Los primeros sistemas de 1G y 2G aparecieron en el mercado en 1979 y 1991 respectivamente. Su expansión no tuvo una geografía uniforme ni siquiera en Europa. Por su parte los sistemas 2,5G nacieron comercialmente en el año 2000 y, los sistemas 3G comenzaron su andadura a finales de 2001.



**Figura 1:** Extraído de <http://www.academica.mx/blogs/redes-inal%C3%A1mbricas-m%C3%B3viles>

Desde un punto de vista técnico, los sistemas de comunicaciones móviles se han desarrollado empleando tecnologías que extienden el servicio gracias a la superposición de la cobertura circular (o celular) de una estación base sobre una determinada zona. Así las tecnologías celulares se emplean en el despliegue de redes que dividen el territorio en celdas para incrementar la capacidad de la red reutilizando las mismas frecuencias en diferentes celdas. Dada la proliferación de estos sistemas en los últimos años, las redes móviles se llaman también en muchos casos redes celulares.

## 1.2. EL PRINCIPIO DE LOS TIEMPOS (OG)



Los primeros sistemas de telefonía móvil civil empiezan a desarrollarse a partir de finales de los años 40 en los Estados Unidos.

Eran sistemas de radio analógicos que utilizaban en el primer momento modulación en amplitud (AM) y posteriormente modulación en frecuencia (FM). Se popularizó el uso de sistemas FM gracias a su superior calidad de audio y resistencia a las interferencias. El servicio se daba en las bandas de HF y VHF.

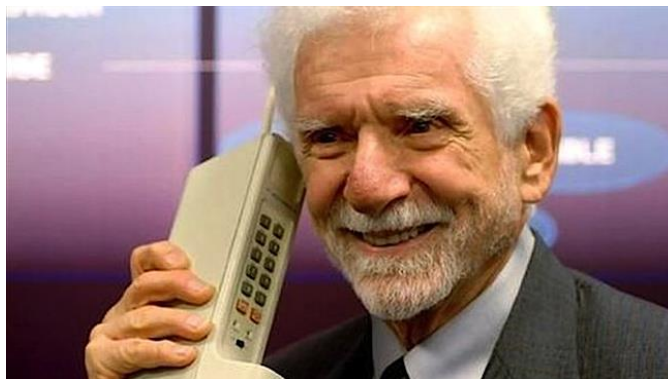


**Figura 2:** La primera llamada desde un teléfono "portátil" en un camión en Chicago, E.E.U.U. (1946). Extraído de <<http://www.atraccion360.com/nostalgia-telefonos-para-automoviles>>

Debido a su excesivo peso y grandes dimensiones, los primeros equipos de telefonía móvil se empleaban únicamente a bordo de automóviles. Normalmente se instalaban en el maletero y se conectaban con la parte frontal del vehículo a través de un cable.

La compañía americana Bell, fue una de las predecesoras en el desarrollo y explotación de este servicio móvil, al que bautizaron como System Service. Sin embargo, la expansión del servicio no fue notoria al ser considerablemente costoso. Aún con eso, estuvo operativo desde 1946 hasta 1985, con diversas actualizaciones tecnológicas.

### 1.3. PRIMERA GENERACIÓN (1G)



**Figura 3:** Dr.Martin Cooper con su prototipo del MotorolaDynaTAC de 1973. Extraído de [http://www.theregister.co.uk/2012/11/29/rockman\\_on\\_motorola/print.html](http://www.theregister.co.uk/2012/11/29/rockman_on_motorola/print.html)

Pero no fue hasta 1981, cuando apareció el primer sistema de telefonía móvil tal y como los conocemos hoy en día. En ese año, la compañía de origen sueco Ericsson, lanza al mercado el sistema NMT 450 (Nordic Mobile Telephony 450

MHz), el cual, seguía basándose en canales de radio analógica (frecuencias en torno a 450 MHz) con modulación en frecuencia (FM).

Aunque los equipos de primera generación nos sorprenden hoy por su aparatosa, lo cierto es que supusieron un destacado avance para su época, principalmente porque podían ser utilizados y transportados por una sola persona.

Ericsson modernizó el sistema con el NMT 900, en el año 1986. Esta nueva versión funcionaba sustancialmente del mismo modo que la anterior pero a frecuencias superiores (del orden de 900 MHz) lo que posibilitó dar servicio a una mayor cantidad de usuarios y avanzar en la portabilidad de los dispositivos.

Además de dicho sistema, durante la década de los 80 se llevaron a cabo otros sistemas de telefonía móvil como: AMPS (Advanced Mobile Phone System) en EE. UU. y TACS (Total Access Communication System).



El sistema TACS se utilizó en España con el nombre comercial de MoviLine. Estuvo en servicio hasta su extinción en 2003.

## 1.4. SEGUNDA GENERACIÓN (2G)

La segunda generación de teléfonos móviles apareció en los años 90, utilizando sistemas como GSM, IS-136, iDEN e IS-95. Las frecuencias utilizadas en Europa fueron de 900 y 1800 MHz.

La explosión de la digitalización de las comunicaciones en esta década aumentó los niveles de seguridad y ofrecía mucha mejor calidad de voz, además de simplificar la fabricación de los terminales, con la reducción de costos que ello conlleva. También a lo largo de estos años aparecieron nuevos estándares de comunicaciones móviles: D-AMPS (EE. UU.), Personal Digital Cellular (Japón), cdmaOne (EE. UU. y Asia) y GSM.



**Figura 4:** Antena GSM

La mayoría de las operadoras telefónicas móviles implementaron el Acceso múltiple por división de tiempo (TDMA) y Acceso múltiple por división de código (CDMA) sobre las redes Amps ya existentes convirtiéndolas de esta forma en redes D-AMPS. Esta implementación permitió a estas empresas migrar de señal analógica a señal digital sin tener que cambiar elementos externos como antenas, torres, cableado, etc. Además, este contenido digital se transmitía sobre los mismos canales (y por lo tanto, las mismas frecuencias de radio) ya existentes y en uso por la red analógica. Pero la máxima diferencia que trajo la tecnología digital fue el hecho de hacer Multiplexion, que permitía transmitir varias conversaciones de forma simultánea por el mismo canal, incrementando con ello la capacidad operativa y el número de usuarios que podían utilizar la red en una misma celda en un momento concreto.



El estándar que ha universalizado la telefonía móvil ha sido el archiconocido GSM: Global System for Mobile communications o Groupe Spécial Mobile.

Las principales características del estándar europeo GSM son las siguientes:

- Destacable calidad de voz (gracias al procesado digital).
- Itinerancia (Roaming).
- Deseo de implantación internacional.

- Terminales realmente portátiles (de reducido peso y tamaño) a un precio asequible.
- Compatibilidad con la RDSI (Red Digital de Servicios Integrados).
- Instauración de un mercado competitivo con multitud de operadores y fabricantes.



Realmente, GSM ha cumplido con todos sus objetivos pero al cabo de un tiempo empezó a acercarse a la obsolescencia porque sólo ofrecía un servicio de voz o datos a baja velocidad (9.6kbit/s) y el mercado empezaba a requerir servicios multimedia que hacían necesario un aumento de la capacidad de transferencia de datos del sistema. Es en este momento cuando se empieza a gestar la idea de 3G, pero como la tecnología CDMA no estaba lo suficientemente madura en aquel momento se optó por dar un paso intermedio: 2.5G.

La tecnología de 2G fue incrementada a 2.5G, incluyendo novedosos servicios como EMS y MMS:

- El servicio de mensajería mejorado, o EMS ofrece la introducción de iconos y efectos sonoros dentro de un mensaje de texto o SMS; un EMS equivale a 3 o 4 SMS.
- El servicio de mensajería multimedia o MMS permite enviar mensajes GPRS y la inserción de fotografías, videos, sonidos y texto. Un MMS se envía en forma de diapositiva. Cada plantilla solamente puede contener un archivo de cada tipo aceptado, es decir, solo puede contener una imagen, un sonido y un texto en cada plantilla. Si el usuario quisiera agregar más de estos tendría que agregarse otra plantilla. Cabe mencionar que no es posible enviar un vídeo de más de 15 segundos de duración.

Estos nuevos servicios exigían de forma indispensable mayor velocidad de transferencia de datos, que se hizo realidad con las tecnologías GPRS y EDGE.

- GPRS (General Packet Radio Service) permite velocidades de datos desde 56 kbit/s hasta 114 kbit/s.
- EDGE (Enhanced Data rates for GSM Evolution) permite velocidades de datos hasta 384 kbit/s.



## 1.5. TERCERA GENERACIÓN (3G) - AÑOS 2000

GSM empieza a quedarse corto a la hora de cubrir las necesidades del mercado (sólo permite transmisión de datos a muy baja velocidad: 9.6Kbps).



Se decide crear un nuevo estándar basado en CDMA (Code Division Multiple Access), sin embargo al tratarse de una tecnología tan verde se opta por un paso intermedio, que fue conocido como 2.5G.

A la tecnología 2G se le incluyeron EMS, MMS (Multiples Message System), GPRS (General Packet Radio Service) y EDGE (Enhanced Data rates for GSM Evolution).

Finalmente nace la tercera generación basada en el un estándar totalmente nuevo conocido como UMTS (Universal Mobile Telecommunications System) que utiliza tecnología CDMA, lo que permite velocidades de hasta 7.2Mbps. La 3G o Tercera Generación de comunicaciones móviles representa el conjunto de estándares diseñados con el objetivo de implantar unas redes completamente nuevas que soportaran mayor capacidad para la transmisión de datos en movilidad frente a sistemas anteriores. El desarrollo de la 3G supone la llegada de la banda ancha a las comunicaciones móviles.

La tecnología UMTS (Universal Mobile Telecommunications System) es un sistema de telefonía móvil de tercera generación (3G). Desde un punto de vista técnico, la mayor innovación que introduce UMTS es el uso de la técnica de espectro ensanchado WCDMA (Wide Code Division Multiplexing Access) ya que GSM o GPRS tan sólo utilizaban FDMA o TDMA. Esta técnica permite aumentar la velocidad de transmisión, así como mejorar la resistencia a las interferencias, facilitar los procesos de transición entre dos celdas (soft handover). Así, UMTS alcanza velocidades de hasta 2Mbps en la transmisión de datos con baja movilidad o 144Kbps sobre vehículos a gran velocidad. Esta capacidad de transmisión unida al soporte del protocolo IP capacita a UMTS para la prestación de servicios multimedia interactivos.

Los sistemas de 3G suponen un paso definitivo en el proceso de convergencia en servicios, ya que además de implementar una arquitectura abierta, dinámica y de fácil interoperabilidad ofrecen unas velocidades de acceso suficientes para el desarrollo de servicios multimedia en movilidad. Se añaden nuevas funcionalidades de comunicación a los terminales: Bluetooth, wifi, etc.



Los terminales móviles asumen cada vez más funcionalidades: Cámara de fotos, acceso a Internet, Gestión de contactos, Correo electrónico, Servicios “Cloud”, etc.

Aparecen iPhone y los móviles Android que hoy en día acaparan la cuota de mercado.



Es posible instalar todo tipo de aplicaciones en los Smartphones:

- Aplicaciones de comunicación.
- Aplicaciones de finanzas y banca electrónica.
- Aplicaciones de ocio y juegos.
- Aplicaciones multimedia.
- Aplicaciones de seguridad.
- Malware.



## 1.6. CUARTA GENERACIÓN (4G)

La generación 4, o 4G es la evolución tecnológica que ofrece al usuario de telefonía móvil un mayor ancho de banda que permite, entre muchas otras cosas, la recepción de televisión en Alta Definición. Como ejemplo, podemos citar al *concept mobile* Nokia Morph.



Hoy en día existe un sistema de este nivel operando con efectividad solo con algunas compañías de EEUU, llamado LTE.

La cuarta generación de tecnologías de telefonía móvil, o 4G, estará basada totalmente en IP, alcanzándose después de la convergencia entre las redes de cables e inalámbricas, así como en ordenadores, dispositivos eléctricos y tecnologías de la información, así como otras convergencias para proveer velocidades de 100 Mbps en movimiento y 1 Gbps en reposo, manteniendo una calidad de servicio de punta a punta. Esta convergencia de tecnologías surge de la necesidad de agrupar los diferentes estándares en uso con el fin de delimitar el ámbito de funcionamiento de cada uno de ellos y con el fin también de integrar todas las posibilidades de comunicación en un único dispositivo de forma transparente al usuario.

La 4G no es una tecnología o estándar definido, sino una colección de tecnologías y protocolos para permitir el máximo rendimiento de procesamiento con la red inalámbrica más barata.

El objetivo que persigue es el de garantizar una calidad de servicio y el cumplimiento de los requisitos mínimos para la transmisión de servicios de mensajería multimedia, video chat, TV móvil o servicios de voz y datos en cualquier momento y en cualquier lugar utilizando siempre el sistema que mejor servicio proporcione. En resumen, el sistema 4G debe ser capaz de compartir dinámicamente y utilizar los recursos de red economizando los requerimientos del usuario.

Algunos de los estándares fundamentales para 4G son WiMAX, WiBro, y 3GPP LTE (Long Term Evolution). Para poder hacer realidad esta red es necesario no sólo integrar las tecnologías existentes (2G, 3G...), también es necesario hacer uso de nuevos esquemas de modulación o sistemas de antenas que permitan la convergencia de los sistemas inalámbricos.

El proyecto Long Term Evolution se inició en el año 2004. La motivación para LTE incluía el objetivo de una reducción en el costo por bit, la adición de los servicios de menor costo con una mejor experiencia del usuario, el uso flexible de las bandas de frecuencias nuevas y existentes, una red simplificada y menor costo con interfaces abiertas, y una reducción en complejidad en el terminal con un consumo de energía razonable.

La interfaz y la arquitectura de radio del sistema LTE es completamente nueva. Estas actualizaciones fueron llamadas Evolved UTRAN (E-UTRAN). Un importante logro de E-UTRAN ha sido la reducción del costo y la complejidad de los equipos, esto es gracias a que se ha eliminado el nodo de control (conocido en UMTS como RNC). Por tanto, las funciones de control de recursos de radio, control de calidad de servicio y movilidad han sido integradas al nuevo Node B, lla-

mado involved Node B. Todos los eNB se conectan a través de una red IP y se pueden comunicar unos a otros usando el protocolo de señalización SS7 sobre IP.

## 2. INTERCEPTACIÓN LEGAL DE LAS COMUNICACIONES (ILT)



Para saber más sobre este tema, del cual hemos extractado parte de este capítulo, te recomendamos que vayas a WikiTel, proyecto promovido por la antigua Comisión del Mercado de las Telecomunicaciones (actual CNMC) y en concreto a <http://wikitel.info/wiki/Sitel>.

### 2.1. CONCEPTO DE ILT

La vigilancia e interceptación de las telecomunicaciones toca unas zonas muy sensibles de la ciudadanía que no se encuentra conforme con que se invada un derecho fundamental, que en muchos países está protegido constitucionalmente, alegando que dichas actuaciones responden a necesidades de la seguridad nacional. Por tanto, para poder invadir el derecho a la intimidad cualquier procedimiento de interceptación debe comenzar teniendo un fundamento legal y unos motivos éticos muy claros y sólidos.

En las redes telefónicas antiguas era relativamente sencillo efectuar escuchas, tanto legales por orden judicial, como ilegales. Como se establecía y dedicaba un circuito de voz para cada conversación y los terminales eran muy sencillos, resultaba fácil interceptar la comunicación en algún punto o poner la llamada en conferencia con el lugar de interceptación, donde quedaba grabada la conversación.

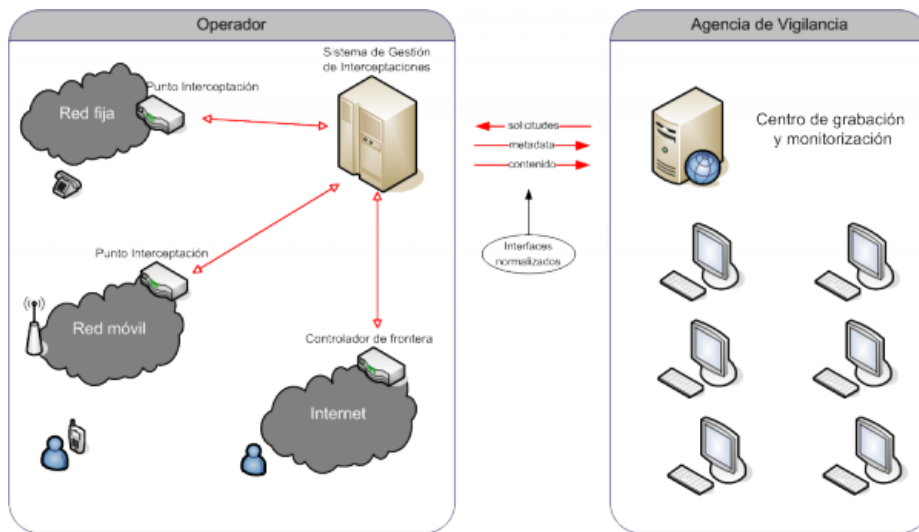


Antes de entrar en detalles, conviene remarcar que la obligación legal de grabar las llamadas a los centros de emergencia, las transacciones bancarias por vía telefónica, la compraventa de valores y otras obligaciones similares de grabación no se consideran interceptación, sino una grabación en destino que se supone conocida por el llamante, a quien se le advierte de algún modo, y que generalmente se efectúa por la entidad que recibe la llamada.

La directiva europea 2006/24/EC, transpuesta en España por la ley 25/2007 del 18 de octubre 2007 sobre la retención de datos, impone a los operadores de telefonía, así como a los proveedores de servicios Internet, que almacenen durante doce meses las informaciones que permiten identificar el origen y el destino de cada comunicación electrónica. Entre otras obligaciones, imponen las siguientes:

- Deben conservar los números de teléfono de origen y de destino. Así como los números IMSI (que identifican las tarjetas SIM) y los números IMEI (que identifican los teléfonos).
- Deben poder identificar a las personas detrás de estos números. Desde noviembre de 2009 las tarjetas prepago ya no pueden ser anónimas y los operadores tienen que identificarlas o desactivarlas.
- Deben conservar la localización del móvil, como mínimo con el identificador de la antena.
- Deben conservar la hora de principio y fin de la llamada así como el tipo de comunicación (llamada, buzón de voz, mensaje, etc.)
- Deben conservar todas estas informaciones incluso en el caso de llamadas perdidas, pero no en el caso de llamadas fallidas.
- Esta ley no permite conservar ningún dato que revele el contenido de la comunicación.
- Tienen que ceder estos datos a los agentes facultados: los miembros de las Fuerzas y Cuerpos de Seguridad cuando desempeñen funciones de policía judicial, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera y el personal del Centro Nacional de Inteligencia.
- El plazo de conservación se puede ampliar hasta dos años.

En España, son los artículos 83 a 101 del “Real Decreto 424/2005, de 15 de Abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, respaldados a su vez por la Ley Ordinaria 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que vino a dar nueva redacción al artículo 33 de la “Ley 33/2003, del 3 de Noviembre, General de Telecomunicaciones, los que determinan la forma de las interceptaciones, es decir, el cómo se han de ejecutar.



**Figura 5:** Esquema básico simplificado ILT. Fuente <http://wikitel.info/wiki/>

La interceptación de la telefonía móvil digital, por tanto con conmutación de paquetes, es una de las cuestiones más candentes, en particular a raíz del escándalo de las escuchas en la telefonía móvil de Atenas<sup>1</sup>, que "puso el dedo en la llaga" o cuestión de fondo, si con métodos automáticos de interceptación no se estará creando un mayor riesgo de seguridad: si son automáticas y las maneja personal del operador quizás se esté abriendo una vía para que personas menos honorables manipulen el sistema en su propio beneficio. Un estudio de ITAA<sup>2</sup> entendió que el problema de las escuchas en Atenas fue obra de personal interno a la compañía y no de alguien ajeno a ella. Lo mismo parece que ha ocurrido en Colombia<sup>3</sup>. En todo caso, queda evidenciado lo sencillo que resulta interceptar las comunicaciones móviles digitales bajo mandato legal, y como también se puede hacer ilegalmente.

## 2.2. PROBLEMÁTICA Y EVOLUCIÓN.

Los sistemas de ILT implementados hasta la fecha se quedaron obsoletos con la irrupción de nuevas plataformas como WhatsApp, Facebook, Skype o voz por IP. Las fuerzas policiales han tenido que actualizar sus herramientas y métodos para interceptar mensajes y adaptarse a los nuevos 'modus operandi' de los criminales a la hora de comunicarse entre ellos. Ahora, un reclutador de yihadistas, por ejemplo, puede enviar un mensaje privado por Facebook a uno de sus objetivos, a la vez que escribe un mail a un contacto en Siria para informarle de sus avances, mientras sube un vídeo a YouTube con propaganda del Estado Islámico.

<sup>1</sup> [http://en.wikipedia.org/wiki/Greek\\_telephone\\_tapping\\_case\\_2004-2005](http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005)

<sup>2</sup> "Designing wiretapping into the communication system raises a fundamental security issue: can the capability be controlled so that only authorized parties can employ it?" Information Technology Association of America (ITAA), 2006

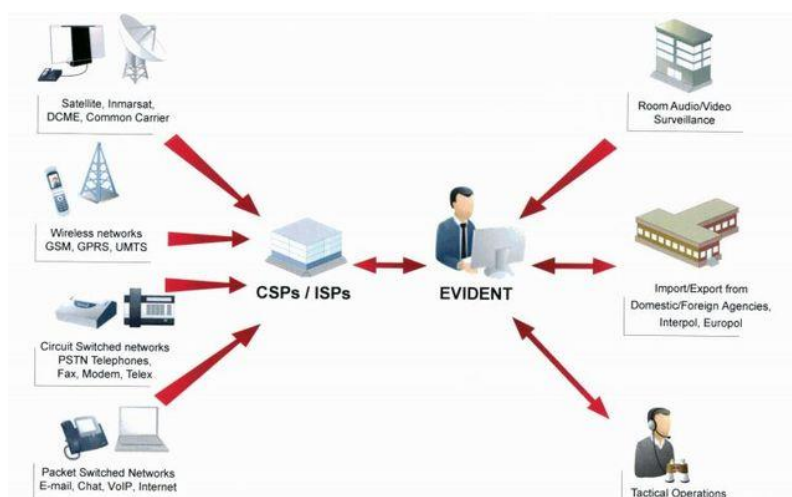
<sup>3</sup> [http://www.eltiempo.com/colombia/justicia/ARTICULO-PRINTER\\_FRIENDLY-PLANTILLA\\_PRINTER\\_FRIENDLY-6165947.html](http://www.eltiempo.com/colombia/justicia/ARTICULO-PRINTER_FRIENDLY-PLANTILLA_PRINTER_FRIENDLY-6165947.html) y [http://www.eltiempo.com/justicia/2008-04-20/ARTICULO-WEB-NOTA\\_INTERIOR-4109441.html](http://www.eltiempo.com/justicia/2008-04-20/ARTICULO-WEB-NOTA_INTERIOR-4109441.html)

co y llama por teléfono a uno de sus colaboradores para darle nuevas instrucciones.

Toda la actividad de un sospechoso quedará reflejada y registrada en tiempo real a través de nuevas plataformas como 'Evident X-Stream', recientemente adquirida por el Ministerio del Interior de España a la multinacional BAE Systems, y que estará plenamente operativo en 2017. Es, en la práctica, un sistema que controla en tiempo real prácticamente todas las comunicaciones de un objetivo. El agente que gestiona el sistema –capaz de seguir simultáneamente todas las comunicaciones de 1.000 sospechosos- recibe en su ordenador un aviso de cualquier actividad o novedad que se produzca. Si recibe una llamada telefónica, el sistema le advertirá y le permitirá, por ejemplo, escucharla en tiempo real.

Aunque estos sistemas de última generación son capaces de interceptar llamadas telefónicas, SMS, conversaciones de chat, páginas web visitadas, foros de internet, conversaciones a través de voz IP, archivos descargados de la red, fax... Sin embargo, algunas comunicaciones como Skype o 'HTTPS' –webs 'seguras' que utilizan bancos y otras empresas- suponen un problema añadido: las comunicaciones están encriptadas y es necesario el uso de otras herramientas para descifrarlas.

Una de las funcionalidades más llamativas es la que ofrece la posibilidad de localizar geográficamente un teléfono móvil, almacenando el historial de lugares en los que ha estado. Se podrá comprobar, así, si el teléfono móvil de un sospechoso de terrorismo coincidió en el mismo lugar y en el mismo momento con el de otro sospechoso. Esta información queda registrada y almacenada, permitiendo así buscar coincidencias entre varios sujetos.



**Figura 6:** Esquema de la operatividad del Evident X-Stream. Fuente [www.elconfidencialdigital.com](http://www.elconfidencialdigital.com)



## 2.3. EL CASO PARTICULAR DE LA TELEFONÍA IP

Como se ha comentado ya, en los sistemas telefónicos tradicionales de conmutación de circuitos o de paquetes TDM/SS7 el servicio telefónico fijo como móvil se prestan mediante un conjunto de equipos, que en las redes de conmutación de circuitos antiguas o "legacy" se conocían como centrales telefónicas y en las NGN reciben otros nombres como enrutadores, pero que, con independencia de la técnica empleada, forman parte del sistema telefónico disponible al público (STDP) del operador. Dicho sistema dispone de técnicas y servicios para realizar interceptaciones legales automáticas por obligación legal.

Sin embargo, cuando se emplean técnicas de Telefonía IP de "Filosofía Internet", la cuestión es bastante más compleja<sup>4</sup>. Este es el caso en telefonía móvil de las aplicaciones OTT (Over The Top) como Skipe, WhatsApp o Movistar TuGo. En el contexto que nos ocupa, de interceptación legal de conversaciones y datos, cuando la conversación a interceptar se establece mediante telefonía IP, con protocolos de señalización normalizados como SIP que están absolutamente separados del flujo de datos, hay que diferenciar:

- Quién conoce que el sujeto tiene interceptadas las llamadas.
- Quién conoce el inicio de las sesiones.
- Quién proporciona el acceso a la red.

Puesto que pueden ser entidades diferentes, e incluso una de ellas (la que conoce el inicio de las sesiones) puede estar ubicada en países extranjeros, sujetas a jurisdicciones y ordenamientos legales diferentes del que emite la orden de interceptación. Y si el interceptado estuviese en RPV, estaría realmente conectado, mediante túnel y encriptación, por medio de un ISP diferente del de acceso.



En cuanto a quién conoce que el sujeto tiene interceptadas las llamadas, se puede afirmar que únicamente aquel operador (de acceso o de telefonía IP) que haya recibido una orden judicial conoce que el sujeto tiene interceptadas las llamadas.

Y hay que tener presente que en la Telefonía IP la señalización (el establecimiento de la sesión) está absolutamente separado del contenido (la voz e imágenes) que intercambian los interlocutores y que el acceso a la red es permanente o "always-on", y que además muy bien puede ocurrir que ambas funciones de acceso y telefonía IP estén prestadas por compañías diferentes.

<sup>4</sup> [http://wikitel.info/wiki/Telefon%C3%ADa\\_IP](http://wikitel.info/wiki/Telefon%C3%ADa_IP)

El acceso es un servicio bastante claro que tiene un ámbito geográfico concreto con puntos de acceso bien determinados, por tanto, generalmente será el operador de acceso quien reciba las órdenes de interceptación.

Sin embargo la señalización (SIP u otra) no está ceñida a un ámbito geográfico y puede tener un alcance global, sin limitaciones geográficas, es más difícil que un operador de Telefonía IP pueda hacer algo eficaz en cuanto a interceptación legal, más que registrar los metadatos. Por tanto, la interceptación física queda muy alejada de las posibilidades del Operador de Telefonía IP (el operador que proporciona y procesa la señalización SIP) y se ha de efectuar por el operador de acceso, sin que las personas que están comunicándose observen ningún cambio o alteración en sus comunicaciones.

No obstante, los jueces podrían exigir al operador de Telefonía IP que comunique al operador de acceso en tiempo real los intentos de inicio de sesión de aquellas de personas sujetas a órdenes de interceptación, es decir sus metadatos.

Además de lo anterior habría que saber si la persona a interceptar está en Red Privada Virtual, RPV o VPN (siglas en ingles), porque se ser así, estaría conectado en túnel con otro ISP, mediante encriptación, y sería imposible que el operador de acceso y los que intervengan en el transporte conozcan el contenido del tráfico y los metadatos.

También hay que tener presente que en algunos casos P2P como Skipe las llamadas no se resuelven en un punto bajo el control del operador. De hecho, en Skipe ni se conoce cuáles son los "supernodos" ni donde están situados, puesto que cambian dinámicamente. También el camino que sigue la "conversación" es completamente aleatorio: los paquetes de voz se generan el terminal del usuario y se enrutan por caminos impredecibles que pueden ser muy diferentes para unos paquetes que para otros, y muchos de ellos estarán fuera del ámbito del ISP e incluso del país donde se inicia o termina la llamada. Téngase en cuenta que mientras en la telefonía tradicional hay centrales con fuertes inversiones (donde se puede interceptar) en los servicios IP las inversiones e inteligencia de la red están en la periferia, realizadas por los propios usuarios, y las conversaciones se establecen extremo a extremo, por tanto no se dispone de ningún elemento central para efectuar la interceptación [6].

Los ISP y operadores de acceso pueden instalar "controladores de frontera" que, entre otras funciones, sirven para efectuar la interceptación de datos dentro del ámbito del ISP, pero conviene que se les alerte en tiempo real de los metadatos de la persona sujeta a interceptación.

La problemática de la Telefonía IP se complica por el hecho que al intentar establecer una llamada el timbre puede sonar en múltiples destinos simultáneamente, a lo amplio del mundo. La llamada se establecerá con el punto que primero descuelgue. Además, el que las conversaciones pueden estar encriptadas o codificadas aumenta la complejidad del problema y dificulta la interceptación, pudiendo llegar a hacerla imposible en sentido táctico.

## 3. INTERCEPTACIÓN MALICIOSA DE LLAMADAS Y SMS

### 3.1. TELEFONÍA 2G

La primera generación de telefonía digital, GSM, lleva más de 20 años en servicio (Desde 1995 en España) y no ha sufrido ningún tipo de revisión. Existen varias debilidades pero las que permiten la interceptación son dos; Por un lado la falta de autenticación entre las estaciones base de la red (lo que permite meter una estación base falsa) y por otro que el algoritmo de cifrado a5/1 ha quedado obsoleto tras 20 años de aumento en la potencia de computación de los ordenadores disponibles en el mercado de consumo.

Estas dos debilidades dan lugar a los dos métodos de interceptación:

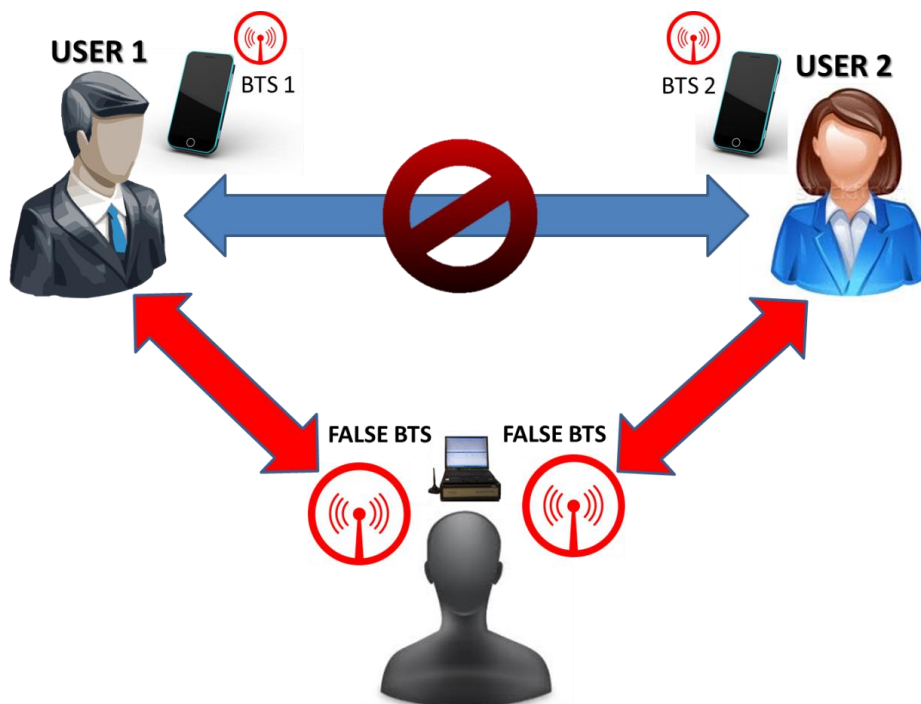
- Mediante ataque de Man-In-The-Middle (IMSI Catchers).
- Mediante captura de los datagramas de la conversación y su posterior descifrado.

### 3.2. MAN IN THE MIDDLE



El ataque de Man-In-The-Middle de GSM se basa en que la configuración por defecto de los terminales hace que estos se conecten a la estación base (BTS) cuya señal resulta más potente.

De este modo, se monta una BTS falsa, se emite hacia la víctima con mucha potencia y se espera a que su terminal se conecte. El tráfico que genere la víctima se re-envía a la estación base real a través de un repetidor. Al negociar la conexión entre el terminal y la estación base falsa, se obliga al terminal a que deshabilite el cifrado, pudiendo capturar así la conversación en claro y en tiempo real.



**Figura 7:** Representación gráfica del ataque. Fuente: Elaboración Propia

Los IMSI-catchers son una técnica utilizada por los cuerpos policiales para investigar y vigilar a activistas políticos o « grupos de interés ». Un IMSI-catcher es un dispositivo que se puede instalar por ejemplo en una furgoneta, y que se hace pasar por la antena de un operador de telefonía móvil. Permite la extracción de identidades de celulares en su área de cobertura (cuando estas identidades son desconocidas) y detectar la presencia de teléfonos celulares conocidos en el área, el sistema notificara al usuario sobre la presencia de los teléfonos.

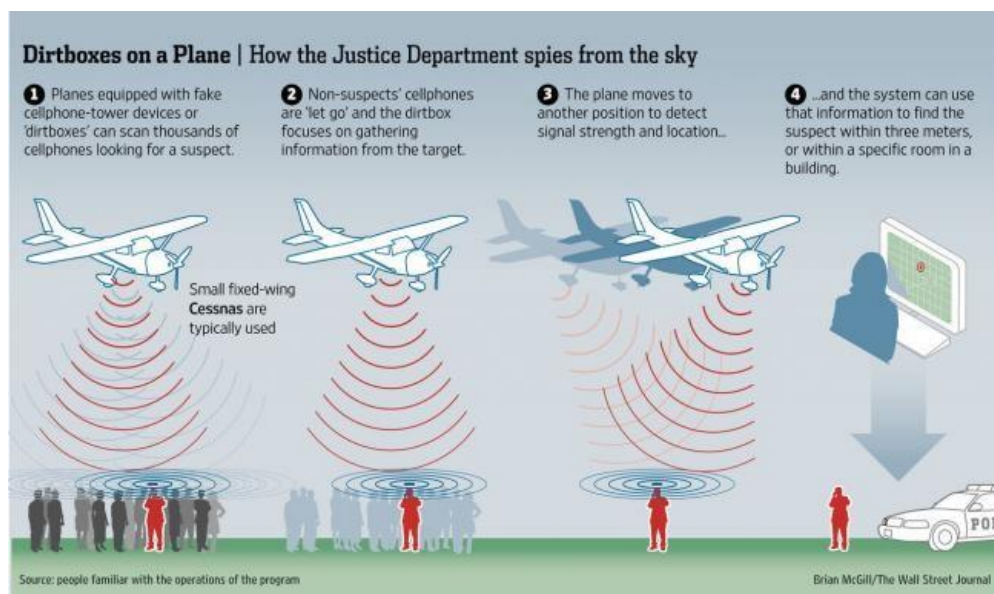
Por tanto este dispositivo permite extraer la IMSI e IMEI de sistemas GSM MS en su área de cobertura (así como algunos datos adicionales). Esto permite a los usuarios que cuentan con una base de datos de IMSI y del IMEI identificar los objetivos potenciales activos en el área y recopilar la información adicional sobre ellos (a través de otras aplicaciones). Una vez instalado, los móviles del operador al que se suplanta en la zona de cobertura del IMSI Catcher se conectarán automáticamente con esta antena de mentira. De esta manera, sirve de dispositivo de localización y de identificación en tiempo real de todos los móviles encendidos de la zona, que aunque no participen en ninguna comunicación, se registran con él y le mandan sus informaciones de identificación (número de teléfono y número de aparato).

El sistema fijo o de vehículo puede ser alimentado desde una fuente externa, la unidad funcionara durante horas con un conjunto de baterías internas que puede ser recargadas o remplazadas cuando sea necesario. La unidad puede ser embalada en bolsas estándar o maletas o montada en un vehículo para permitir operar en zonas pobladas. El equipamiento radio del IMSI Catcher soporta hasta 4 bandas GSM (850, 900, 1800, 1900), haciéndolo aplicable a cualquier sitio en el mundo que cuenta con una red GSM. El módulo 3G soporta hasta 5 bandas UMTS (2100, 1900, 1700, 900, 850).



**Figura 8:** Escuchas utilizando IMSI Catcher. Fuente [www.computerworld.com](http://www.computerworld.com)

El IMSI-catcher puede también retransmitir las comunicaciones hacia afuera de un móvil en concreto de tal manera que no pueda percibir su presencia. Tendrá acceso directo al contenido de estas comunicaciones emitidas que retransmite y puede así servir de dispositivo de escucha en vivo. Pero algunos indicios permiten detectar los IMSI-catchers. Por ejemplo, los móviles conectados con un IMSI-catcher no pueden recibir ninguna comunicación de la red. Esta técnica fue utilizada, por ejemplo, para vigilar las preparaciones y las acciones de las contrasumbres del G8 y de la OTAN de estos últimos años.



**Figura 9:** Esquema de uso de IMSI Catcher por US Justice Department. Fuente Wall Street Journal

Así recientemente el diario Wall Street Journal aseguraba haber descubierto que el Departamento de Justicia de EEUU los ha instalado en aviones. El IMSI-catcher finge ser una antena de telefonía, al que cada móvil encendido dentro de su rango de alcance se intenta conectar por ser la "torre" más cercana. Cuando el teléfono manda una petición de conexión, el aparato en cuestión obtiene su número de móvil. Las autoridades descartan, supuestamente, aquellos números que no se correspondan con los del sospechoso.

Para localizar el teléfono que sí es objeto de investigación, el avión se mueve y ve cómo varía la potencia de la señal. Al final, son capaces de localizar el móvil en cuestión (y, por tanto, al sospechoso si lo lleva con él) con una precisión de tres metros.

Este programa, que lleva en funcionamiento desde 2007, utiliza aviones de tipo Cessna, aunque se desconoce el número de aeronaves equipadas con estos dispositivos. Tienen presencia, eso sí, en más de cinco aeropuertos, desde los que pueden cubrir la mayor parte de la superficie de Estados Unidos. Para ahorrar tiempo, y siempre según el WSJ, en cada pasada que hacen buscan el móvil de varios sospechosos a la vez.

### 3.3. CAPTURA Y DES-ENCRIPCIÓN 2G / 3G



Esto es un extracto del blog de Lázaro Escudero (<http://www.tierradelazaro.com>). Accede a los siguientes documentos donde encontrarás más información que la aquí mostrada <http://www.tierradelazaro.com/cripto/gsm.htm> y <http://www.tierradelazaro.com/cripto/3g.htm>

#### 3.3.1. INTRODUCCIÓN



Este método es mucho más complejo y surgió a partir de 2003 cuando se consiguió romper el algoritmo de cifrado mediante pre-computación de todo el espacio de claves (16 Trillones de claves posibles).

La comunicación en GSM se establece en dos direcciones, del terminal a la BTS (Uplink) y de la BTS al terminal (Downlink). La voz de la víctima viaja por uplink y la voz de la persona con la que habla viaja por Downlink. Además, el canal que



se usa tanto en downlink como en uplink va cambiando para hacer que sea más compleja la interceptación, esto se llama "Channel Hopping".

Para interceptar usando este método se necesitan cuatro dispositivos receptores GSM. Dos dispositivos se usan para "escuchar" la señalización entre BTS y terminal y controlar el salto de canales y otros dos dispositivos se usan para capturar los datagramas, cambiándolos de canal según sea necesario a lo largo de toda la llamada.

Una vez capturada la conversación, se des-encrpta calculando la clave de cifrado (KC) utilizada. Para evitar este tipo de ataques, se recomienda realizar llamadas con el 3G habilitado, cuyo cifrado es mas robusto y no es vulnerable (por ahora). A continuación se muestra una imagen de una estación falsa, presentada en el congreso de Seguridad Defcon. El presupuesto necesario para llevarlo a cabo rondó los 1.000€.



**Figura 10:** Chris Paget creó una BTS falsa que interceptó las llamadas de 30 personas. Extraído de DefCon 2010

En un principio, los algoritmos de la telefonía de tercera generación fueron mantenidos en secreto, como ya pasó con los del GSM. Pero en Septiembre de 2000, la ETSI realizó un comunicado en el que mostraban los algoritmos de confidencialidad, F8, e integridad, F9, que protegen el tramo radio en las comunicaciones 3G. Este sistema de comunicación sólo se usa para el tramo que está entre el nodo de la operadora de telefonía y el móvil del usuario, para el resto de los tramos hasta llegar al receptor, la comunicación está a cargo de la operadora y no está cifrada. También se han hecho públicos los detalles de funcionamiento del conjunto de algoritmos para autenticación y generación de claves: F1, F1\*,

F2, F3, F4, F5 y F5\*. En el caso de 3G, el conjunto de algoritmos de autenticación y generación de claves sugerido como ejemplo se denomina MILENAGE.

Este conjunto denomina MILENAGE está construido alrededor del cifrado Rijndael y que después se convirtió en el AES, Advanced Encryption Standard elegido por el NIST, Instituto Nacional de Estándares y Tecnología, de los EEUU como su sistema de cifrado universal. Existían buenos motivos para elegir Rijndael: tiene clave de 128 bits, ha sido bien estudiado, es de dominio público, es decir, carece de patentes que puedan limitar su uso, es eficiente tanto en funcionando en hardware como en software, y es el sucesor del cifrado DES. Esto último significa que Rijndael ya sido extensamente atacado por la comunicad criptográfica.

Como contrapartida, la confidencialidad e integridad en el intervalo aéreo (entre el móvil y la estación base o nodo de la operadora) es tarea reservada al algoritmo KASUMI y no sobre el AES. KASUMI, también llamado A5/3, es una unidad de cifrado por bloques utilizada en algoritmos de confidencialidad, F8, e integridad, F9, para Telefonía móvil por 3GPP. KASUMI fue diseñado por el grupo SAGE (Security Algorithms Group of Experts), que forma parte del organismo de estándares europeos ETSI. Debido a las presiones por la seguridad del algoritmo y por la falta de tiempo, en lugar de inventar un cifrado desde cero, SAGE tomó un algoritmo existente llamado MISTY1, y para su implementación en hardware, se le realizaron algunas modificaciones. De allí que MISTY1 y KASUMI sean muy similares, de manera que los análisis disponibles sobre uno se adaptan fácilmente al otro y el tiempo empleado por el SAGE para comprobar la robustez de su algoritmo se reduzca considerablemente.



No hay publicaciones sobre ataques a MISTY1, ni tampoco se han detectado graves vulnerabilidades, por tanto podemos decir que MISTY1 es un sistema criptográfico bueno, por desgracia no podemos decir lo mismo de su pariente KASUMI al que ya desde hace tiempo se le han encontrado debilidades. SAGE modificó MISTY1 para que la implementación en hardware fuera más sencilla y según afirman ellos, no pretendían bajar su seguridad, pero lo cierto es que sí que lo han hecho. Y ya en 2001, Kühn presentó un ataque contra KASUMI.

### 3.3.2. ATAQUES 1G/2G:

Con el advenimiento de la telefonía móvil, el cifrado se convirtió en una necesidad. Para pinchar un teléfono fijo, antiguamente había que introducirse físicamente en el sistema, sea en la central telefónica, en los cables de transmisión o en uno de los teléfonos que se quiere intervenir. Pero si usamos un teléfono móvil, el tramo final de la conversación, entre el nodo y el móvil, tiene lugar en el



aire mediante microondas. Estas pueden ser captadas con un receptor adecuado y si están en claro, se pueden escuchar y por tanto saber que se está diciendo o haciendo.

Los teléfonos móviles de primera generación, como era el sistema de Moviline, carecían de protección contra escuchas ilegales. Ejemplo de esta debilidad del sistema fueron las escuchas a Txiqui Benegas del PSOE y su posterior publicación en los medios de comunicación.

La segunda generación de telefonía móvil, la 2G o GSM usa tecnología digital más segura, porque al usar envío de datos digitales las señales se pueden cifrar a conveniencia. También por esa fecha se perfeccionan los sistemas de autenticación, de manera que nadie podía clonar un móvil y hacerse pasar por otro. Esto no significa que este encriptado se cifre durante todo el recorrido de la llamada, lo que se conoce por un cifrado punto a punto, sino solamente entre la estación base, la antena nodo a la que se conecta el móvil, y el teléfono del usuario; el resto del camino la señal va sin cifrar y por tanto se pueden pinchar los teléfonos como antaño en la central telefónica.

El sistema GSM fue desarrollado por el Instituto Europeo de Estándares en Telecomunicaciones ETSI para proporcionar un estándar común a los sistemas de telefonía móvil en Europa. Se incluyeron un conjunto de protocolos criptográficos para proporcionar tanto confidencialidad como autenticación:

- a) A3: Es el algoritmo de autenticación. Es el que hace que cada teléfono móvil sea único. Identifica al móvil y con la base de datos de la operadora se puede asociar al usuario propietario. Permite, entre otras cosas, saber a quién hay que cobrar la llamada.
- b) A5: Es el algoritmo de cifrado de voz. Gracias a él, la conversación va encriptada. Se trata de un algoritmo de flujo con una clave de 64 bits. Hay dos versiones, denominadas A5/1, y A5/2; esta última es la versión autorizada para la exportación, y en consecuencia resulta más fácil de atacar. En la actualidad hay otra versión, la A5/3 o KASUMI, que se usa en la tecnología 3G.
- c) A8: Es el algoritmo que genera claves tanto para autenticación, el A3, como para encriptación, el A5. Básicamente, se trata de una función unidireccional parecida a las funciones hash, del tipo MD5 o SHA-1, que permiten la firma digital en los documentos electrónicos.
- d) COMP128: Es un algoritmo que permite funcionar a los A3 y A8. No es el único posible, pero sí uno de los más usados.

Cada vez que un usuario de la tecnología GSM realiza una llamada, primero inserta su número PIN y después marca el número al que quiere llamar. Esto provoca que su terminal tome de la tarjeta SIM una clave que está almacenada en su interior (clave Ki). A continuación, el teléfono toma ciertos datos aleatorios que se intercambian entre éste y la estación base más cercana (semilla aleatoria / random seed): El conjunto clave + semilla son transformados mediante el algo-

ritmo de autenticación A3 y el resultado de dicha transformación es enviada a la estación base.

La operadora, con su base de datos y el Ki (que está almacenado a disposición de su operadora) y autentifica la identidad de quien llama, comprobando que es el propietario legítimo y los servicios contratados por éste. Seguidamente la estación base da vía libre a la comunicación. Toma la clave del teléfono Ki y otra semilla aleatoria para crear una clave de sesión Kc, de 64 bits de longitud. Esa clave es usada para encriptar la comunicación, gracias al algoritmo A5.

Adicionalmente, cada vez que se usa el A3 y el A5 interviene el A8, que es el algoritmo que genera resúmenes. La autenticación de la llamada recae sobre el algoritmo A3, en tanto que la confidencialidad es tarea del algoritmo A5. Ambos algoritmos requieren de una clave, generada mediante el algoritmo A8. De hecho, los algoritmos A3 y A8 suelen tratarse prácticamente como si fuesen uno solo.



En la especificación de GSM se utilizó el algoritmo COMP128 como ejemplo de uso para A3 y A8, pudiéndose usar otros. Sin embargo la gran mayoría de las telecom implementaron COMP128, es decir, usaron el algoritmo que venía como ejemplo en esas especificaciones. El problema es que a últimos del 2009 este algoritmo COMP128 fue roto y dejó al descubierto todas las comunicaciones GSM que usan este algoritmo.

Un ingeniero alemán anunció en 2009 que había logrado romper el sistema de seguridad utilizado para cifrar las comunicaciones de los teléfonos móviles que operan bajo el sistema GSM: Karsten Nohl, de la Universidad de Virginia, hizo el anuncio en el Chaos Communication Congress de Berlín.

Para este ataque, Nohl y sus colaboradores crearon un fichero de unos dos Terabytes conteniendo todas las claves válidas (rainbow table), con el que cualquier persona con buenos conocimientos de informática puede violar el sistema GSM sin necesidad de tener que utilizar ningún sistema de fuerza bruta que pruebe con todas las combinaciones posibles. Si bien el hacker se negó a proporcionar el enlace que permita descargar dicho fichero, se sabe que el codiciado archivo ya circulaba por el año 2010 por las redes P2P, en emule, amule y BitTorrent. Además de esta tabla, para interceptar una comunicación GSM se necesita un receptor de radio que opere en la misma frecuencia que los teléfonos móviles y un software especial para el procesamiento de las señales capturadas.

También por ese año, Karsten Nohl y su compañero Sylvain Munaut con una pila de viejos teléfonos Motorola realizaron una demostración a la BBC de localización de un terminal GSM. Desde su ordenador localizaron un móvil específico, siguieron sus movimientos desde una distancia superior a 500 metros y guardaron copia de las conversaciones hechas desde él. Demostraron con ello que el ataque al sistema GSM es una realidad y no una teoría. Sus herramientas de trabajo son una computadora portátil y un modelo específico de teléfonos Moto-

rola cuyo sistema operativo base, su firmware, había sido desentrañado y sus detalles publicados en Internet. Los programadores utilizaron esa información para crear un programa propio que les permite obtener información técnica oculta de las torres de telefonía celular.

Pero las debilidades de este sistema GSM no terminaron aquí, ya a últimos del siglo XX se realizaron ataques al A3. Puesto que A3 es el algoritmo de autenticación, su ruptura permitiría clonar teléfonos; es decir, hacer que un tercero utilizase el mismo número de teléfono que otro y le cargase a éste las facturas. En Abril de 1998, se publicó la noticia de que Ian Goldberg y David Wagner del grupo ISAAC de la Universidad de Berkeley, junto con Marc Briceno de la Smartcard Developer Association consiguieron clonar un móvil que usaba COMP128 como algoritmo de A3 y A8. Lo que hicieron se denomina ataque mediante texto escogido. Básicamente, interrogaban al teléfono de forma controlada. Cotejando los datos emitidos por el móvil, los investigadores consiguieron obtener la clave Ki, que como vimos anteriormente se utilizaba para la autenticación y la identificación del cliente final.

El proceso requiere acceso físico al teléfono, cierto equipo informático y un proceso de interacción con el teléfono de unas 8 horas de duración con los ordenadores de la época. Sin embargo un ataque interactuando en el segmento radio, sin acceso físico, no es imposible. De hecho, los investigadores no clonaron un móvil en el aire, no porque no fuese técnicamente posible, sino porque es ilegal. Esto se podría hacer usando una estación falsa que se dedicase a interrogar a todo móvil que permaneciese unas cuantas horas en su radio de acción.



De esta manera ya a finales del siglo pasado se había demostrado que el algoritmo COMP128 usado por A3 resulta vulnerable. Resulta especialmente llamativo el hecho de que COMP128 fuese un algoritmo secreto, por lo que los investigadores consiguieron recomponerlo mediante técnicas de ingeniería inversa y diversos documentos.

Por otro lado, también se ha atacado el A5. Si el conocimiento de la clave Ki permite clonar teléfonos, también permite descifrar la conversación en el segmento radio. Esto es posible porque la clave de sesión Kc, usada para cifrar esa llamada únicamente, se obtiene mediante la clave Ki y una semilla aleatoria. En principio hay que obtener esa semilla para cada conversación, y hay que recordar que el ataque anteriormente descrito requiera horas o días (y solamente son vulnerables los sistemas que utilicen el algoritmo COMP128 para autenticación y generación de claves).

Como ya se ha dicho, la clave de sesión Kc, usada por el algoritmo A5 para cifrar las llamadas, tiene una longitud de 64 bits. Esto significa que, si el algoritmo estuviese bien diseñado, un atacante tendría que probar las  $2^{64}$  combinaciones posibles de claves para descifrar el mensaje, que teóricamente no es posible salvo para organizaciones con una elevada capacidad de proceso. Sin embargo, Goldberg, Wagner y Briceno demostraron que de los 64 bits de la clave de sesión Kc, diez de ellos son siempre iguales a cero. Este debilitamiento, aparente-

mente deliberado, de la clave, pone las cosas  $2^{10} = 1.024$  veces más fáciles a un atacante interesado.

Este debilitamiento se vio en todas las implementaciones del algoritmo generador de claves A8, incluso las que no usaban COMP128. Es decir, parece ser una característica global a toda la infraestructura GSM. Hay un ataque cripto analítico que requiere un total de  $2^{40}$  cifrados, y entre  $2^{40}$  y  $2^{45}$  operaciones informáticas, al alcance de los ordenadores actuales de alta velocidad, o bien de chips contruidos a tal efecto.

En Diciembre de 1999, los investigadores israelíes Alex Biryukov y Adi Shamir (la S en RSA) lanzaron un ataque cripto analítico sobre A5/1 aprovechando ciertos fallos. Con el título de Criptoanálisis de A5/1 en tiempo real con un PC, el artículo de Biryukov y Shamir demostró que se pueden descifrar conversaciones cifradas mediante A5/1 con relativa facilidad y sin grandes equipos informáticos: un ordenador personal con 128 Mb de RAM, una capacidad de almacenamiento equivalente a entre 150 y 300 Gb y un escáner digital para capturar la señal.

El ataque precisa de una etapa de cálculo previo consistente en unos  $2^{48}$  pasos, que solamente ha de llevarse a cabo una vez. Una vez hecho, el atacante puede elegir entre diversos tipos de ataque. En uno de ellos se precisa el equivalente a un par de segundos de conversación cifrada, y el ataque requiere unos minutos. En otro, es preciso obtener dos minutos de conversación, pero el tiempo del ataque se reduce a apenas un segundo (¡se puede decir que es en tiempo real!).

### 3.3.3. ATAQUES 3G.

Los siguientes es un repaso a los diferentes ataques realizados contra el cifrado en telefonía 3G:

- a) En 2001, un ataque diferencial imposible en seis rondas de la versión de A5/3 o KASUMI, que se usa en la tecnología 3G fue presentado por Kuhn.
- b) En 2003 Elad Barkan, Eli Biham y Nathan Keller demostraron que existe un ataque de MiM (Man in the Midle) contra el protocolo del GSM que evita el algoritmo A5/3 y con ello pueden romper el protocolo. Este método no ataca el A5/3, pero consiguen evitarlo. La versión completa de su trabajo fue publicado a finales de 2006.
- c) En 2005, los investigadores israelíes Eli Biham , Orr Dunkelman y Nathan Keller publicaron un ataque tipo boomerang contra KASUMI que puede romper las 8 rondas más rápido que la búsqueda exhaustiva por fuerza bruta. El ataque requiere el análisis de muchos textos y necesita mucho tiempo computacional. Si bien esto no es un ataque práctico, invalida algunas pruebas sobre la seguridad de los protocolos 3GPP que se había basado en la supuesta fuerza de KASUMI.

- d) Pero sin duda el ataque que más repercusión ha tenido es el realizado por Shamir y sus compañeros en 2010. Recordemos que Shamir es la S del sistema de cifrado RSA y por tanto toda una autoridad en la materia.

Orr Dunkelman, Nathan Keller y Adi Shamir publicaron en 2010 un trabajo titulado A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony «Un ataque práctico en cuanto a tiempo sobre el cripto sistema A5/3 empleado en telefonía 3G».



Los científicos han conseguido atacar el algoritmo con un PC convencional y romper el sistema de cifrado en unas dos horas. Eso no es tiempo real, pero dicen que se puede mejorar todavía considerablemente, dando lugar a la posibilidad de interceptar las comunicaciones completas de los teléfonos inteligentes y las transmisiones a través de Internet en las redes 3G.

El algoritmo propuesto para el ataque es una variación del ataque boomerang al que los autores han denominado ataque sandwich. En líneas generales el ataque consiste en enviar múltiples valores de entrada a través del proceso de cifrado con diferencias controladas de algunos bits entre ellas. A continuación se analizan pares de entradas y sus resultados para detectar similitudes entre las claves. Las similitudes permiten a los autores del estudio determinar en qué momento se utilizan claves de cifrado relacionadas, e identificar algunos de los bits de esas claves. Estas operaciones se van repitiendo y en cada paso se mejora el conocimiento que se dispone de la clave de cifrado.

Según la documentación del estudio, el algoritmo que utilizaron fue capaz de recuperar 96 de los bits de las claves en apenas unos minutos usando un PC normal, y los 128 bits al completo en menos de dos horas. Y todo ello a pesar de utilizar una versión de borrador del programa de descifrado, no optimizado, por lo que los tiempos podrían reducirse. Este ataque es de una complejidad tan baja que demuestra que los cambios realizados para simplificar MISTY1 han debilitado muchísimo el sistema de cifrado.

Otro ataque es el que realizaron Investigadores de la Universidad de Birmingham junto a la Universidad Técnica de Berlín; ellos realizaron un estudio donde dieron a conocer graves fallos de seguridad en los códigos que conectan los teléfonos a las redes 3G, las que permitirían a cualquiera rastrear la ubicación del móvil de forma precisa y sin enterarnos. El ataque se hace con un nodo de la operadora infestado o duplicado, una especie de hotspot para redes UMTS, y una segunda persona que ayude a identificar específicamente el dispositivo a hackear.

En primer lugar el atacante puede forzar a los dispositivos móviles a revelar su TMSI (Identificador Temporal del Abonado Móvil, Temporary Mobile Subscriber Identity), asumiendo que es conocido el número IMSI (Identidad Internacional del Abonado a un Móvil, International Mobile Subscriber Identity). En segundo lugar, el atacante puede obtener el AKA (mecanismo de respuesta en redes UMTS, Authentication and Key Agreement) de un teléfono específico, porque al enviar una solicitud a todos los teléfonos celulares en cierta distancia, todos responden

con problemas de sincronización excepto el teléfono atacado, distinguiéndolo inmediatamente, lo que permitiría incluso rastrear los movimientos al interior de un edificio.



Todos estos ataques nos dicen que el sistema de comunicación 3G es débil, más débil de lo que creen sus creadores, y aunque no hay una ruptura de este algoritmo en tiempo real como sucede con GSM sí que es un toque de atención para que las operadoras cambien de tecnología y adopten algoritmos más fuertes.

## 4. CASO PRACTICO DE ANÁLISIS PARA LA DETECCIÓN DE TELÉFONOS INTERVENIDOS/INTERCEPTADOS

### 4.1. INTRODUCCIÓN



Accede al siguiente documento, que seguro te va a ayudar:  
<https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html>

Como se ha visto en secciones anteriores, hoy los móviles ya casi no se intervienen en el propio dispositivo, sino que se intervienen en la red. Es cierto que pueden ser intervenidos mediante la alteración de su tarjeta SIM, introduciéndoles sistemas de escucha o instalando en ellos software especialmente destinado a interceptar llamadas, como por ejemplo FlexiSpy, que se vendía en su día con el reclamo de ser un método práctico para inutilizar o monitorizar tu móvil si lo roban. También existen los “móviles espías”, que se venden con el pretexto de controlar las llamadas de hijos.

Sin embargo, hoy en día el método de intervención de llamadas más frecuente en los móviles es el rastreo de la señal y es imposible detectarlo. Además, ese método de espionaje precisa de medios más o menos asequibles e incluso existe software para romper el cifrado A5/1 que usan las comunicaciones GSM de los móviles actuales. Para hacer frente a esta amenaza existen en el mercado varias soluciones, como el software de encriptación para móviles e incluso los móviles encriptados.



Existe otro aspecto a tratar sobre el espionaje a los móviles y que desarrollaremos a continuación. Se trata de la técnica que se conoce como roving bug o escucha itinerante (activado remoto del micrófono del móvil). Sobre la misma existencia de esta técnica de espionaje se ha especulado mucho durante años, siendo la primera noticia de su utilización en España fue en 2006. Las especulaciones terminaron cuando en diciembre de 2006 un juez de EEUU reconoció que el FBI había activado remotamente los micrófonos de los móviles de una banda de mafiosos.

El roving bug consiste, por tanto, en activar el micrófono de un móvil de forma remota, aunque esté apagado, para utilizarlo como método de escucha. Aunque la técnica permanece en secreto, en principio todo indica que hace falta la instalación en él de un software que lo permita, bien físicamente o recibiendo un sms que lo contenga (al igual que los virus informáticos). Otra técnica consiste utilizar el hecho que muchos móviles se activan si está programada una alarma a determinada hora y esto tal vez pueda usarse para convertirlos en micrófonos sin que su dueño se entere.

De momento, existen tres formas de saber si un móvil está siendo usado como un roving bug, pues la activación remota del micrófono no se traduce en símbolo alguno en la pantalla del aparato. El primero es vigilar el consumo de energía: si el móvil consume batería más rápido de lo normal en reposo, es posible que el micrófono haya sido activado a distancia. También se puede notar ese uso en el calentamiento del móvil entre llamadas, al estar procesando más información de lo habitual en estado de reposo. Otro indicio es escuchar en el altavoz de una radio, de un televisor o de un ordenador la típica interferencia que provocan los móviles al recibir una llamada o un sms. Si un móvil en reposo produce continuamente esa interferencia tal vez esté remitiendo datos -los que recoge su micrófono- de forma furtiva.

Obviamente, la mejor forma de evitar el espionaje mediante roving bug es dejar el móvil fuera de la sala en la que se mantenga una reunión en la que se intercambie información delicada, o bien directamente sacarle la batería al móvil mientras dure esa reunión, pues el micrófono de tu móvil precisa de la energía de la batería para funcionar.

## 4.2. EJEMPLO FLEXISPY



Flexispy es, en realidad, un Troyano desarrollado para el sistema operativo Symbian Series 60.

Este SO inicialmente diseñado para utilizado por móviles Nokia, y es vulnerado por el archivo Spy.Flexispy.A, permitiendo la recopilación de información de llamadas, mensajes, agenda y correo, en la actualidad FlexiSpy funciona con iPhone, iPad, Nokia Symbian, Blackberry, Android y Android Tablet. Una vez instala-



do, Flexispy puede examinar, registrar y reportar el uso del móvil por bluetooth o a un servidor de Internet. La interfaz queda oculta y sólo puede accederse a ella al ingresar una secuencia especial de dígitos (que, por supuesto, sólo conoce la persona que instaló el Flexispy). A través de la interfaz se configuran las aplicaciones que serán monitorizadas y qué información será almacenada.

FlexiSpy es un producto de pago. Recientemente se está ofreciendo la posibilidad de instalación remota, aunque otra posibilidad es accediendo al dispositivo. Una vez que el usuario contrata el producto, la empresa envía el archivo por mail y, a su vez, provee una dirección URL para la descarga. El software puede instalarse a través de USB, Bluetooth, infrarrojo o por OTA (conexión por aire). La forma más sencilla de instalar el producto es utilizando OTA. Se ingresa la URL provista en el navegador del móvil a espiar, y al darle “sí” (o “conectar”) se inicia la instalación, concluyendo con un mensaje de “instalación completa”. Al salir del navegador, el software ya estará activo en el móvil.

Todos los datos que se recopilen del móvil serán enviados al servidor de FlexiSpy, y el usuario podrá acceder a los mismos a través de [www.flexispy.com](http://www.flexispy.com). Deberá loguearse con su cuenta de correo electrónico y clave (los que haya informado al momento de contratar el producto). Los reportes se muestran en una tabla con los siguientes datos:

- a) Ubicación: IMEI, Hora Cliente, Hora servidor, Tipo de evento, Ubicación (latitud y longitud), ID del móvil, Nombre del móvil, Información de la red (ID, nombre, código de país, código de área)
- b) Mails: IMEI, Hora cliente, Hora servidor, Tipo de evento, Dirección (saliente/entrante), Tamaño, Nombre del contacto, Destinatario, Asunto, Contenido del mensaje
- c) SMS: IMEI, Hora cliente, Hora servidor, Tipo de evento, Dirección (saliente/entrante), Número de móvil, Nombre del contacto, Contenido del mensaje
- d) Llamadas: IMEI, Hora cliente, Hora servidor, Tipo de evento, Dirección (saliente/entrante), Duración de llamada, Número de teléfono, Nombre del contacto.



Figura 11: Panel de Control. Fuente: [www.flexispy.com](http://www.flexispy.com)

## 4.3. OTROS SOFTWARE ESPÍA.

### 4.3.1. mSPY

mSpy es un software espía para espiar y rastrear teléfonos móviles con una gran lista de funciones. Tiene funciones que permiten monitorizar llamadas, espiar mensajes de texto, rastrear la ubicación de los teléfonos con el GPS, controlar el calendario, vigilar mensajes instantáneos y ver fotos/vídeos realizados con el teléfono.

- a) Bloquear páginas web y aplicaciones: Con mSpy podrá analizar su historial de navegación, ver qué páginas han visitados e introducir las URLs y aplicaciones que desea bloquear.
- b) Capacidad para realizar el registro de las teclas pulsadas: Poder tener un registro de las teclas pulsadas es muy útil ya que puede registrar cualquier mensaje del teléfono monitorizado — incluso aquellos enviados en aplicaciones de chat no soportadas por mSpy. Esta función solamente está disponible para dispositivos Android.
- c) Restringir llamadas entrantes.
- d) Geo-cercas: La función para crear geo-cercas le permite saber si el usuario están entrado o saliendo de una ubicación marcada como restringida.
- e) Redes Wi-Fi: Coordenadas más precisas del dispositivo recogiendo la información sobre cada red Wi-Fi a la que se conecta el teléfono vigilado.

### 4.3.2. HIGHSTER MOBILE

Permite monitorizar todos los aspectos de un teléfono móvil, aunque no tiene funciones tan avanzadas como FlexiSPY Extreme o mSpy:

- a) Monitorización de Redes Sociales: Monitoriza WhatsApp, Facebook, Twitter, iMessage, BBM, Skype, Viber, Instagram y correos electrónicos.
- b) Rastreo GPS en tiempo real: Dónde está el dispositivo en todo momento con la tecnología de rastreo GPS. La ubicación aparece en un mapa en el panel de control.

- c) Cámara oculta: Inicio de la cámara del teléfono para realizar fotos secretas que serán enviadas a su cuenta.
- d) Monitor de llamadas: Monitorizar llamadas recibidas y enviadas, la fecha y la hora, el número de la persona que llama o a la que ha llamado, y registro activo con todas las llamadas realizadas.
- e) Registro de fotos y vídeo: Ver las fotos y vídeos realizados en el teléfono móvil que está monitorizando.
- f) Historial de navegación: Ver todas las páginas web visitadas desde el teléfono.
- g) Contactos y calendario: Ver los nuevos contactos y las entradas del calendario.
- h) Monitorización de mensajes de texto: Grabar y registrar todos los mensajes de texto SMS. Mantiene un registro de todos los mensajes de textos enviados y recibidos y pueden verse dentro del panel de control.

## 4.4. EJEMPLO DE DETECCIÓN

Estos software se venden como indetectables, pero ¿es cierto?. Veamos lo que ocurre con FlexiSpy en el caso de iPhone.



Como se ha comentado, para el mundo iPhone también se han creado soluciones, aunque la mayoría de ellas requieren hacer jailbreak al dispositivo e instalarlo físicamente, como es el caso de FlexiSpy.

El funcionamiento es sencillo: Se instala el troyano en el terminal con jailbreak, y éste se ocultará para hacerse invisible en el sistema con el objetivo de que la víctima no pueda darse cuenta de que hay algo nuevo en el iPhone. A partir de ese momento, todo lo que haga con el teléfono será registrado en un servidor y el atacante podrá revisar todos los datos recolectados desde una página web.

Para analizar su existencia una de las mejores maneras es utilizar software anti-spyware. Como este tipo de herramientas, a pesar de que se venden como indetectables, hace tiempo que son estudiadas por los analistas forenses, existen soluciones como Oxygen Forensics que buscan y encuentran una larga cantidad de ellas, por lo que no son tan indetectables. Más adelante veremos este software con mayor detalle.

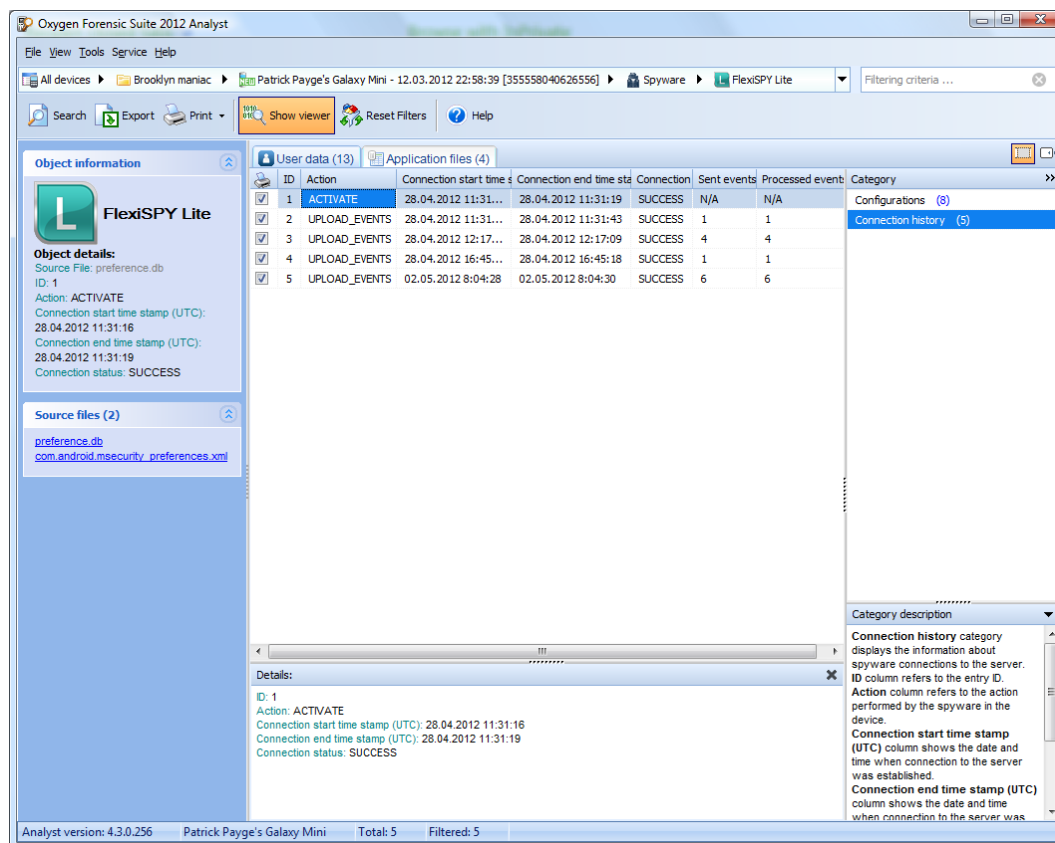


Figura 12: Panel de Control Oxygen Forensics. Fuente: [www.oxygen-forensic.com](http://www.oxygen-forensic.com)

Por tanto, como conclusión, en terminales iPhone lo mejor es tener controlado físicamente el terminal, con passcode complejo, actualizado a la última versión y sin jailbreak. En el caso de terminales Android, además evitar bajar apps con permisos extraños para la misma, poner un antimalware y evita rootear el teléfono... y cuidado con versiones no directas del fabricante de aplicaciones populares como WhatsApp.

## 4.5. EJEMPLO ANÁLISIS IMSI CATCHER

Vamos a ver un caso de análisis de terminal del que se sospecha ha sido objeto de un IMSI Catcher. Con el fin de descubrir si el dispositivo se encuentra intervenido con una estación falsa podemos analizar los "logs" del mismo, concreta-

mente el archivo “cache\_encryptedA.db” En este fichero se almacena la información referente a las celdas GSM a las que se ha conectado el dispositivo no encontrándose ninguna situación sospechosa.



Por otro lado hay que indicar que este fichero se elimina y se vuelve a crear cada vez que se sincroniza el dispositivo por lo que aunque a priori no existe ningún indicio que lleve a pensar que el teléfono ha sido intervenido no se garantiza que no se haya comprometido anteriormente a la sincronización.

A continuación se muestra el fichero que indica la última vez que se sincronizó el mismo:

Description	
Selected: /media/sf_test/efb858b2673/Info.plist	bb6936a4efb858b2673/bcbd8155b99f912943bc1bb6936a4

ASCII content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Build Version</key>
  <string>9B206</string>
  <key>Device Name</key>
  <string></string>
  <key>Display Name</key>
  <string></string>
  <key>GUID</key>
  <string></string>
  <key>ICCID</key>
  <string></string>
  <key>IMEI</key>
  <string></string>
  <key>Last Backup Date</key>
  <date>2012-05-23 22:31:26</date>
  <key>Phone Number</key>
  <string></string>
  <key>Product Type</key>
  <string>iPhone4,1</string>
  <key>Product Version</key>
  <string>5.1.1</string>
  <key>Serial Number</key>
  <string></string>
```

Figura 13: Fuente: Elaboración Propia

A continuación se muestra una captura de pantalla de esa base de datos en la que no se ha encontrado información relevante acerca de la intervención del dispositivo. Lo que hay que buscar, para encontrar indicios de conexiones a estaciones falsas,

son patrones de conexión a una estación (movistar en este caso) con coordenadas muy similares. Así podríamos ver si el móvil se ha conectado a una estación falsa que suplanta una real de movistar y que estén en coordenadas similares:

Database Structure												Browse Data		Execute SQL	
Table: CellLocationHarvest												New Record		Delete Record	
	Operator	Transmit	BundleId	Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Speed	Course	Confidence			
1	Iovistar	1	com.apple.Maps	363172048.2	30720055	3.64839823523208	30.0	89355469	57.0	0.0	-1.0	90			
2	Iovistar	1	com.apple.Maps	363172109.0	26010355	3.64841664468951	10.0	02929688	19.0	0.0	-1.0	90			
3	Iovistar	1	com.apple.Maps	363172306.2	36935109	3.64832500729286	200.0	77734375	100.0	0.0	-1.0	72			
4	Iovistar	0	com.apple.Maps	363172366.9	77386183	3.64844454008307	10.0	04003906	3037742984	0.0	-1.0	90			
5	Iovistar	0	com.apple.Maps	363172416.	16629411	3.65052752898641	10.0	18828125	7703518337	8.22656325396873	223.968490615551	90			
6	Iovistar	0	com.apple.Maps	363172416.9	51717046	3.65060408626227	10.0	07617188	6121177112	7.97515929538568	225.539702126031	90			
7	Iovistar	0	com.apple.Maps	363172477.9	38546257	3.65315307751016	10.0	49609375	5977607238	2.97486536709781	215.348584012289	90			
8	Iovistar	0	com.apple.Maps	363172529.9	70863432	3.65714293617656	10.0	74121094	9002249998	7.46109348084313	231.953497029753	90			
9	Iovistar	1	com.apple.Maps	363172590.	45043058	3.6591448685908	30.0	24609375	5214427439	9.91464557722231	350.435790513312	90			
10	Iovistar	0	com.apple.Maps	363172605.9	56943456	3.65948102922933	30.0	09179688	9049949758	13.0031935119042	344.954395233468	90			
11	Iovistar	0	com.apple.Maps	363172625.9	23008844	3.66063703808179	30.0	20703125	5468714616	22.1985079177595	335.042183169163	90			
12	Iovistar	0	com.apple.Maps	363172638.9	79212377	3.6620351872425	10.0	98925781	3832721742	25.633604828303	344.35249932382	90			
13	Iovistar	0	com.apple.Maps	363172643.9	45275453	3.66241228117157	10.0	86425781	6073477617	25.1662514266426	348.988052323216	90			
14	Iovistar	0	com.apple.Maps	363172671.	44766771	3.66351273737349	10.0	10546875	5723566623	25.1964639695589	352.19416189369	90			
15	Iovistar	0	com.apple.Maps	363172694.	78917057	3.66500191089033	10.0	11035156	0340169516	21.4328543667764	340.116160548342	90			
16	Iovistar	0	com.apple.Maps	363172714.9	38232039	3.66713151989256	10.0	66210938	0256372337	23.840029384352	337.349605341074	90			
17	Iovistar	0	com.apple.Maps	363172743.9	30817509	3.67127722741125	10.0	77246094	3300094291	28.4452667418777	328.53782143473	90			
18	Iovistar	0	com.apple.Maps	363172769.9	77963754	3.67446734456851	10.0	08691406	5110806726	28.8464529256016	352.509103031602	90			
19	Iovistar	0	com.apple.Maps	363172791.9	76394777	3.67371965087494	10.0	95507813	1866450304	20.761198090899	9.7872507348103	90			
20	Iovistar	0	com.apple.Maps	363172808.1	75666067	3.67268096626476	10.0	71972656	0298124152	15.222079889619	350.156082827115	90			
21	Iovistar	0	com.apple.Maps	363172828.9	99494314	3.67628844543991	10.0	72265625	8787505515	18.7046593818039	234.145985642397	90			
22	Iovistar	0	com.apple.Maps	363172850.9	52997826	3.68134254233752	10.0	30566406	5022478099	20.8402134066766	252.130590548743	90			
23	Iovistar	0	com.apple.Maps	363172881.	79313589	3.69015800504001	10.0	92871094	8525928744	23.821170004347	296.898962907241	90			
24	Iovistar	0	com.apple.Maps	363172906.0	88940955	3.69562805927171	10.0	33496094	8765561613	19.7976149483404	307.118381992867	90			

Figura 14: Fuente: Elaboración Propia

## 5. TÉCNICAS DE INFECCIÓN DE TERMINALES



Lo siguiente es una recopilación de ejemplos de varias fuentes. Te recomendamos que para más información vayas al Blog de Chema Alonso llamado Un informático en el lado del mal (<http://www.elladodelmal.com/>) y en concreto el libro Hacking de dispositivos iOS: iPhone & iPad de Chema Alonso y otros (ver bibliografía).

### 5.1. TÉCNICAS DE INFECCIÓN

Una de las formas más frecuentes que se utilizan para infectar dispositivos móviles es camuflando virus bajo la apariencia de programas que simulan ser aplicaciones o juegos. El usuario, pensando que es una app confiable, la descarga e instala sin ser consciente de que acaba de “abrir las puertas” de su dispositivo a los ciber delincuentes. En Internet, podemos encontrar apps para nuestros móviles en muchos sitios web, sin embargo, lo más recomendable siempre es hacerlo desde las tiendas oficiales: Google Play, Apple Store, Windows phone, BlackBerry World, etc. Y aun así, debemos tener mucha precaución, ya que pese a los esfuerzos que hacen las compañías desarrolladoras de las distintas plataformas móviles para evitar que se publiquen apps “dudosas”, se ha demostrado que es posible “colar” alguna app maliciosa en estos markets.



Un truco muy utilizado para infectar ordenadores que se ha trasladado rápidamente a los móviles es el envío de ficheros maliciosos a través del correo electrónico, redes sociales o mensajería instantánea.



Utilizando trucos de ingeniería social, consiguen que abramos el fichero para verlo; sin embargo, si no descargamos una app que nos sugieren, no podremos ver el archivo. ¿Dónde está la trampa? El virus está escondido en el supuesto reproductor de vídeo, visor de imagen, etc. que acabamos de descargar e instalar para ver correctamente el fichero.

Otra vía de infección por virus en nuestro dispositivo podría ser la descarga de ficheros que no son aplicaciones como tales. Los documentos de texto, presentaciones, imágenes, vídeos, etc. aunque no contienen el virus de forma directa, pueden aprovecharse de fallos de seguridad de las aplicaciones instaladas que los manejan, y ser capaces de descargar un virus a nuestro dispositivo. Este tipo de infección es muy común en ordenadores y portátiles, y es probable, que comience a serlo en dispositivos móviles.

Algunas páginas web, en ocasiones legítimas, han sido manipuladas por “hackers” para que cuando las visitemos, si no tenemos el software y las aplicaciones correctamente actualizados, infecten nuestros dispositivos. En este caso, nuevamente la ingeniería social se usaría para guiarnos hasta esa página web maliciosa. Para este tipo de infección, se necesita que la página web manipulada identifique el sistema operativo y navegador que la está visitando y, a continuación, buscará fallos del sistema operativo, aplicaciones o del navegador, y si encuentra alguno, lo aprovechará para colarse en el dispositivo (descargar y ejecutar el virus).

Otras formas puede llegar un fichero a nuestro smartphone o tableta es a través de algún dispositivo extraíble que conectemos. Por ejemplo, la tarjeta de memoria (microSD). Cuando conectamos un móvil a un ordenador, la memoria del teléfono y la tarjeta microSD, si la tiene, se comportan como unidades extraíbles del propio ordenador, y si el ordenador está infectado con un virus, éste podría copiarse en estas memorias. El virus, si está programado para un sistema operativo Windows, no infectará el dispositivo móvil, pero actuará como “portador”. Esto quiere decir que si conectamos el móvil a otro equipo Windows, éste podría infectarse con el virus que las memorias del móvil almacenan.

## 5.2. INFECCIÓN EN IOS

La infección en terminales Android es mucho más sencilla, por la propia idiosincrasia del entorno, sin embargo esto no debería pasar en IOS. Cuando se realiza un jailbreak a un dispositivo iOS se rompe la seguridad de la firma del código, lo que impide garantizar que las aplicaciones que se descargan desde el Store alternativo vienen aprobadas por Apple, han pasado unos controles de seguridad y tienen controlados los permisos en el terminal, y que han pasado un proceso de test de seguridad antes de ser publicadas con el objetivo de proteger al usuario.





Aunque los tests de seguridad que pasan las aplicaciones en App Store pueden ser eludidos, y hay muchos casos en los que se han metido aplicaciones con comportamientos maliciosos (como Find & Call, aplicaciones de robo de datos como el caso de Storm8 o que directamente eludían las protecciones del sistema como la prueba de concepto de Charlie Miller con InstaStock) que demuestra que los controles no son perfectos.

Si el usuario ha realizado Jailbreak, existen varias formas de instalarle el malware al terminal. En el caso de un terminal con jailbreak, la confianza en la tienda de aplicaciones que se usa es fundamental. La tienda de aplicaciones más popular en el mundo del jailbreak es Cydia y se supone que las apps que allí se publican pasan un mínimo de controles. Sin embargo siempre es posible instalar el troyano desde algún repositorio usando Cydia y logrando que la víctima instale esa aplicación (por ejemplo camuflándolo como un juego).

Por tanto, en principio, un terminal iPhone o iPad con iOS cuenta con muchas protecciones contra apps no deseadas en la AppStore, y de que el sistema está limitado a usuarios no privilegiados por defecto, siguen existiendo posibilidades y formas de meter un malware dentro de un terminal iPhone o iPad para espiar a su dueño. Aún así han habido casos de software malicioso como Find & Call, los robos de datos de los juegos de Storm-8, o los comportamientos "maliciosos" de algunas apps como Twitter for iOS o Path.

Contando con acceso físico al terminal con Jailbreak, se puede, en caso de no tener cambiadas las contraseñas de los usuarios por defecto, un ataque de Juice Jacking usando la conexión OpenSSH o USBMux con solo conectar el terminal a un equipo desde el que se va a hacer el ataque.

Si no tiene Jailbreak pero tiene un chip A4, en caso de tener un passcode sencillo, se rompe este con Untethered Jailbreak usando iPhone DataProtection o Gecko y se reinicia el terminal para que pierda el Untethered Jailbreak para iniciar la sesión con el passcode e instalar un troyano basado en un fichero de despliegue temporal firmado por un Apple Developer ID. En caso de tener un passcode complejo, los iPhone 4 y los iPad 1 cuentan con un bug en el boot que permite que se pueda hacer Jailbreak en el arranque sin necesidad de conocer el passcode con lo que es posible instalar un programa empaquetado que se ejecuta en el terminal (para meter OpenSSH o un malware). El terminal quedaría con Jailbreak y el usuario podría darse cuenta, aunque los troyanos comerciales ocultan las pistas de ello.

Finalmente, si el terminal no tiene Jailbreak y es un iPhone 4S, iPhone 5/5S o iPhone 6, es posible instalar un troyano en el equipo si este va firmado digitalmente (siempre que dispongamos también del passcode o fichero de despliegue temporal firmado). Por ello, si se cuenta con un Apple Developer ID se puede firmar el código e instalarlo en el equipo aun no habiéndose hecho el Jailbreak.



Existen otros muchos trucos, basándose en fallos del proceso de arranque o firma de las diversas aplicaciones, por lo que enumerarlos todos resulta muy difícil. Lo importante es ser consciente de que no existe sistema invulnerable, por lo que el usuario debe ser cauteloso y proteger su equipo.

## 6. ESTRUCTURA DE CARPETAS PARA EL ANÁLISIS DE DISPOSITIVOS



Para saber más sobre este tema puedes acceder a <http://conexioninversa.blogspot.com.es/2009/09/analisis-forenses-dispositivos-android.html> y a los blogs de la comunidad DragonJar (<http://www.dragonjar.org>) de donde se extrajeron partes de este capítulo.

### 6.1. INTRODUCCIÓN

Examinar el contenido de un dispositivo no es complicado, solo debemos conocer la estructura del dispositivo y tener muy claro lo que estamos buscando. Lo primero es acceder al dispositivo e ir a su estructura de carpetas.



Hay que tener en cuenta que las aplicaciones instaladas en los dispositivos por norma general los desarrolladores NO cifran la información sensible, por tanto, con examinar dentro de la carpeta de la aplicación en los directorios clásicos (Documents, Library y tmp), pero también examinar el contenido de la aplicación podemos encontrar información que puede sernos útil.

El objeto de este capítulo es mostrar dónde se debe buscar información dentro de los dispositivos. Si se deseara hacer un análisis forense, no basta con sólo ir a los directorios indicados, sino que se debería seguir un procedimiento mucho más amplio que incluye la preservación de la integridad de la prueba, así como la forma de presentar los resultados para que sean válidos.

## 6.2. ANDROID

La lista de ficheros que proporciona un dispositivo Android es:

- **boot.img:** Contiene datos relativos al inicio del sistema operativo. Nada relevante para nuestra revisión.
- **cache.img:** Contiene los datos volátiles que estaban en memoria en el momento de volcarlos a disco. Importante su análisis.
- **data.img:** Contiene todos los datos relativos al móvil, agendas, tareas, llamadas. Muy importante
- **misc.img:** Contiene datos relativos a las aplicaciones instaladas. Importante también.
- **recovery.img:** Contiene los datos del proceso que utiliza recovery. Irrelevante
- **system.img:** Contiene los datos relativos a configuración del sistema. Importante.

Los ficheros que vamos a tratar como interesantes por su contenido son: data.img y cache.img, los cuales deben ser convertidos en un formato revisable.

En ellos se pueden obtener lo siguiente, buscando con "grep" expresiones regulares:

- **Parámetros de sitios visitados:** `strings data.img | grep -oE "((mailto:|(news|(ht|f)tp(s?))\:\/\/){1}\S+)"`  
Sitios donde se ha realizado inicios de sesión `strings data.img | grep -n10 "login">login.html`
- **Correos electrónicos:** `strings data.img | egrep "[a-z A-Z_\-\.]+@[a-zA-Z\-\.\.]+\.[a-zA-Z\-\.\.]+"`
- **Números de teléfono:** `strings data.img | grep -oE "\b[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]\b"`
- **Imágenes JPG:** `strings data.img | grep -oE "(.*\jpe?g|.*\JPE?G)"`  
**Paquetes de programas instalados:** `strings data.img | grep -oE "(.*\ptk?g|.*\PTK?G)"`
- **Ficheros MP3:** `strings data.img | grep -oE "(.*\ptk?g|.*\PTK?G)"`  
**Dominios visitados:** `strings data.img | grep -oE "^[a-zA-Z0-9\-\.\.](es|com|org|net|mil|edu|COM|ORG|NET|MIL|EDU)$"`
- **Tarjetas de crédito:** `strings data.img | grep -oE "^(4\d{3})(5[1-5]\d{2})(6011)-?\d{4}-?\d{4}-?\d{4}|3[4,7]\d{13}$"`
- **Comandos SQL:** `strings data.img | grep -oE "(NOT)?(\s*(\w+)\s*(=LIKE|IN)\s*\(((\^)*))'|([\^'])*|(-?\d*\.\d+))(\s*)*(AND|OR)?"`

Así, si abrimos directamente el fichero 'data.img' nos encontramos con información muy valiosa como la siguiente:

- Direcciones MAC.
- Estado de la configuración.
- Datos del operador.
- Parámetros del móvil.
- Red WIFI.
- Vídeos visualizados.

### 6.3. IOS

A continuación se indican las rutas y archivos de donde se puede extraer la información que guarda un dispositivo iOS sobre su estado:

- Applications: Es un enlace simbólico a /var/stash/Applications.pwn
- Library: Como en cualquier sistema Mac OS X, contiene los plugins, configuraciones, etc.
- System: Contiene las preferencias del sistema y del dispositivo.
- User: Es un enlace simbólico a /var/mobile.
- bin: Contiene los ejecutables del sistema.
- etc: Es un enlace simbólico a private/etc/
- private: Contiene los directories etc y var (aquí encontraremos los archivos fstab, passwd y muchos más)
- /sbin: Contiene los ejecutables del sistema.
- tmp: Es un enlace simbólico a private/var/tmp/
- usr: Contiene los datos de zona horaria y ejecutables del sistema.
- var: Es un enlace simbólico a private/var/

NOTA: Developer, boot, cores, dev, lib y mnt son carpetas del sistema que están vacías.

La siguiente es una lista de archivos de interés, de los cuales podemos extraer mucha información que nos ayudarán en nuestro análisis de dispositivos iOS:

- `/private/etc/master.passwd` y `/private/etc/passwd` utilizando john the ripper o cualquier otra herramienta para crackear passwords, podremos obtener las claves del sistema.
- En la carpeta `/private/var/Keychains/` encontraremos los archivos `TrustStore.sqlite3`, `keychain-2.db`, `ocspcache.sqlite3` donde encontraremos en texto plano algunas de las contraseñas guardadas por los usuarios en diferentes aplicaciones.
- `/private/var/logs/` y `/private/var/log/` en estas carpetas encontraremos una gran cantidad de logs del sistema iOS que nos pueden ayudar en la elaboración de nuestra línea de tiempo.
- `/var/wireless/Library/Logs` logs sobre las conexiones inalámbricas (*3G, Bluetooth, WiFi*) del dispositivo.
- `/private/var/preferences/SystemConfiguration` encontramos una gran cantidad de información sobre la configuración del equipo, rangos de ips, información sobre las redes inalámbricas a las que se ha conectado, nombre del teléfono y mucha más información.
- `/private/var/root/Library/Caches/locationd` encontraremos información que nos ayudaran a geo-referenciar el dispositivo y el famoso archivo `consolidare.db` del que ya hemos hablado en la comunidad.
- `/private/var/root/Library/Lockdown/` en esta carpeta encontraras los certificados públicos y privados del dispositivo.
- `/private/var/root/Library/Cookies/` aquí encontraremos las cookies que están almacenadas en el dispositivo, las cuales nos pueden arrojar información muy útil sobre los sitios visitados y permitirnos realizar un robo de sección para intentar entrar a los servicios que visitaron desde el dispositivo.
- `/private/var/run` aquí encontraremos los logs del system.
- `/private/var/tmp` encontraremos información temporalmente almacenada por las aplicaciones.

Algunos archivos que pueden interesarnos, podemos abrirlos con cualquier editor de texto, otros son bases de datos en SQLite (clientes son SQLitebrowser o SQLiteman) y otros son “listas de propiedades” con extensión .plist (visualizable con Plist Editor o plutil.pl)

Especialmente interesante es la carpeta `/private/var/mobile/Library` que contiene una gran cantidad de información sobre el dispositivo útil.

- `/private/var/mobile/Library/Logs`: esta carpeta de logs muestra los errores de las aplicaciones instaladas en el equipo.
- `/private/var/mobile/Library/AddressBook`: una de las más importantes, en ella encontraremos los archivos `AddressBookImages.sqlitedb` donde están almacenadas las imágenes asociadas a los contactos y `AddressBook.sqlitedb` que hacen referencia a la libreta de contactos.
- `/private/var/wireless/Library/CallHistory/`: en esta carpeta está el archivo `call_history.db` donde está el listado de las últimas 100 llamadas realizadas por el dispositivo.
- `/private/var/mobile/Library/Calendar`: aquí encontraremos el `Calendar.sqlitedb` que contiene toda la información sobre los calendarios del dispositivos, alarmas y fechas.
- `/private/var/mobile/Library/Maps`: encontraremos los archivos `History.plist` y `Directions.plist` con la información que está almacenada en la aplicación mapas del dispositivo iOS.
- `/private/var/mobile/Library/Mail`: con información sobre los correos recibidos desde el dispositivo, las cuentas de correo, los tiempos de actualización, archivos adjuntos y mensajes de correo electrónico.
- `/private/var/mobile/Library/Preferences`: con archivos de configuración para el sistema iOS y aplicaciones instaladas, de ellos podemos sacar mucha información útil (últimas búsquedas en el programa de mapas, alarmas puestas en el reloj, números de llamada rápida, últimos vídeos buscados en youtube, últimas búsquedas en safari, zona horaria del dispositivo, ...)
- `private/var/mobile/Library/Safari`: encontramos los favoritos del safari `Bookmarks.db`, el historial `History.plist` y los buscadores usados `SearchEngines.plist` además del archivo `SuspendState.plist` que almacena las "pestañas" o paginas suspendidas de Safari.
- `/private/var/mobile/Library/Spotlight`: aquí encontraremos un listado con las aplicaciones abiertas por medio del buscador `spotlight db.sqlitedb` y los mensajes que están indexados por este buscador `SMSSearchdb.sqlitedb`.
- `/private/var/mobile/Library/SpringBoard`: aquí encontraremos las aplicaciones instaladas `applicationstate.plist` la organización de estas aplicaciones dentro del equipo `IconState.plist` y una miniatura del fondo utilizado `LockBackgroundThumbnail.jpg`

- `/private/var/mobile/Library/Voicemail`: aquí están los correos de voz que se encuentren en el dispositivo.
- `/private/var/mobile/Library/Notes`: la información ingresada en la aplicación notas de iOS.
- `/private/var/mobile/Library/Keyboard`: en esta carpeta encontraremos el archivo, `(idioma)-dynamic-text.dat` que almacena todas las palabras que son escritas desde el dispositivo para generar un diccionario con las palabras más usadas (¡¡es un keylogger!!).
- `/private/var/mobile/Media/DCIM/100APPLE` y `/private/var/mobile/Media/PhotoData`: con las fotos tomadas con el dispositivo iOS, además de las bases de datos de donde se obtiene información de las mismas (por defecto las fotos tomadas con un dispositivo iOS incluye la posición GPS del lugar donde fue tomada en sus meta-datos).
- `/private/var/mobile/Media/Recordings`: con las notas de voz y una base de datos `Recordings.db` con la fecha de creación, duración, y ruta, además de las etiquetas personalizadas de la nota `CustomLabels.plist`
- `/private/var/mobile/Library/Logs/ADDDataStore.sqlitedb` es una base de datos con información de cuando se utiliza una aplicación y cuánto tiempo se estuvo utilizando.



## 7. HERRAMIENTAS PARA ANÁLISIS DE TERMINALES

---

### 7.1. INFORMACIÓN PROPORCIONADA

El uso de herramientas para realizar los análisis de los terminales resulta muy útil, por la simplicidad que da al proceso. Herramientas como la Suite Oxygen Forensic 2011 (que permite una versión de prueba de 30 días) es un ejemplo de estas.

Las herramientas vienen con soporte para cientos de dispositivos móviles, entre los cuales se encuentran los de Apple, Android, Windows,.. y entre la información que podemos extraer con ellas se encuentra:

- Información básica del dispositivo y de la SIM.
- La lista de contactos con toda su información y foto si la tiene.
- Archivos Multimedia (fotos, vídeos, audios, etc.)
- Mensajes SMS.
- Log de eventos.
- Información del calendario.
- Notas almacenadas en el dispositivo.
- Navegador de archivos capturados.
- Genera una línea de tiempo.
- Extrae archivos de las aplicaciones instaladas.
- Historial, favoritos y cache del navegador web.

- Listado de diccionarios personalizados.
- Correos electrónicos con sus adjuntos.
- Llamadas realizadas, recibidas y perdidas.
- Trafico de en las redes GPRS, EDGE, CSD, HSCSD y Wi-Fi.
- Información de la SIM card (si aplica).
- Notas de voz y buzón de voz.
- Geo-posicionamiento del dispositivo.
- Saca una firma con hash MD5, SHA-1, SHA-2, a los archivos.
- Genera reportes del dispositivo.
- Conversaciones y registro de llamadas por Skype.
- Contactos y correos de los contactos en Facebook.

## 7.2. HERRAMIENTAS

Existen varias herramientas que ayudan en la tarea de realizar un análisis forense en dispositivos móviles. Sin intención de ser exhaustivos, se pueden nombrar las siguientes:

### 7.2.1. IPHONE

- iPhoneBrowser - Accede al sistema de ficheros del iPhone desde entorno gráfico.
- iPhone Analyzer - Explora la estructura de archivos interna del iPhone.
- iPhoneBackupExtractor - Extrae ficheros de una copia de seguridad realizada anteriormente.
- iPhone Backup Browser - Extrae ficheros de una copia de seguridad realizada anteriormente.
- iPhone-Dataprotection - Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad.
- iPBA2 - Accede al sistema de ficheros del iPhone desde entorno gráfico.
- sPyphone - Explora la estructura de archivos interna.

### 7.2.2. **BLACKBERRY**

- Blackberry Desktop Manager - Software de gestión de datos y backups.
- Phoneminer - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
- Blackberry Backup Extractor - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
- MagicBerry - Puede leer, convertir y extraer la base de datos IPD.

### 7.2.3. **ANDROID**

- android-locdump. - Permite obtener la geolocalización.
- androguard - Permite obtener, modificar y desensamblar formatos DEX/ODEX/APK/AXML/ARSC.
- viaforensics - Framework de utilidades para el análisis forense.
- Osaf - Framework de utilidades para el análisis forense.

## 8. POSICIONAMIENTO Y LOCALIZACIÓN DE PERSONAS MEDIANTE TECNOLOGÍA GSM

---

### 8.1. INTRODUCCIÓN



El posicionamiento de una persona, sin su consentimiento o con él, siempre parte de los datos que proporciona la red y del uso de ciertas funcionalidades de esta.

El terminal móvil de un usuario necesita para su buen funcionamiento cierta información de la red celular que le permita entre otras cosas hacer su acto de presencia, login, etc... Parte de esta información está relacionada con la localización geográfica del terminal, y dicha información, pese a ser una pequeña parte de toda la información que el terminal tiene, es la que detallamos a continuación, puesto que puede sernos útil para nuestros propósitos:

- **MCC (Mobile Country Code):** Es un dato que hace referencia al país en el que se encuentra el usuario en el instante de la medición (o para ser más exactos, el país en el que se ubica la estación base a la que el usuario está asociado en ese instante). El identificador MCC es un número de 3 dígitos decimales y es único para cada país en el mundo.
- **MNC (Mobile Network Code):** Identificador del operador de red. Es único para cada operador dentro de su país, lo que quiere decir que mismos identificadores pueden repetirse fuera del territorio nacional. Por cada operador, se asigna dicho identificador, el cual está compuesto por dos dígitos decimales. Asimismo, un operador puede tener asignados varios MNCs.

- **LAC (Location Area Code):** Código identificador de área. A aquellas regiones con cobertura GSM se les asigna un código LAC único dentro de cada país. Dicho código está representado por 4 dígitos decimales y hace referencia a una región más o menos extensa de territorio. Los 4 dígitos decimales tienen un significado, determinando la comunidad autónoma, la región y la localidad.
- **Cell ID Identificador de célula.** Es un número de entre 1 y 5 dígitos decimales que identifica de forma unívoca a una célula dentro de un territorio nacional. Cada dígito tiene un significado propio de los operadores, pero dicha información para la red móvil española no está bien documentada o bien no es de libre acceso.
- **Células vecinas:** El teléfono móvil almacena por orden las 7 células más (teóricamente) cercanas al terminal. Dicho criterio de cercanía se basa en la potencia de la señal recibida por cada BS.

Con esta información, que puede ser accedida se puede posicionar un equipo de forma bastante aproximada. Veamos a continuación algunas técnicas utilizadas para localizar la posición de un usuario sin su consentimiento usando funcionalidades de la red.

## 8.2. PROBLEMÁTICA



Investigadores de la Universidad de Minnessota, (Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim) han publicado un estudio titulado "Location Leaks on the GSM Air interface" que confirma que cualquier atacante, con unos medios técnicos de muy bajo coste, puede saltarse fácilmente la protección del anonimato frente a terceras partes que proporciona GSM.

Para salvaguardar la identidad de los usuarios frente a terceras personas que pudieran interceptar las comunicaciones móviles en el aire, el estándar GSM establece que la red del operador asigne periódicamente identificadores temporales a los usuarios, estos operadores reciben el nombre de (TMSI), de modo que sean esos identificadores temporales los que se transmitan por el aire, al menos en la mayoría de los casos, en lugar de los identificadores permanentes y unívocos de los usuarios (IMSI). Esta medida de seguridad permite que, un atacante escuchando las comunicaciones de radio podría ver que hay ciertos dispositivos móviles comunicándose en una determinada zona, pero no podría identificar a quién, o a qué número de teléfono, corresponde cada una de las comunicaciones salvo que llegara a descifrar la comunicación e identificara la voz del hablante.

Descifrar la comunicación una vez interceptada, también es posible, debido a que el algoritmo que utiliza *GSM* para realizar el cifrado, conocido como *A5/1*, es muy débil y ya ha sido roto.

Un atacante puede estar interesado simplemente en saber si una determinada persona está o no presente en una determinada zona, por ejemplo para entrar a robar en su casa cuando la persona no esté presente, o para confirmar su participación o no en una manifestación.

La técnica utilizada para determinar la presencia o no de una determinada persona en una determinada área consiste en realizar llamadas al número de teléfono móvil de la persona cuya presencia se quiere corroborar, y comprobar al mismo tiempo los mensajes enviados por la red a los móviles de la zona avisándoles de que hay una llamada entrante para ellos. Si repetimos el proceso varias veces se puede observar a qué identificador temporal (*TMSI*) van dirigidas las notificaciones que se producen instantes después cada vez que se inician las llamadas destinadas a la víctima.

Se puede pensar que esta técnica es fácilmente detectable por la víctima, ya que las llamadas entrantes “perdidas” quedarían reflejadas en su pantalla. Si los intentos de llamada se cortaran después de transcurrido demasiado tiempo, el teléfono víctima registraría el intento de llamada y mostraría en su pantalla el conocido mensaje de llamada entrante perdida. De otro modo, si se cortaran los intentos de llamada demasiado pronto, el aviso por parte de la red al teléfono llamado no llegaría a observarse en la red. Pero existe una franja intermedia de tiempo, en la cual, si los intentos de llamada se cortan dentro de ese intervalo, la red llega a enviar el aviso de llamada entrante por el aire, y en cambio el móvil de la víctima no llega a registrar el intento de llamada como llamada perdida, siendo por tanto totalmente transparente para la víctima.



Utilizando esta técnica, se ha demostrado que, utilizando simplemente un PC, un teléfono móvil antiguo, y software gratuito de dominio público, un atacante puede determinar si el propietario de un determinado número de teléfono está o no presente en la zona en la que se encuentre el atacante, con una precisión que puede variar entre unos 100 metros a la redonda (o varios bloques de edificios, en entorno urbano), y varios kilómetros, dependiendo del entorno y de la distribución y organización de las estaciones base del operador en la zona.

Llevando a cabo esta técnica, el atacante puede determinar el identificador temporal (*TMSI*) asignado por la red a ese usuario víctima en ese momento, cosa que podría ser utilizada para realizar otros ataques, como capturar selectivamente sus

comunicaciones, obtener la clave de sesión, y con ello descifrar sus comunicaciones o incluso suplantar la identidad del teléfono víctima.

Ésta no es la única técnica disponible para determinar el *TMSI* de un usuario. En diciembre de 2010 unos investigadores alemanes demostraron una técnica similar, basada en el envío de mensajes *SMS* especiales o mal formados al teléfono de la víctima, pero la técnica recién descrita tiene la ventaja de que utiliza solamente mecanismos totalmente estándar de *GSM*, como son la solicitud de establecimiento de llamada y el aborto de la misma.



En definitiva, una prueba más de lo inseguras que son las comunicaciones GSM.

## 9. CASO PRÁCTICO DE INTERCEPTACIÓN DE COMUNICACIONES DE APLICACIONES DE SMARTPHONES

---

### 9.1. ESTUDIO DE CASO PRÁCTICO: WHATSAPP

En este apartado, se verá cómo la aplicación WhatsApp en versiones más antiguas a la actual no enviaba los mensajes cifrados y un ejemplo práctico de las últimas versiones de whatsapp que ya cifra los mensajes enviados.

La última moda en aplicaciones móviles se llama [WhatsApp](#), una App que cada vez se hace más popular y está redefiniendo el sistema de mensajería SMS. ¿Que qué nos ofrece? Un servicio mucho más completo, mejor y de momento gratuito.

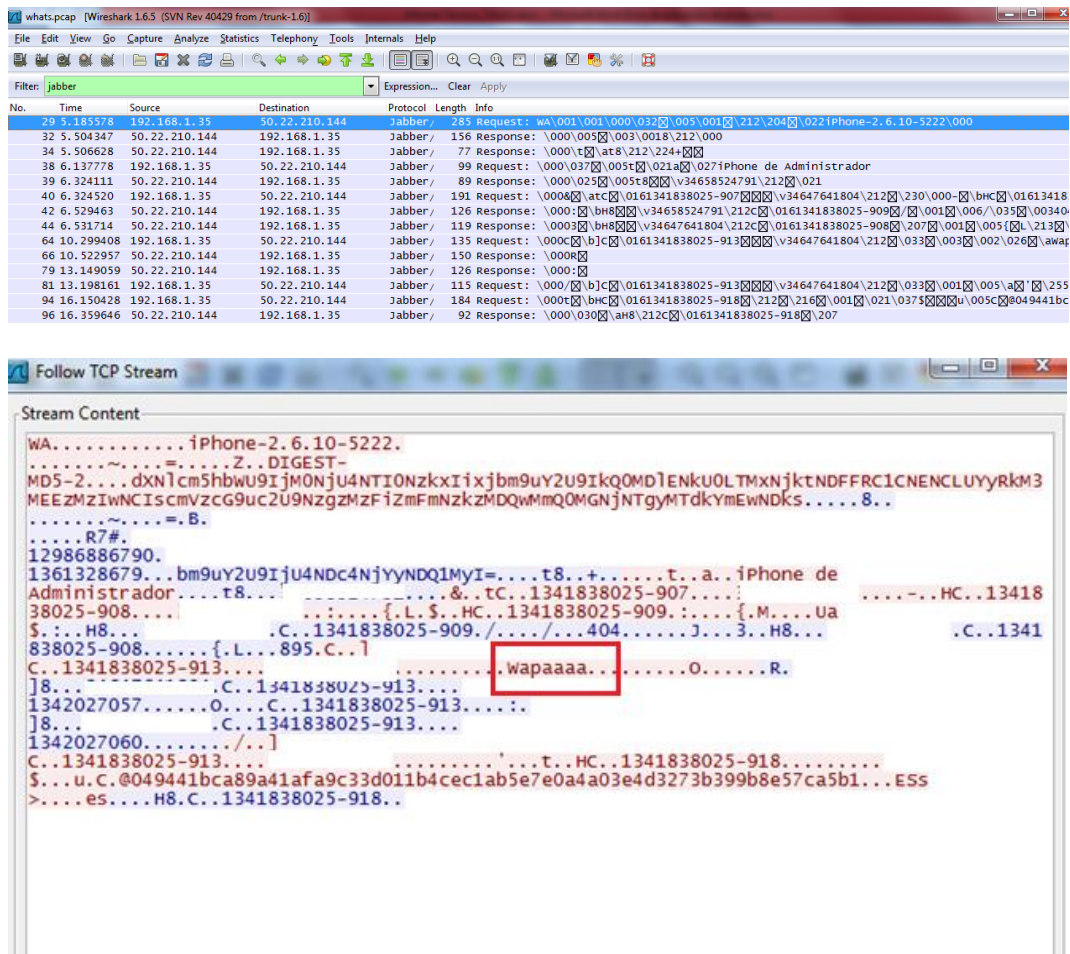


La "pega" es que necesitamos conexión a Internet para poder comunicarnos, y que tanto emisores como receptores deben tener la aplicación instalada.

En el tráfico de la red generado por la aplicación lo primero que llama la atención es que el destino del servidor es el puerto 443 (HTTPS) , aunque el puerto https sea utilizado para realizar conexiones seguras mediante SSL/TLS , en este caso whatsapp envía por este puerto todos los mensajes en texto claro, sin ningún tipo de cifrado.



## Ejemplo de captura de mensaje de whatsapp sin cifrar:



Figuras 15 (Superior) y 16 (Inferior): Fuente: Elaboración Propia

Realizando un ataque man-in-the-middle al teléfono, es posible interceptar todos los mensajes en texto claro y enviarlos a internet para que el usuario no note ningún problema.



La "pega" es que necesitamos conexión a Internet para poder comunicarnos, y que tanto emisores como receptores deben tener la aplicación instalada.

```

1. rpcap://\\Device\\NPF_{2F7C4701-09E2-4D34-A877-E63196C9F182}
<Network adapter 'Realtek RTL8192S Wireless LAN USB NIC
  (Microsoft's Packet Scheduler)' on local host>
2. rpcap://\\Device\\NPF_{7F59B3DA-7F0A-4273-80BE-A046063E0623}
<Network adapter 'NVIDIA nForce MCP Networking Adapter Driver (Microsoft's Packe
t Scheduler)' on local host>

Enter your interface number please->1
Numero:03461111111111111111
Message:oB
Numero:00161011111111111111
Message:eCeaJordyPrueba realizada con exito
Numero:00161011111111111111
Message:oB
Numero:00161011111111111111
Message:eCeaJordyPrueba realizada con exito
Numero:00161011111111111111
WhatsUserid:00161011111111111111

```

Figura 17: Fuente: Elaboración Propia.

Las nuevas versiones de Whatsapp utilizan ya un cifrado propio en las comunicaciones; a continuación se presenta un ejemplo de análisis de una de las últimas versiones de la aplicación, donde se pueden observar estas características y otras relativas a la seguridad:

Las pruebas se han realizado sobre la versión de la aplicación WhatsApp del 27 de Agosto del 2012. El tipo de dispositivo sobre el que se han realizado los test es un IPHONE 4 identificado con la dirección IP: 192.168.130.190

Los análisis realizados a la aplicación inciden en dos niveles:

- Nivel de seguridad en el cifrado del transporte de mensajes.
- Nivel de seguridad en los datos almacenados por la aplicación en el dispositivo.

Éste último análisis nos posibilitará realizar la valoración de las implicaciones e impacto producido tras el acceso a un dispositivo con la aplicación instalada, por parte de un elemento no autorizado, a nivel físico como una persona o a nivel lógico como un proceso malware que hubiese infectado el sistema.



Se ha realizado un análisis del cifrado utilizado dado que la aplicación no usa un cifrado estándar, sino que se trata de un cifrado propietario del desarrollador de la aplicación.

Para la realización de las pruebas de esta sección se ha procedido a realizar una interceptación de tráfico mediante técnicas de envenenamiento ARP sobre el dispositivo, capturándose el tráfico emitido por la aplicación mediante un Sniffer.

## 9.2. CAPTURA DE DATOS EN EL PROCESO DE COMUNICACIÓN

Tras realizar la inyección de las tablas ARP del dispositivo iPhone con dirección IP: 192.168.130.190 se ha capturado el tráfico con un Sniffer como puede verse en la siguiente captura:

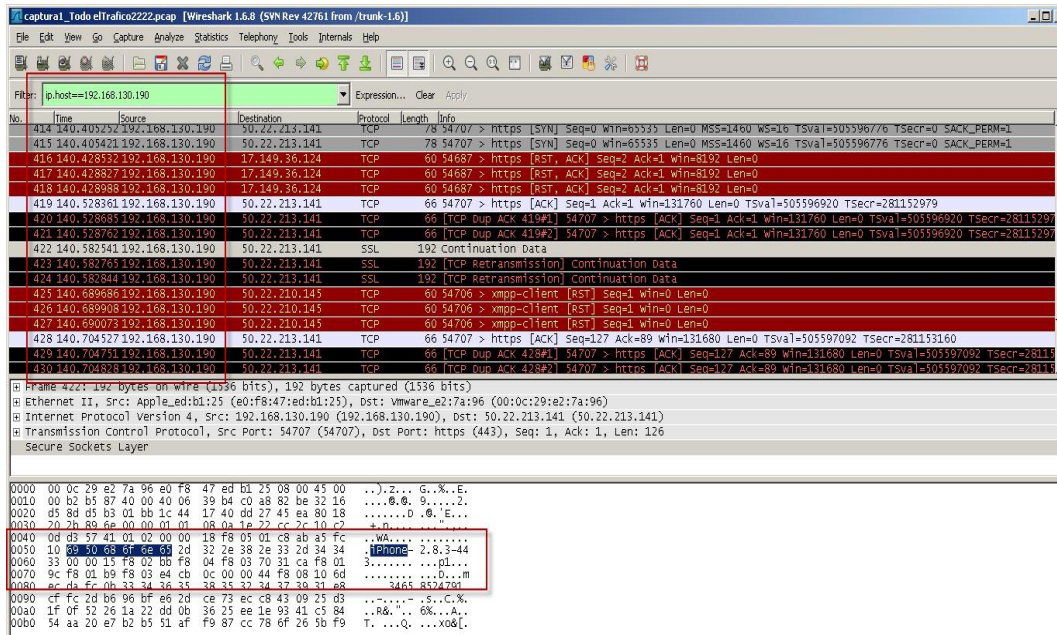


Figura 18: Fuente: Elaboración Propia

Como puede apreciarse en la siguiente captura, podemos ver que se ha usado el puerto 443 para la transmisión de los datos, motivo por el cual el Sniffer indica que se trata de cifrado SSL pero este dato no es correcto ya que se usa un cifrado propio.



Puede observarse la comunicación para la transferencia de mensajes con el servidor de la aplicación ubicado en diferentes direcciones IP ubicadas en EEUU.

438	140.838556	192.168.130.190	50.22.213.141	SSL	104 [TCP Retransmission]	Continuation Data
439	140.838556	192.168.130.190	50.22.213.141	SSL	104 [TCP Retransmission]	Continuation Data
440	141.038796	192.168.130.190	50.22.213.141	SSL	203	Continuation Data
441	141.039044	192.168.130.190	50.22.213.141	SSL	203 [TCP Retransmission]	Continuation Data
442	141.039125	192.168.130.190	50.22.213.141	SSL	203 [TCP Retransmission]	Continuation Data
449	150.838569	192.168.130.190	50.22.213.141	SSL	188	Continuation Data
450	150.838960	192.168.130.190	50.22.213.141	SSL	188 [TCP Retransmission]	Continuation Data
451	150.839061	192.168.130.190	50.22.213.141	SSL	188 [TCP Retransmission]	Continuation Data
452	151.459679	192.168.130.190	50.22.213.141	SSL	256 [TCP Retransmission]	Continuation Data
453	151.460272	192.168.130.190	50.22.213.141	SSL	256 [TCP Retransmission]	Continuation Data
454	151.460361	192.168.130.190	50.22.213.141	SSL	256 [TCP Retransmission]	Continuation Data
455	151.667064	192.168.130.190	82.223.191.248	TLSv1	103 [TCP Retransmission]	Encrypted Alert
456	151.667260	192.168.130.190	82.223.191.248	TLSv1	103 [TCP Retransmission]	Encrypted Alert
457	151.667334	192.168.130.190	82.223.191.248	TLSv1	103 [TCP Retransmission]	Encrypted Alert
458	152.185022	192.168.130.190	50.22.213.141	SSL	378 [TCP Retransmission]	Continuation Data
459	152.185300	192.168.130.190	50.22.213.141	SSL	378 [TCP Retransmission]	Continuation Data
460	152.185385	192.168.130.190	50.22.213.141	SSL	378 [TCP Retransmission]	Continuation Data

Frame 451: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)									
Ethernet II, Src: Vmware_e2:7a:96 (00:0c:29:e2:7a:96), Dst: Fortinet_09:0b:07 (00:09:0f:09:0b:07)									
Internet Protocol Version 4, Src: 192.168.130.190 (192.168.130.190), Dst: 50.22.213.141 (50.22.213.141)									
Transmission Control Protocol, Src Port: 54707 (54707), Dst Port: https (443), Seq: 302, Ack: 276, Len: 122									
Secure Sockets Layer									

0000	00 09 0f 09 0b 07 00 0c	29 e2 7a 96 08 00 45 00	.....).Z...E.
0010	00 ae eb c1 40 00 40 06	03 7e c0 a8 82 ba 32 16	....@.~....2.
0020	d5 8d d5 b3 01 bb 1c 44	18 6d dd 27 46 fd 80 18	.....D.m."F...
0030	20 1a b4 c5 00 00 01 01	08 0a 1e 22 f4 12 10 c2	....."z.>."<
0040	10 4f 80 00 77 2d 99 c8	94 ea 7a 13 3e 04 22 3c	.O.W-...>....B
0050	b7 2a 30 e9 0e 0a d8 dc	d2 3e dc da a7 83 d3 42	.*O.....>....B
0060	85 18 d5 65 cc 1c 51 9b	a0 0b 55 0f 3a d0 03 ef	...e..Q...U....
0070	fa 78 df b6 10 3e 23 b7	aa 21 ea a0 ab 03 21 02	.x...>#. !.....!
0080	db f7 2c fe 0a b6 7c 4e	e8 66 c3 85 ba 2d 04 8f	..... N.f...-.
0090	d5 8c 77 63 b3 50 57 b8	68 b4 96 d3 cc 28 4a 00	..wc.Pw. h....(J.
00a0	1c 43 0e 30 ba 89 46 a6	e6 0d d6 04 52 e6 2f 58	.C.O..F. ....R./X
00b0	49 03 7f 6b 81 b4 cb 98	26 c6 cf f2	I..k.... &...

Figura 19: Fuente: Elaboración Propia

## 9.3. ANÁLISIS DE DATOS CAPTURADOS

Para analizar los datos capturados se han utilizado dos aplicaciones que muestran información de dispersión, frecuencia y entropía del cifrado de los datos transmitidos.

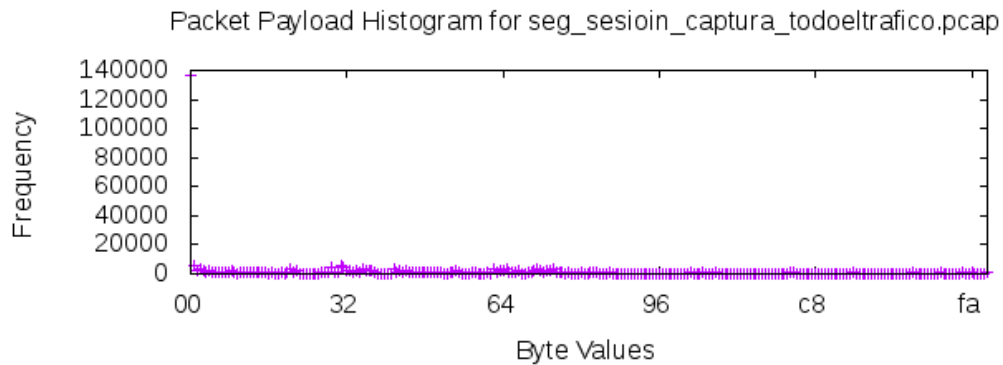


Un principio común en los sistemas cifrados es que los datos cifrados deben ser no distinguibles de los datos aleatorios. Cuando evaluamos la salida de los datos de un sistema de cifrado no deberíamos poder detectar patrones predecibles.

Aplicando este concepto, podemos visualizar los datos de una captura de paquetes para producir un histograma gráfico de la frecuencia de cada valor de byte en cada carga útil del paquete. Si los datos están cifrados, el histograma debe revelar una distribución uniforme de los valores de byte.

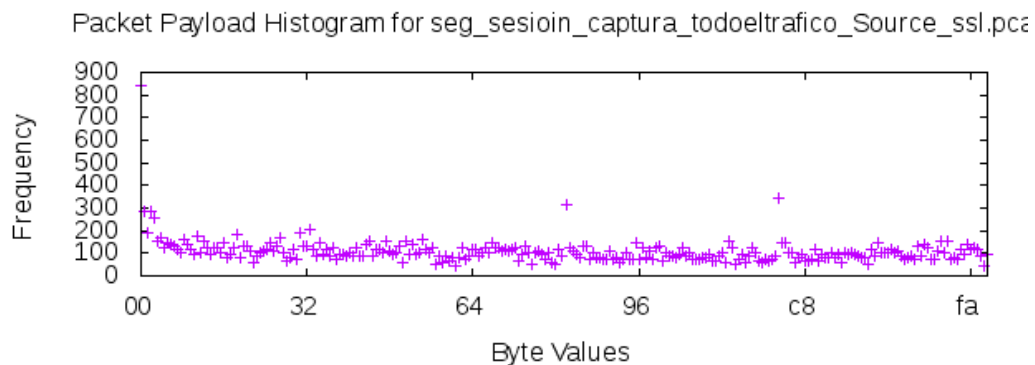
Se ha utilizado una aplicación para generar dichos histogramas gráficos con el siguiente resultado.

En el gráfico que puede verse a continuación se analiza una muestra del global de tráfico transmitido por el dispositivo; puede observarse una frecuencia mínima de repetición de datos, así como una aparición mínima de representación de datos comunes de valores en bytes representados desde los valores hexadecimales 30 hasta 7<sup>a</sup>.



**Figura 20:** Fuente: Elaboración Propia

En el siguiente gráfico veremos la representación de los datos capturados utilizando el filtrado de los datos capturados, para indicar al gráfico que realice el análisis sobre los datos emitidos por el dispositivo en protocolo cifrado. Puede observarse un incremento en la frecuencia de aparición de valores, así como la aparición de picos mínimos de valores de bytes legibles.



**Figura 21:** Fuente: Elaboración Propia

El segundo valor de referencia que se ha tomado para determinar la robustez del cifrado utilizado por la aplicación ha sido la entropía.



Para tener una visión clara de cómo afectan los valores obtenidos de este parámetro a la robustez del cifrado, definamos la entropía tomando como referencia la wikipedia “se puede considerar como la cantidad de información promedio que contienen los símbolos usados. Los símbolos con menor probabilidad son los que aportan mayor información; por ejemplo, si se considera como sistema de símbolos a las palabras en un texto, palabras frecuentes como "que", "el", "a" aportan poca información. Mientras que palabras menos frecuentes como "corren", "niño", "perro" aportan más información. Si de un texto dado borramos un "que", seguramente no afectará a la comprensión y se sobrentenderá, no siendo así si borramos la palabra "niño" del mismo texto original. Cuando todos los símbolos son igualmente probables (distribución de probabilidad plana), todos aportan información relevante y la entropía es máxima.”

Los valores de entropía recomendados en sistemas de cifrado con este volumen de bytes de clave pueden enmarcarse en los rangos:

- **Muy Alto:** 7.4x a 7.99.
- **Alto:** 7.00 a 7.399.
- **Muy Bajo:** 5.2x.

Para el análisis de este parámetro sobre los datos capturados se han utilizado herramientas para la separación de los datos y su posterior estudio entrópico. Los resultados obtenidos son los siguientes:

En la siguiente captura de imagen se muestra el proceso de división de los datos capturados en tramas separadas según protocolo de comunicación utilizado, utilizando como valor de discriminación el puerto de comunicación.



```

root@bt:~/Desktop/WhatsApp# tcpick -r seg_sesioin_captura_todoeltrafico_Source.pcap -wR
Starting tcpick 0.2.1 at 2012-09-04 03:37 EDT
Timeout for connections is 600
tcpick: reading from seg_sesioin_captura_todoeltrafico_Source.pcap
1 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
2 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
3 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
4 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
5 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
6 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
7 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
8 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
9 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
10 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
11 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
12 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
13 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
14 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
15 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
16 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
17 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
18 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
19 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
20 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
21 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
22 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
23 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
24 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
25 SYN-SENT 192.168.130.146:54837 > 17.149.36.78:5223
26 SYN-SENT 192.168.130.146:54837 > 17.149.36.78:5223

```

Figura 22: Fuente: Elaboración Propia

Los archivos de datos generados por protocolos podemos verlos en la siguiente captura (recordando que los indicados como https son los que procederemos a estudiar dado que si bien no es ssl, el puerto utilizado por WhatsApp 2.8.3 es el 443, el mismo que dicho protocolo, por lo que las herramientas indican https:

```

root@bt:~/Desktop/WhatsApp# ls *.dat
tcpick_192.168.130.146_17.149.36.185_5223.serv.1.dat  tcpick_192.168.130.146_74.125.230.241_www.serv.dat
tcpick_192.168.130.146_17.149.36.185_5223.serv.dat  tcpick_192.168.130.146_74.125.230.242_www.serv.dat
tcpick_192.168.130.146_17.149.36.207_https.serv.dat  tcpick_192.168.130.146_74.125.230.243_www.serv.dat
tcpick_192.168.130.146_173.194.67.193_https.serv.dat  tcpick_192.168.130.146_74.125.230.244_www.serv.dat

```

Figura 23: Fuente: Elaboración Propia

En la siguiente captura se procede al estudio de entropía de los datos de comunicación de la aplicación WhatsApp 2.8.3:

```

root@bt:~/Desktop/WhatsApp# ent tcpick_192.168.130.146_17.149.36.207_https.serv.dat
Entropy = 7.487728 bits per byte.

Optimum compression would reduce the size
of this 1761 byte file by 6 percent.

Chi square distribution for 1761 samples is 2024.34, and randomly
would exceed this value 0.01 percent of the times.

Arithmetic mean value of data bytes is 95.0857 (127.5 = random).
Monte Carlo value for Pi is 3.344709898 (error 6.47 percent).
Serial correlation coefficient is 0.259066 (totally uncorrelated = 0.0).

```

Figura 24: Fuente: Elaboración Propia

Se ha repetido el proceso con más capturas de paquetes utilizando tramas que se centran en el proceso de comunicación de la aplicación de forma más concreta:

```
root@bt:~/Desktop/WhatsApp# tcpick -r seg_sesioin_captura_todoeltrafico_Source.pcap -wR
Starting tcpick 0.2.1 at 2012-09-04 03:43 EDT
Timeout for connections is 600
tcpick: reading from seg sesioin captura todoeltrafico Source.pcap
1 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
2 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
3 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
4 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
5 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
6 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
7 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
8 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
9 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
10 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
11 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
12 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
13 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
14 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
15 SYN-SENT 192.168.130.146:54835 > 17.149.36.190:5223
16 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
17 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
18 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
19 SYN-SENT 192.168.130.146:54836 > 17.149.36.208:5223
20 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
21 SYN-SENT 192.168.130.146:54831 > 17.149.36.185:5223
22 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
23 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
24 SYN-SENT 192.168.130.146:54832 > 17.149.36.90:5223
25 SYN-SENT 192.168.130.146:54837 > 17.149.36.78:5223
26 SYN-SENT 192.168.130.146:54837 > 17.149.36.78:5223
27 SYN-SENT 192.168.130.146:54837 > 17.149.36.78:5223
28 SYN-SENT 192.168.130.146:54834 > 173.194.67.193:https
29 SYN-SENT 192.168.130.146:54833 > 17.149.36.101:5223
```

```
root@bt:~/Desktop/WhatsApp# ls *.dat
tcpick_192.168.130.146_17.149.36.185_5223.serv.1.dat  tcpick_192.168.130.146_74.125.230.241_www.serv.dat
tcpick_192.168.130.146_17.149.36.185_5223.serv.dat  tcpick_192.168.130.146_74.125.230.242_www.serv.dat
tcpick_192.168.130.146_17.149.36.207_https.serv.dat  tcpick_192.168.130.146_74.125.230.243_www.serv.dat
tcpick_192.168.130.146_173.194.67.193_https.serv.dat  tcpick_192.168.130.146_74.125.230.244_www.serv.dat
```

```
root@bt:~/Desktop/WhatsApp# ent tcpick_192.168.130.146_17.149.36.207_https.serv.dat
Entropy = 7.487728 bits per byte.

Optimum compression would reduce the size
of this 1761 byte file by 6 percent.

Chi square distribution for 1761 samples is 2024.34, and randomly
would exceed this value 0.01 percent of the times.

Arithmetic mean value of data bytes is 95.0857 (127.5 = random).
Monte Carlo value for Pi is 3.344709898 (error 6.47 percent).
Serial correlation coefficient is 0.259066 (totally uncorrelated = 0.0).
```

Figuras 25 (Superior) 26 (Media) y 27 (Inferior): Fuente: Elaboración Propia



```

root@bt:~/Desktop/WhatsApp# ent tcpick_192.168.130.146_173.194.67.193_https.serv.dat
Entropy = 5.161006 bits per byte.

Optimum compression would reduce the size
of this 179 byte file by 35 percent.

Chi square distribution for 179 samples is 3117.54, and randomly
would exceed this value 0.01 percent of the times.

Arithmetic mean value of data bytes is 63.7877 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is -0.001623 (totally uncorrelated = 0.0).

```

Figura 28: Fuente: Elaboración Propia

Como podemos observar, los valores de entropía ofrecidos tras el estudio son:

7.487728 en dos de las tramas analizadas lo cual supone un valor alto y un valor bajo de 5.161006 en otra de las tramas.

Esta diferencia de valores en los resultados entrópicos se puede asociar con las diferentes tramas de datos transmitidas durante el proceso de comunicación. Dichos procesos no suelen ser en ningún caso homogéneos por lo que este tipo de valores obtenidos son claramente explicables.

## 9.4. ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS DATOS ALMACENADOS



El bloque de análisis que se procede a mostrar, se incluye como muestra de los resultados tras un acceso por una persona ajena al control del dispositivo o bien por el acceso a los datos del dispositivo a través de malware instalado en el mismo.

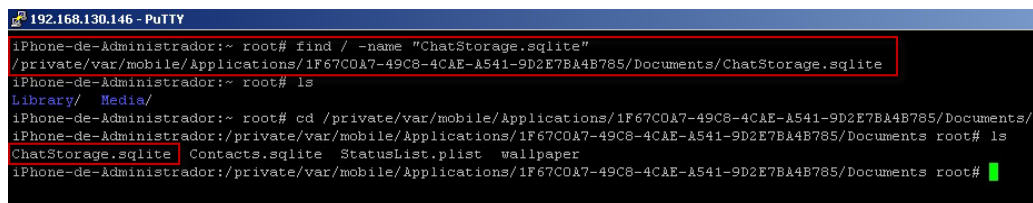
### Captura de Almacén de datos de la aplicación:



Para el siguiente proceso se ha realizado una conexión vía ssh con el dispositivo del mismo modo que la podría realizar un atacante en el caso de tener acceso al mismo por ejemplo tras una sustracción del dispositivo.

En primer lugar se procedería al Jail Break del dispositivo (existen multitud de técnicas y software actualmente para la realización de Jail Break de dispositivos móviles). Tras obtener control del teléfono con el proceso anterior se procede con la extracción de los datos:

En la siguiente captura realizamos la búsqueda del archivo ChatStorage.sqlite que contiene la base de datos almacenada de mensajería de la aplicación Whatsapp:

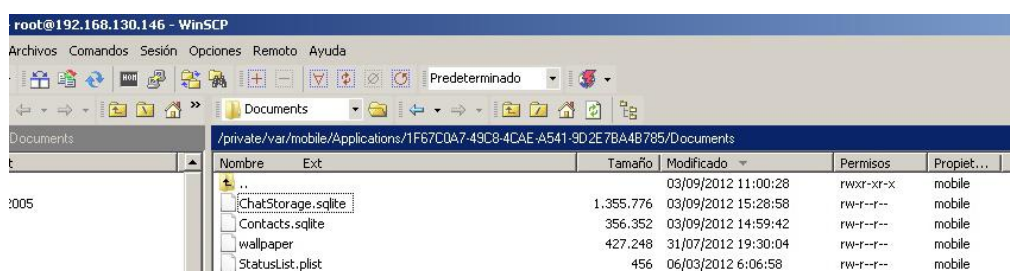


```

192.168.130.146 - PuTTY
iPhone-de-Administrador:~ root# find / -name "ChatStorage.sqlite"
/private/var/mobile/Applications/1F67C0A7-49C8-4CAE-A541-9D2E7BA4B785/Documents/ChatStorage.sqlite
iPhone-de-Administrador:~ root# ls
Library/ Media/
iPhone-de-Administrador:~ root# cd /private/var/mobile/Applications/1F67C0A7-49C8-4CAE-A541-9D2E7BA4B785/Documents/
iPhone-de-Administrador:/private/var/mobile/Applications/1F67C0A7-49C8-4CAE-A541-9D2E7BA4B785/Documents root# ls
ChatStorage.sqlite  Contacts.sqlite  StatusList.plist  wallpaper
iPhone-de-Administrador:/private/var/mobile/Applications/1F67C0A7-49C8-4CAE-A541-9D2E7BA4B785/Documents root#
  
```

Figura 29: Fuente: Elaboración Propia

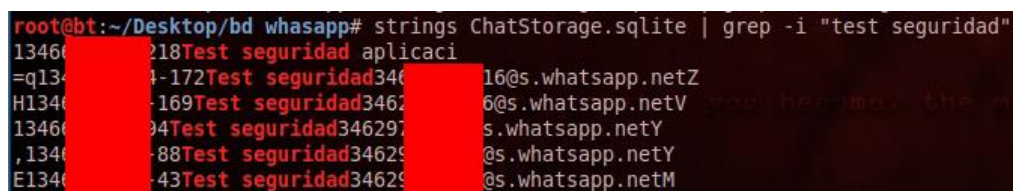
Procedemos a realizar una copia a nuestro sistema en local del archivo de datos como puede verse en la siguiente captura:



Nombre	Ext	Tamaño	Modificado	Permisos	Propiet...
..			03/09/2012 11:00:28	rwxt-xr-x	mobile
ChatStorage.sqlite		1.355.776	03/09/2012 15:28:58	rw-r--r--	mobile
Contacts.sqlite		356.352	03/09/2012 14:59:42	rw-r--r--	mobile
wallpaper		427.248	31/07/2012 19:30:04	rw-r--r--	mobile
StatusList.plist		456	06/03/2012 6:06:58	rw-r--r--	mobile

Figura 30: Fuente: Elaboración Propia

Finalmente, una vez que tenemos copiado el archivo de base de datos en nuestro sistema, procedemos a leerlo en busca de mensajes que se han enviado durante el proceso de pruebas con el texto "Test de Seguridad"



```

root@bt:~/Desktop/bd whatsapp# strings ChatStorage.sqlite | grep -i "test seguridad"
1346...218Test seguridad aplicaci
=q13...4-172Test seguridad346...16@s.whatsapp.netZ
H1346...169Test seguridad3462...6@s.whatsapp.netV
1346...94Test seguridad34629...s.whatsapp.netY
,1346...88Test seguridad34629...@s.whatsapp.netY
E1346...43Test seguridad34629...@s.whatsapp.netM
  
```

Figura 31: Fuente: Elaboración Propia

Como podemos observar en la captura anterior, puede verse el texto de mensaje y los números de teléfono (que se han ocultado por motivos de seguridad).



En el caso de producirse un borrado de datos del historial completo de la conversación en el terminal, se ha verificado que el borrado de conversaciones en la base de datos no es total, borrándose únicamente los datos del historial de la sesión activa, y permaneciendo en la base de datos del dispositivo y siendo por lo tanto accesibles los datos de conversaciones anteriores con el mismo contacto.

## 9.5. CONCLUSIONES GENERALES SOBRE EL CIFRADO DE LOS MENSAJES

Las conclusiones que se pueden extraer tras el análisis realizado al proceso de cifrado de los mensajes enviados por la aplicación WhatsApp 2.8.3, manifiestan que en general se cuenta con un cifrado seguro. Al no tratarse de un estándar de cifrado con una robustez demostrada, es imposible asegurar que dicho cifrado no será roto en el futuro. Actualmente existen diversos investigadores realizando trabajos al respecto, que en un plazo de tiempo indeterminado podrían o no tener éxito en sus investigaciones.

## 9.6. CONCLUSIONES GENERALES SOBRE EL ALMACENAMIENTO DE DATOS EN DISPOSITIVO

Las conclusiones que se pueden extraer tras el análisis realizado al proceso de almacenamiento que realiza la aplicación WhatsApp 2.8.3, manifiestan que son altamente inseguros, pudiéndose acceder a la totalidad de mensajes almacenados por la aplicación en el caso de tener acceso directo al dispositivo por una sustracción, pérdida o infección de éste. Como se ha verificado también, en el caso del borrado en el terminal de una conversación con un contacto, el borrado sólo se produce de la conversación activa, manteniéndose los datos en el dispositivo de conversaciones anteriores.

## 9.7. CONCLUSIONES GENERALES SOBRE EL USO DE LA APLICACIÓN WHATSAPP 2.8.3 PARA ENTORNO LABORAL

Tras el estudio realizado, y los análisis realizados de los resultados obtenidos, se puede deducir que el uso de dicha aplicación para entornos laborales debe quedar restringida a la comunicación de estratos del organigrama que el desempeño de su labor diaria no implique el manejo de información altamente sensible. Para perfiles del organigrama cuyo manejo de información sea sensible, su uso no es recomendable dado que si bien el transporte de mensajes hasta el momento es seguro, la pérdida, robo o infección del dispositivo podría desembocar en un grave fallo de seguridad por la posibilidad de obtención de mensajes almacenados en el dispositivo.



## CONCLUSIONES

---

A lo largo del tema hemos podido comprobar que el malware en terminales móviles es actualmente el mayor problema de seguridad en esta tecnología.

El sistema utilizado en Android, de distribución de las APP mediante el market de Google Play tiene algo muy bueno para los desarrolladores, y es que te permite subir las APP sin pasar por ningún filtro. Esto es bueno porque no es necesario esperar un mínimo de dos semanas que tarda Apple en aprobar el software o denegarlo. Esto ha permitido que sea en el entorno Android donde el malware ha sufrido su mayor expansión frente a otros entornos, al poder subir el malware sin ningún tipo de barrera.

Según el informe de Tren Micro de 3Q 2012 se indica que el malware, cuyo fin es recabar los datos personales de los usuarios de Android, se han disparado un 483%, de 30.000 en junio de 2012 a casi 175.000 en septiembre de 2012. En el ámbito de Apple, como se hace previamente una comprobación de las APP antes de que estén disponibles en App Store se ha logrado minimizar este tipo de problemas. Sin embargo, la plataforma abierta de Google se ha convertido en el epicentro de una virulenta actividad maliciosa.

Las versiones falsas de aplicaciones legítimas de Android son el tipo de 'malware' más común. Muchas de estas aplicaciones se han concebido para desviar datos o controlar el smartphone del usuario, con el consiguiente riesgo de recibir facturas muy elevadas por el envío de SMS a números de tarificación especial.

## RECAPITULACIÓN

---

Hemos visto a lo largo de este tema que las comunicaciones móviles han experimentado un alto crecimiento en los últimos años, y actualmente los terminales tienen una potencia de procesamiento muy elevada, lo que ha permitido la aparición de malware que permite a extraños tomar el control de nuestros equipos y poder ejecutar acciones sin nuestro consentimiento.

Además hemos visto que uno de los aspectos que debe tener en cuenta a la hora de elegir un dispositivo móvil es el tema de la seguridad. Además hemos visto que Android es una de las plataformas donde se puede instalar este tipo de malware, y hemos visto cómo se puede analizar este tipo de malware.

El principal problema está en la instalación de aplicaciones de fuentes no confiables, es decir, directamente de las páginas de los creadores de los programas, en lugar de hacerlo a través de Google Play u otras plataformas autorizadas.

## AUTOCOMPROBACIÓN

1. **Los primeros sistemas de telefonía móvil civil empiezan a desarrollarse...**
  - a) A partir de finales de los años 40 en los Estados Unidos.
  - b) A partir de los 90 en Europa.
  - c) En Japón con el sistema NTSC.
  - d) A partir de los años 80, en EEUU.
  
2. **La implementación del Acceso múltiple por división de tiempo (TDMA) y Acceso múltiple por división de código (CDMA) sobre las redes Amps, trajo como ventaja para estas empresas:**
  - a) Aumentar la cobertura por antena.
  - b) Poder ocupar frecuencias diferentes a las utilizadas.
  - c) Poder lograr una migración de señal analógica a señal digital sin tener que cambiar los terminales de los usuarios.
  - d) Poder lograr una migración de señal analógica a señal digital sin tener que cambiar elementos como antenas, torres, cableado, etc.
  
3. **El ataque de Man-In-The-Middle de GSM se basa en:**
  - a) La introducción de malware en el terminal que desvía las comunicaciones.
  - b) La configuración por defecto de los terminales hace que estos se conecten a la estación base (BTS) cuya señal resulta más potente, de este modo, se monta una BTS falsa, se emite hacia la víctima con mucha potencia y se espera a que su terminal se conecte.
  - c) La introducción de equipos en la red móvil que hace que todo el tráfico se desvíe al atacante.

d) Ninguna de las demás respuestas.

**4. La comunicación en GSM se establece en dos direcciones:**

- a) Utilizando el mismo canal de comunicación radio mediante TFM.
- b) Del terminal a la BTS (Uplink) y de la BTS al terminal (Downlink). La voz del usuario viaja por Downlink y la voz de la persona con la que habla viaja por Uplink.
- c) Del terminal a la BTS (Uplink) y de la BTS al terminal (Downlink). La voz del usuario viaja por Uplink y la voz de la persona con la que habla viaja por Downlink.
- d) Ninguna de las demás respuestas.

**5. Con el fin de descubrir si el dispositivo se encuentra intervenido con una estación falsa podemos analizar los "logs" del mismo, concretamente el archivo "cache\_encryptedA.db" En este fichero:**

- a) Se almacena la información referente a las celdas GSM a las que se ha conectado el dispositivo.
- b) Se almacena la información de usuarios que han validado en cada celda GSM.
- c) Contiene los datos de navegación del usuario.
- d) Contiene posiciones del GPS del Smartphone.

**6. Según los investigadores de la Universidad de Minnessota han publicado un estudio titulado "Location Leaks on the GSM Air interface" que confirma que:**

- a) Cualquier atacante, con unos medios técnicos de muy bajo coste, puede saltarse fácilmente la protección del anonimato frente a terceras partes que proporciona GSM.
- b) Ningún atacante puede saltarse fácilmente la protección del anonimato frente a terceras partes que proporciona GSM.
- c) Unos pocos atacantes, con unos medios técnicos específicos y formación específica, puede saltarse la protección del anonimato frente a terceras partes que proporciona GSM.
- d) GSM no proporciona protección del anonimato frente a terceras partes.

**7. El algoritmo que utiliza GSM para realizar el cifrado, es el...**

- a) AES.
- b) Bellman-Fort.
- c) A5/1.



d) DES.

**8. WhatsApp es una App que:**

- a) Utiliza mensajes SMS para transmitir información.
- b) Envía todos los mensajes en texto claro, sin ningún tipo de cifrado.
- c) Envía todos los mensajes con cifrado.
- d) Ninguna de las demás respuestas.

**9. Whatsappsniiffer es una aplicación que:**

- a) Obtiene los datos de la agenda del usuario infectado.
- b) Es una herramienta que permite identificar posibles atacantes en la red.
- c) Rompe los cifrados existentes en las comunicaciones.
- d) Permite realizar un ataque man-in-the-middle al teléfono, interceptando todos los mensajes en texto claro y enviarlos a internet para que el usuario no note ningún problema.

**10. Un principio común en los sistemas cifrados es que:**

- a) No pueden ser utilizados en tráficos con gran ancho de banda.
- b) Los datos cifrados deben ser no distinguibles de los datos aleatorios.
- c) Se detectan patrones asociados al algoritmo utilizado.
- d) Ninguna de las demás respuestas.



## SOLUCIONARIO

---

1.	a	2.	d	3.	b	4.	c	5.	a
6.	a	7.	c	8.	b	9.	d	10.	b

## PROPUESTAS DE AMPLIACIÓN

---

Busca en Internet análisis existentes sobre malware en terminales móviles y trata de ver cuáles son las actuales tendencias de contramedidas que se están proponiendo para evitar el malware en terminales Android.

Por otro lado, trata de ver qué estrategias de ataque se están utilizando en la distribución del malware Android, para lograr que las víctimas se instalen este tipo de malware. En Android 4.2, se ha implementado una nueva ventana a la hora de instalar una aplicación que muestra los permisos que van a ser utilizados por la aplicación, y una función de escanear las aplicaciones de terceros que se instalen.



## BIBLIOGRAFÍA

---

- Instituto Nacional de Tecnologías de la Comunicación (INTECO), (2012). “Malware y dispositivos móviles Ed. INTECO. Cuaderno de notas del OBSERVATORIO”. Recuperado de [www.inteco.es/Seguridad/Observatorio/Articulos/malwer\\_moviles](http://www.inteco.es/Seguridad/Observatorio/Articulos/malwer_moviles)
- Root-Secure. (2012). “Seguridad en Dispositivos Móviles”. Recuperado de <http://www.root-secure.com/arch/Seguridad%20en%20Dispositivos%20Moviles%20Smartphone%20y%20Pocket%20PC.pdf>
- BBVA INNOVATION CENTER. (2012). “Seguridad y privacidad en dispositivos móviles”. Recuperado de <https://www.centrodeinnovacionbbva.com/contents/4880-seguridad-y-privacidad-en-dispositivos-moviles>
- Alonso, JM. (2011). “Un Informático en el lado del mal”. Recuperado de <http://www.elladodelmal.com>
- McAfee, Inc. (2013). McAfee Delivers on Mobile Security Vision to Protect Devices, Data and Apps for Consumers and Organizations. Ed McAfee Inc. Recuperado de <http://www.mcafee.com/es/products/virusscan-mobile.aspx>
- Varios autores. (2012). IBM X-Force Research and Development. Ed IBM Recuperado de <http://www-03.ibm.com/security/xforce/>
- Baker, W. Hutton, A y otros (2012) 2011 Data Breach Investigations Report. Ed. Verizon. Recuperado de [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf)
- Chema Alonso, Alejandro Ramos, Pablo González, David Barroso, et al. “Hacking de dispositivos iOS: iPhone & iPad”, Ed 0xWORD, ISBN: 978-84-616-4217-5
- Proyecto colaborativo del regulador español Wikitel <http://wikitel.info>
- Blog de <http://conexioninversa.blogspot.com.es/2009/09/analisis-forenses-dispositivos-android.html>



- Blogs de la comunidad DragonJar <http://www.dragonjar.org>
- Blog Lázaro Escudero <http://www.tierradelazaro.com/cripto/gsm.htm> y <http://www.tierradelazaro.com/cripto/3g.htm>