UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Análisis Forense Para Dispositivos Móviles

Trabajo Monográfico

para obtener el grado de

Ingeniero en Redes

PRESENTA

Carlos Suriel Cohuo Aguayo

Supervisores de Monografía

MTI.Vladimir Veniamin Cabañas Victoria

MSI.Laura Yésica Dávalos Castilla

Ing.Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Octubre de 2011.

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo monográfico elaborado bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo Monográfico

Supervisor

MTI. Vladimir Veniamin Cabañas Victoria

Supervisor:

MSI. Laura Yésica Dávalos Castilla

Supervisor:

Ing. Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Octubre de 2011.

Agradecimientos

A MIS ASESORES:

Al M.T.I. Vladimir Veniamin Cabañas Victoria, por ser como un amigo durante el desarrollo de este trabajo y la carrera, siempre transmitió confianza además de ser un excelente maestro.

A la M.S.I. Laura Yésica Dávalos Castilla, por ser una amiga dentro del salón de clases además de ser una excelente maestra y por ser parte de este proyecto.

Al Ing. Rubén González Elixavide, por ser un ejemplo de profesionalismo que nunca olvidaré además de su buen humor, siempre transmitió una gran confianza y muchos conocimientos al ser un excelente maestro.

A MIS AMIGOS:

A todos mis amigos Juan Guillermo, Nazario Martínez, Miguel Ángel, muchas gracias por estar conmigo por ser como hermanos, gracias por ser mis amigos y recuerden que siempre los tendré presente, nunca los olvidare.

Y un agradecimiento muy especial a la Lic. Addy Lorena Peña, por preocuparse por el ladito más desvalido de mí y apoyarme cuando lo necesité, por ser un humano espectacular. Por valorar los mejores rasgos de mi persona y llenarme de afecto de un modo tan dulce y frecuente, junto a ella aprendí el valor de contar con algo cuando no se sabe aún como pedirlo y apoyar a los demás estando "ahí" para ellos.

A la Universidad de Quintana Roo y a la División de Ciencias e Ingeniería ya que el presente trabajo fue financiado en la Convocatoria 2010 “Apoyo a la titulación” de la División de Ciencias e Ingeniería.

Dedicatoria

A mis padres, Gracias papá y mamá por darme una carrera para mi futuro y por creer en mí, se los agradezco de todo corazón me toca corresponderles, aquí tienen mi esfuerzo tarde pero seguro este triunfo es de los dos, gracias por apoyarme.

A mis hermanos Josué Javier y Joezer Alain porque siempre estuvieron ahí brindándome su aliento.

Resumen.

Los teléfonos celulares son los dispositivos que hoy en día nos mantienen en constante comunicación con familiares, amigos, compañeros de trabajo, socios y empleados, en ellos se utilizan diversos servicios como el almacenamiento de datos, mensajes instantáneos, mensajes multimedia, llamadas de voz entre otras cosas.

Estos dispositivos móviles son además repositorios de información que en muchos casos pueden llegar a ser utilizados para fines diferentes para los que fueron creados. Cada día es más común utilizar estos dispositivos en actos delictivos como lo son: transacciones financieras ilícitas, espionaje industrial, pornografía infantil, acoso, secuestros, narcotráfico y un largo etcétera.

Es en ese contexto donde cobra una gran relevancia el análisis forense para dispositivos móviles, la cual se define como la ciencia que permite la recuperación, preservación, y examinación de la evidencia digital de teléfonos celulares utilizando una metodología estándar.(1)

Identificar la importancia de contar con una metodología adecuada y herramientas y técnicas pertinentes para la recuperación de la evidencia digital y en un caso legal sirva y aporte pruebas relevantes para la impartición de justicia en nuestro país, es la principal razón de este trabajo de investigación; el cual aborda los temas fundamentales y los principios del análisis forense a través de la aplicación de una metodología que permita obtener evidencia digital (borrada o no) de un dispositivo móvil a través de la tarjeta SIM, la cual le permite la comunicación con otros dispositivos móviles.

Contenido

Índice de figuras y Tablas

Introducción

Los teléfonos celulares son los dispositivos móviles más utilizados actualmente en todo el mundo. Al igual que las computadoras estos dispositivos han dejado de ser un lujo, pues se han convertido en una necesidad; representan el producto de mayor demanda de tecnología móvil con más de 80 millones de líneas de celulares sólo en México(2) los cuales son utilizados tanto para fines personales como para la actividad profesional.

El clima de inseguridad, violencia y delincuencia organizada que se vive en México, ha generado que el uso de estos dispositivos se vea involucrado en actos delictivos y por esa razón surgen analistas que estudian las ciencias forenses y aplican las herramientas y técnicas que permitan la recuperación de la información almacenada en un dispositivo móvil. (Como parte de evidencia digital, o para identificar relaciones de complicidad en las redes del crimen organizado).

Existen compañías como CSI -*Computer Security Institute* que es el Instituto de Seguridad Informática en los Estados Unidos, TX, San Francisco que se dedica a la investigación para salvaguardar la información, aplicando diversos métodos forenses con el fin de recabar la información necesaria, el uso de estos dispositivos ha llevado a diferentes gobiernos y empresas a tomar medidas extremas, como la de México y Perú que decretaron una ley para el registro de los celulares y sus usuarios, para mantener una normatividad en seguridad con los medios de comunicación.

El tema de análisis forense da la iniciativa a los especialistas informáticos para integrar soluciones en seguridad informática que involucra a organizaciones dedicadas a la búsqueda de evidencias digitales que coadyuvan a revelar

delitos cibernéticos ya que cada vez es mayor el número de víctimas involucradas en este tipo de delitos.

Objetivo general

Documentar una metodología para la adquisición de la información en los medios móviles utilizando las herramientas adecuadas para el estudio de un dispositivo de telefonía celular que pertenece al sistema GSM.

Objetivos particulares

- Definir los fundamentos generales del análisis forense a equipos de telefonía celular, y los procedimientos al respecto al tratamiento de la evidencia digital.

- Identificar la arquitectura de un teléfono celular para administrar los componentes de almacenamiento de la información en dispositivos de telefonía celular.

- Aplicar una metodología estándar utilizando herramientas diseñadas para realizar un análisis forense en los dispositivos de telefonía celular.

Justificación

La informática forense es un campo que poco a poco ha ido apareciendo; sin embargo, tiene aún muchas áreas por investigar y profundizar por tanto, esta investigación establece un conjunto de elementos conceptuales sobre los dispositivos móviles, lo que se busca con esta investigación es recopilar y analizar la información con el objetivo de proponer una guía con los métodos y herramientas que se conocen hoy en día y en un futuro ser útil como modelo para realizar un análisis forense orientado a incidentes sobre teléfonos móviles GSM y de esta manera, dar a conocer el campo de la informática forense en dispositivos móviles.

Metodología

La informática forense sobre equipos móviles utiliza una amplia gama de técnicas y herramientas para la recaudación de la información digital almacenada en estos dispositivos, en esta investigación se empleará un análisis y un modelo de evaluación entre las diversas metodologías que existen para la recuperación de la información llamada evidencia digital almacenada en estos dispositivos. La metodología estándar tendrá como finalidad los siguientes puntos.

- **Determinar:** la problemática real.
- **Identificar**: todo tipo de registro guardado en un celular para usarla como evidencia digital.
- **Establecer:** un proceso para el estudio de los dispositivos móviles.
- **Dar seguimiento y control:** Al estudio realizado dar presentación de los hallazgos, y custodia de la evidencia digital en el proceso judicial correspondiente.

Marco teórico

El Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los estados unidos (*NIST*, por sus siglas en inglés) define la informática forense sobre dispositivos móviles como la ciencia que se encarga de recuperar y recolectar evidencia digital de un teléfono móvil bajo una serie de condiciones forenses usando los métodos aceptados en la actualidad (3).Se conocen algunas de las herramientas y procedimientos así como los estándares para llevarse a cabo los conceptos de análisis forense que pudiera ayudar en un proceso legal.

Historia de la tecnología móvil.

El teléfono móvil se remonta a los inicios de la segunda guerra mundial, dónde ya se veía que era necesaria la comunicación a distancia, es por eso que la compañía Motorola creó un equipo llamado *HandieTalkie* H12-16, que era un equipo que permitía el contacto con las tropas por medio de vías onda de radio que en ese tiempo no superaba más de 600 KHz (4)

La telefonía móvil usa ondas de radio para poder ejecutar todas y cada una de las operaciones ya sea llamar, mandar mensajes de texto, mensajes multimedia, entre otras, esto es producto de lo que sucedió hace algunas décadas.

En los años 80, la industria de teléfonos móviles en Europa comenzó a presentar un crecimiento importante, lo cual trajo como consecuencia la aparición de diferentes estándares en esta industria por parte de diferentes

fabricantes. Estos sucesos, como se ha visto en la historia con otras tecnologías de alta relevancia, plantearon la necesidad de crear una unificación de tecnologías, para así generar un estándar sobre la cual se pudiera trabajar de manera conjunta y beneficiosa.

Así fue como inició en 1982 el desarrollo del estándar GSM, en el cual participaron varios países europeos, quienes serían los primeros beneficiados con la creación de esta especificación, algunos años después, dado el éxito el estándar fue incluido en la ETSI (*European Telecommunication Standards Institute*, por sus siglas en inglés) el cual prácticamente esparció el sistema en toda Europa, impulsando el desarrollo del estándar y la posterior finalización de la primera especificación.

La tecnología GSM, entre otras cosas, permitió tener un sistema de interconexión de redes locales e internacionales, manteniendo una identidad única en cualquiera de las locaciones en donde se encontrara un usuario gracias al sistema *roaming*. Otras de las características importantes fue que el sistema era totalmente digital, a diferencia de los otros sistemas de telefonía móvil de la época, lo cual permitía manejar eficientemente tanto datos como voz sobre la misma red aunque existen mejores tecnologías desarrolladas desde ese entonces, hoy en día GSM es el sistema más utilizado alrededor del mundo. (5)

La palabra forense proviene del latín *forensis* (sitio donde los tribunales juzgan las causas) e implica un ejercicio y aplicación de procedimientos utilizando ciencias relacionadas que estudian y resuelven casos ligados normalmente a situaciones legales. Entonces el término forense se refiere a cualquier aspecto de una determinada ciencia relacionada con el derecho, o aquello relativo a los tribunales y administración de justicia. (6)

La informática forense

La Informática Forense es la ciencia se encarga de: adquirir, preservar, obtener y presentar los datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos.

La evidencia digital.

Es la Información almacenada digitalmente, que puede llegar a ser utilizada como prueba en un proceso Judicial.

Para que esto sea viable es necesario seguir unos procedimientos en su recuperación, almacenamiento, y análisis, es muy importante seguir una serie de cuidados lo suficientemente estrictos, en la actualidad ya hay expertos en derecho de las TI y expertos técnicos en metodología forense esto con el fin de asegurar la conservación de la evidencia y garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Descripción de un teléfono celular

Las funciones que realiza un celular ha dado como respuesta una buena aceptación ante la sociedad ya que estos artefactos hoy en día realizan diversas funciones independientemente del modelo o del fabricante, prácticamente todos los celulares soportan los servicios de voz y mensajes de texto, así como conjunto de aplicaciones básicas (7) como son la siguientes:

- Realizar y recibir llamadas. Conversaciones de voz mediante un celular.

- Administrar información personal, incluyendo notas, lista de tareas, organización de información personal, uso de calendario, alarmas directorio telefónico, y administrador de tareas.
- Buzón de voz, el usuario puede dejar un mensaje si el equipo al que se está llamando no estuvo disponible.
- Correo electrónico (e-mail).enviar y recibir correos.
- Revisar contenido móvil (obtener noticias, clima, deportes, y otros datos).
- Reproducir música, a través de un reproductor mp3 o bien mediante del sintonizador de radio.
- Tomar fotos o videos, utilizando una cámara integrada, luego, enviar los archivos a otros dispositivos.
- Descargar fotos o imágenes, apoyados por visores de imágenes o reproductores de video.
- Diversas aplicaciones. Capacidad para instalar programas tales como procesadores de texto o video juegos.

Arquitectura de los dispositivos móviles.

Los teléfonos móviles son dispositivos de comunicación portátil que efectúan un conjunto de funciones de capacidades limitadas. Estos dispositivos son diseñados para facilitar la movilidad de los usuarios, por ello se diseñan de tamaño compacto, con baterías de alta eficiencia y de peso ligero.

Los celulares cuentan con un conjunto básico de componentes como: microprocesador, memoria de sólo lectura (ROM), memoria de acceso aleatorio (RAM), un módulo de radio, un procesador de señal digital, un micrófono y alta voz, una variedad de piezas hardware e interfaces, y una pantalla de cristal liquida (LCD). (1)

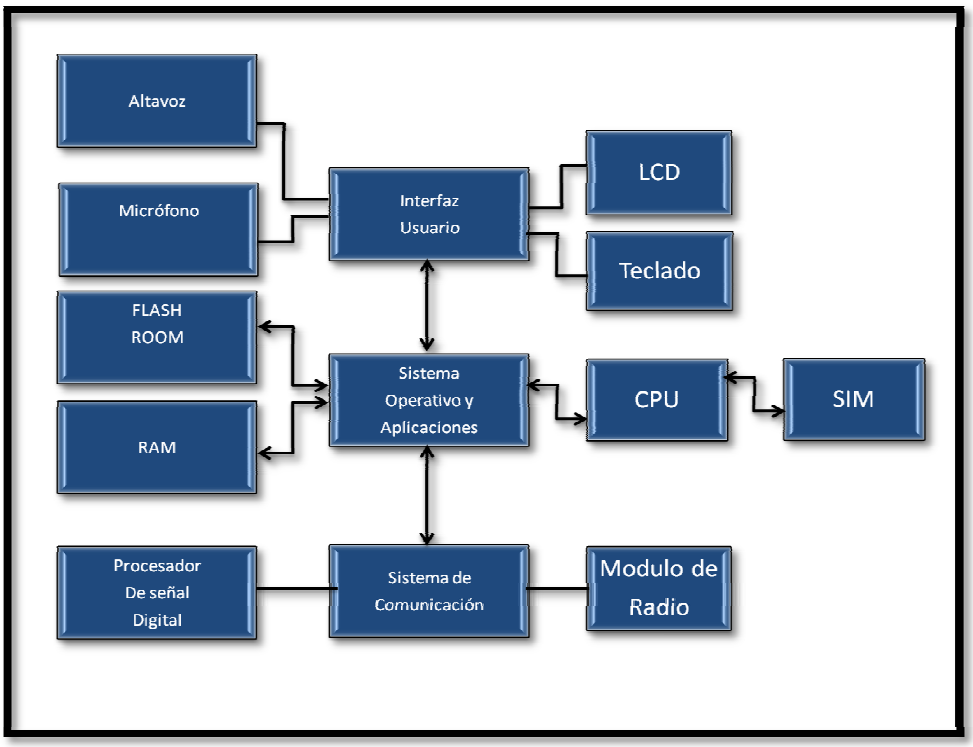

Figura 1 Arquitectura general equipo móvil.

En la figura 1 (8), se puede apreciar algunas partes como la CPU (unidad central de procesamiento) la cual controla los circuitos de comunicación del teléfono, además de controlar la comunicación con el usuario. Como medio de almacenamiento intermedio y a la vez utiliza la RAM esta es utilizada para todo almacenamiento intermedio durante la comunicación y la interacción del usuario. La RAM se puede implementar como un circuito integrado separado o puede ser integrado con el CPU en un único circuito. El teléfono también necesita un medio de almacenamiento secundario no volátil, mostrado como la Flash ROM en la (Figura 1) el cual requiere para almacenar todos los datos relacionados con el usuario y su comunicación, los cuales deben permanecer después de que ocurra una falla en el suministro de energía.

La tarjeta SIM

La tarjeta SIM (ver figura 2) es un tarjeta inteligente *Smartcard* utilizada en los equipos de telefonía celular, es obligatorio para redes GSM sirve para identificarse ante la red.

Figura 2 La tarjeta SIM.

Los estándares internacionales para estas tarjetas están regulados por la ISO/IEC a través de la familia de normas 7816. Estos entandares definen las propiedades básicas de las tarjetas inteligentes tales como son las características físicas, características de comunicación, datos almacenados, esta norma específica el hardware de la tarjeta y el chip así como los mecanismos y propiedades de las aplicaciones y sistemas operativos para las tarjetas inteligentes, además de los aspectos informáticos asociados.(9)

En la SIM es posible encontrar varios elementos de evidencia digital por ejemplo, contactos, mensajes de texto, entre otras cosas etc.

Dado que en México no se tiene claros avances de las metodologías en la informática forense, se desarrolla a continuación esta investigación a través del Internet, reportes y documentos relacionados para ello se tomó en cuenta como referencias las siguientes: NIJ *National Institute of Justice Washinton DC* y la siguiente referencia de la NIST *National Institute of Standards and Technology de los Estados Unidos.*

NIJ: Es la agencia de investigación, desarrollo y de control de delincuencia y de justicia, A través del conocimiento y herramientas orientados al manejo de evidencias que permitan resolver los desafíos de la delincuencia y la aplicación de la justicia. Este organismo presenta documentos relacionado con el manejo de evidencia digital.

Fases del proceso forense.

Para análisis forense, la investigación se divide en las siguientes fases (10):

1. **Identificación de la escena del crimen:** en esta fase se hace el reconocimiento del incidente con el objetivo de identificar el tipo de crimen. Es primordial tener precauciones para evitar la contaminación de la escena de esta fase en adelante.

2. **Preparación:** en esta fase se realiza la preparación de herramientas, técnicas, órdenes de registro y autorizaciones para acceder a la escena del crimen.

3. **Preservación de la escena del crimen:** en esta fase se realiza el aislamiento de la evidencia física y digital del mundo externo, es decir, de personas no autorizadas y dispositivos electromagnéticos.

4. **Recolección de la evidencia**: en esta fase se realiza la recolección de toda la evidencia encontrada en la escena del crimen, empezando por la más volátil hasta la menos volátil, es importante que al momento de realizar la inspección de (los) equipo (s) evitar alterar cualquier variable ya que un cambio a la vista insignificante podría invalidar todo el proceso de investigación en un proceso judicial. Por otro lado la recolección debe ser realizada mediante herramientas especializadas y certificadas por los especialistas en materia de análisis forense con el objetivo de evitar

modificaciones en las fechas de acceso y en la información del registro del sistema.

5. **Preservación de la evidencia:** es importante que durante todo el proceso de investigación forense la evidencia conserve sus propiedades con las que fue recolectada para evitar que pierda su valor de carácter legal, por lo tanto, es primordial realizar toda la investigación sobre copias exactas de la evidencia obtenida en la escena del crimen, comprobando periódicamente la integridad de dicha copia. Por otro lado es necesario actualizar la cadena de custodia de la evidencia cada vez que esta cambie de responsable, este documento debe contar con la información de donde, cuando y quien manejo la evidencia, quien la custodia y en donde esta almacenada.

6. **Análisis de la evidencia:** el objetivo de esta fase es lograr identificar como fue efectuado el ataque, cual fue la vulnerabilidad explotada y en lo posible identificar al atacante, para lograr lo anterior es necesario reconstruir la secuencia temporal del ataque, para lo cual se debe recolectar la información de los archivos asociados, marcas de tiempo, permisos de acceso y estado de los archivos.

7. **Presentación del informe forense:** Finalmente culmina la investigación y en este paso se presentan los resultados por parte del investigador sobre su búsqueda y análisis de los medios, lo que se encontró en la fase de análisis de la evidencia, así como información puntual de los hechos y posibles responsables. Debido al rigor que requiere una investigación de este tipo, cada movimiento por parte del investigador o su equipo de trabajo se debe documentar hasta que se resuelva o se dé por concluido el caso. Esta documentación se debe llevar a cabo por medio de formularios que hacen parte del proceso estándar de

investigación, entre los cuales se encuentran el documento de custodia de la evidencia, el formulario de identificación de equipos y componentes, el formulario de incidencias tipificadas, el formulario de recogida de evidencias y el formulario de medios de almacenamiento.

8. Luego de realizar las fases del modelo anterior, para que la evidencia digital pueda ser usada en procesos judiciales debe cumplir con las siguientes características:

- **Admisibilidad:** toda evidencia recolectada debe ajustarse a ciertas normas jurídicas para presentarlas ante un tribunal.
- **Autenticidad:** la evidencia debe ser relevante al caso, y el investigador forense debe estar en capacidad de representar el origen de la misma.
- **Completitud:** la evidencia debe contar todo en la escena del crimen y no una perspectiva en particular.
- **Fiabilidad:** las técnicas usadas para obtener la evidencia deben gozar de credibilidad y aceptadas en el campo en cuestión, evitando dudas sobre la autenticidad y veracidad de las evidencias.

- **Entendimiento y Credibilidad:** se debe explicar con claridad y pleno consentimiento, que proceso se siguió en la investigación y como la integridad de la evidencia fue preservada, para que ésta sea comprensible y creíble en el tribunal.

También se toma en cuenta la propuesta de la NIST la cual ha desarrollado documentos en el cual presenta una amplia discusión sobre el proceso forense en equipos de telefonía celular. Entre los diversos temas presentan un marco de trabajo para realizar el proceso de investigación digital que involucre la participación de un equipo de telefonía móvil. Y dividen en 4 faces**: 1.Preservación, 2. Adquisición, 3. Inspección y análisis, 4. Reporte**

Desarrollo

Las herramientas forenses son fundamentales para la extracción de los datos de teléfonos móviles, son las interfaces a través de la cual un analista forense puede conectarse a un dispositivo y revisar la información disponible. Algunas de las herramientas más utilizadas en esta rama son las siguientes. (11)

- Mobiledit! (C), versión lite disponible.
- Bitpim
- Tulp2g
- Secureview ®
- Celldek ®
- DeviceSeizure ®
- Pilot-Link
- Gsm .Xry ®
- Oxygen Phone Manager ®, versión lite disponible.
- Simis2 ®
- Forensic sim ®
- Forensic Card Reader ®
- Simcon ®
- Phonebase2 ®
- Usim detective ®

En este listado se representa algunas con símbolo ® que las define como uso comercial, y todas están destinadas a facilitar el trabajo de los analistas forenses.

Herramientas forenses

Las herramientas forenses para celulares y otros dispositivos portátiles son diversas hoy en día existe una gran variedad de software y herramientas, pero la gama de dispositivos sobre los que operan normalmente se redujo a plataformas distintas de la línea de productos de un fabricante, a una familia de sistemas operativos y arquitectura de hardware, por otra parte las herramientas que requiere un analista son de completo acceso al dispositivo en caso que esté protegido por algún mecanismo de autentificación o el analista puede adaptase a cualquier mecanismo de autenticación.

En la actualidad los Kits de herramientas forenses contiene una completa gama de adquisición, estas herramientas son capaces de utilizar diferentes interfaces por ejemplo de infrarrojos o Bluetooth para adquirir el acceso al contenido del dispositivo, pero la información que se puede adquirir puede variar como la información personal ;agenda de teléfonos, los registros de llamadas telefónicas, SMS, EMS, MMS, correo electrónico ,mensajería instantánea , las URL y el contenido de los sitios web visitados, audio, video, imágenes, el contenido de la SIM.

Presentar la información o contenido digital de un teléfono celular puede variar dependiendo de varios factores que son los siguientes: Las capacidades inherentes del teléfono aplicadas por el fabricante.

- Las modificaciones introducidas en el teléfono por el proveedor de servicios u operador de red.
- Los servicios de la red social suscrito y utilizado por el usuario.
- Las modificaciones introducidas en el teléfono por el usuario.

La adquisición a través de un cable de interfaz general, produce resultados superiores a los de la adquisición de las interfaces de otro dispositivo. Sin embargo, una interfaz inalámbrica, tales como el infrarrojo o Bluetooth puede servir como una alternativa cuando el cable correcto no está disponible, se debe utilizar como último recurso debido a la posibilidad de la modificación del dispositivo durante la adquisición. Independientemente de la interfaz utilizada, se debe estar alerta acerca de los problemas forenses, fijarse también que la capacidad de adquirir el contenido de una SIM puede no ser compatible con algunos instrumentos, en particular las muy orientadas hacia la PDA. En la tabla 1 se muestra las herramientas disponibles y las facilidades que ofrecen para determinados tipos de teléfonos celulares.

Herramientas forenses para dispositivos móviles.

	Función	Características
DeviceSeizure	Adquisición, Examinación, Reporte	• Palm OS , Pocket PC, teléfonos RIM OS, y ciertos modelos de GSM, TDMA,y dispositivos CDMA • Ayuda la recuperación interna SIM • Sólo es compatible con cable interfaz
Pilot-link	Adquisición	• Teléfonos OS Palm • Software de fuente abierta • No hay soporte para la recuperación de información SIM • Sólo es compatible con cable interfaz
GSM.XRY	Adquisición, Examinación, Reporte.	• Funciona con algunos modelos de GSM y CDMA • Ayuda a la recuperación interna SIM • Requiere de PC / SC de tarjetas inteligentes compatible con lector externo de tarjetas SIM • Interfaces compatible con cable, Bluetooth y infrarrojos • Compatible con radio-aislamiento SIM
Oxygen PM Forensicversion	Adquisición, Examinación, Reporte	• Funciona con modelos GSM • Compatible con varias interfaces cable USB, Bluetooth e infrarrojos • Soporte para recuperación datos SIM
MOBILedit! Forensic	Adquisición, Exanimación	• Determinados modelos de teléfonos GSM • Soporte para recuperación dato SIM • Compatible con cables e interfaces IR
BitPIM	Adquisición, Reporte	• Determinados modelos de teléfono GSM • Software libre • No hay soporte para la recuperación de información SIM

TULP2G	Adquisición, Examinación	• Soporte para teléfonos GSM y CDMA que utilizan los protocolos de apoyo para establecer la conectividad • Soporte para recuperación de datos SIM • Requiere lector PC / SC de tarjetas inteligentes compatible con tarjetas SIM • Apoya la creación de aislamiento de radio-SIM con la tarjeta de GEM Xpresso
Secure View	Adquisición, Examinación Reporte.	• Soporte para teléfonos GSM, CDMA y TDMA que utilizan los protocolos de apoyo para establecer la conectividad • Soporte para recuperación de datos SIM • Requiere lector PC / SC de tarjetas inteligentes compatible con tarjetas SIM • Cable, Bluetooth y de infrarrojos interfaces compatibles
PhoneBase2	Adquisición, Examinación Reporte	• Soporte para teléfonos GSM, CDMA y TDMA que utilizan los protocolos de apoyo para establecer la conectividad • Soporte para recuperación de datos SIM • Requiere lector PC / SC de tarjetas inteligentes compatible con tarjetas SIM Cable, Bluetooth y de infrarrojos interfaces compatibles
CellDEK	Adquisición, Examinación Reporte	• Soporte para teléfonos GSM, CDMA y TDMA que utilizan los protocolos de apoyo para establecer la conectividad • Soporte para recuperación de datos SIM • Requiere lector PC / SC de tarjetas inteligentes compatible con tarjetas SIM Cable, Bluetooth y de infrarrojos interfaces compatibles

En esta tabla las aplicaciones de software que se describen, operan sobre dispositivo de comunicación, a través de una interfaz conectada.

Tabla 1 Herramientas forenses.

Debido a la arquitectura de estos dispositivos móviles han surgido herramientas y software forenses que tiene que ver exclusivamente con tarjetas SIM de forma independiente de sus teléfonos móviles.

La tarjeta SIM debe ser removida desde el teléfono y se inserta en un lector apropiado para la adquisición. Se requiere de un lector especializado que acepta una tarjeta SIM telefónica.

La tabla 2 enumera varias herramientas SIM forense. Los siete primeros en la lista de incautación de dispositivos, TULP2G, GSM. XRY, MOBILedit!, Secure View, PhoneBase2 y CellDEK también se ocupan de la adquisición de la memoria del teléfono, como se señaló anteriormente.

Herramientas forenses (SIM)

La siguientes softwares de la tabla que se describe se especializan únicamente sobre las tarjetas SIM's.

	Función	Características
Device Seizure	Adquisición , Examinación Reporte	• También Recupera la información de una tarjeta SIM a través del auricular • Requiere lector de propiedad del paraben SIM
TULP2GF	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC • Soporta la creación de radio de aislamiento SIM

GSM.XRY	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC • Soporta la creación de radio de aislamiento SIM
Mobiledit! Forensic	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC
Secure View	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC
PhoneBase2	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC
Cell DEK	Adquisición , Examinación Reporte	• También se recupera la información de una tarjeta SIM a través del auricular • Compatible con lector PC / SC
SIMIS2	Adquisición , Examinación Reporte	• Factores externos tarjetas SIM • Compatible con lector PC / SC • Soporta la creación de radio de aislamiento SIM
Forensic SIM	Adquisición , Examinación Reporte	• Factores externos tarjetas SIM • Requiere ForensicSIM • Soporta la creación de radios aislamiento
Forensic Card Reader	Adquisición , Examinación Reporte	• Factores externos tarjetas SIM • Compatible con lector PC / SC
SIMCon	Adquisición , Examinación Reporte	• Factores externos tarjetas SIM • Compatible con lector PC / SC
USIM detective	Adquisición , Examinación Reporte	• Factores externos tarjetas SIM • Compatible con lector PC / SC

Tabla 2 Forense SIM.

Es esta etapa de investigación que se llevó a cabo sobre dispositivos móviles se profundizo sobre las tarjetas SIM, tarjeta inteligente desmontable usada en teléfonos móviles. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta.

El uso de la tarjeta SIM es obligatorio en las redes GSM Su equivalente en las redes UMTS se denomina USIM.

Las tarjetas SIM están disponibles en dos tamaños. El primero es similar al de una tarjeta de crédito (85,60 × 53,98 × 0,76 mm). El segundo y más popular es la versión pequeña (25 × 15 × 0,76 mm).

La tarjeta también posee información independiente a la del sistema operativo del teléfono y la información que suele contener es:

- IMSI (Clave identificativa para cada dispositivo en el sistema), información sobre idiomas preferidos.
- Información sobre la localización: La SIM guarda la última área en donde el dispositivo se registró ante el sistema.
- MSISDN: el cual puede ser usado para recuperar las llamadas originadas por el usuario a otros números de teléfono.
- Información sobre el tráfico SMS: Es posible leer mensajes enviados y recibidos fuera de la tarjeta SIM y saber si fue leído o no cada mensaje.
- Información sobre el proveedor: Es posible obtener el nombre del proveedor y la red celular comúnmente usada para la comunicación, junto con las redes que están prohibidas para el dispositivo.

Niveles de seguridad SIM

PIN: Al intentar acceder la información de la SIM se requiere introducir el número de identificación personal de la tarjeta. En caso de que sea introducido más de tres veces de forma errónea, esta se bloquea, siendo necesario el código PUK, suministrado por el fabricante u operadora.

PUK: Este código sirve para habilitar tarjeta SIM debido a la introducción errónea del PIN. En algunos sistemas, si el PUK es introducido de manera incorrecta determinado número de veces, la información de la SIM se elimina de manera automática y de manera irrecuperable.

Analizando una tarjeta SIM

Lo fundamental es disponer de un lector de tarjetas *SIMOMNIKEY* (Figura 3) en este caso se eligió por su compatibilidad y disponibilidad en el mercado se adquirido a un costo de $ 2.100.00 enviado del país de Estado Unidos de la Ciudad Austin Texas, dispositivo que es compatible con los controladores PC/SC.

Figura 3 Omnikey

Las características son las siguientes:

- Dispositivo de lectura y escritura por USB.
- Busca, edita, añade y borra entradas de la tarjeta SIM.
- Permite hacer copias de seguridad.
- Permite manejar los PIN's.
- Exporta la libreta de direcciones a Outlook, MS Office.
- Software de exploración de ficheros.

En esta ocasión para obtener información de la **SIM** se utilizará MOBILedit! En la versión 5.0.2.1015**,** y el resultado se muestra en la (figura 4).

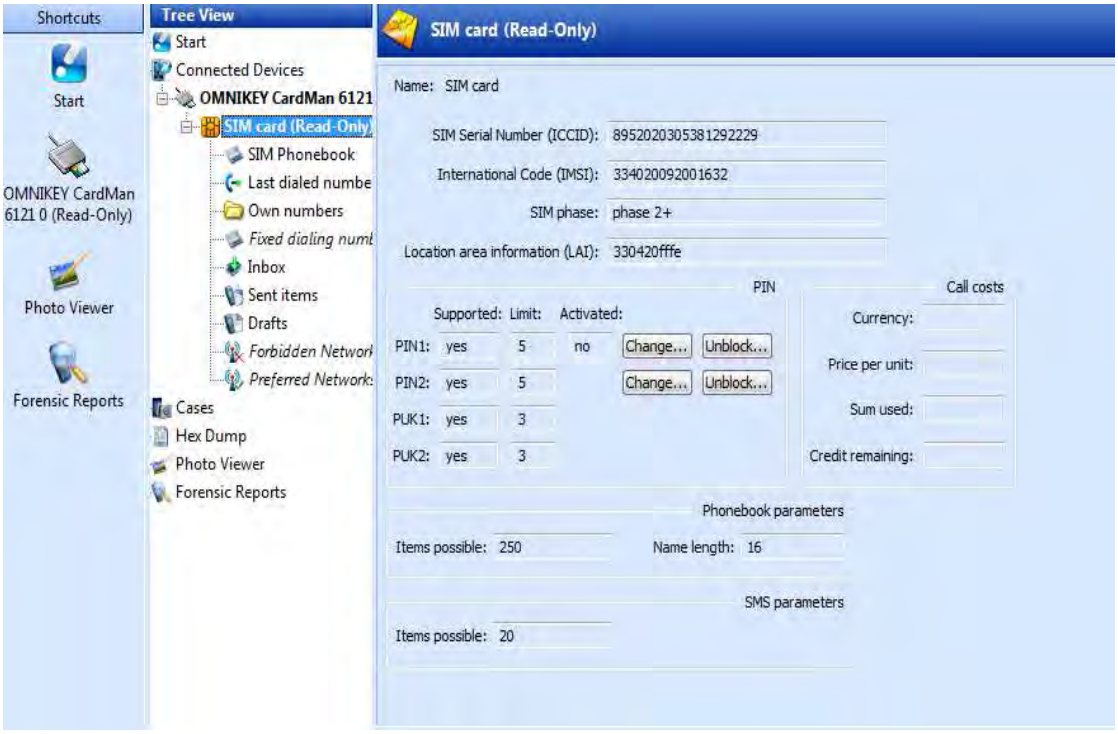

Figura 4 Leyendo Sim Card.

En esta pantalla se puede cambiar o deshabilitar el acceso a las contraseñas o PIN's. A simple vista se puede observar (**IMSI)** de la SIM (Ver figura 4), que es Clave identificativa para cada dispositivo en el sistema, las tarjetas SIM se identifican en sus redes móviles individuales mediante un IMSI único. Los operadores de telefonía móvil conectan las llamadas a teléfonos móviles y se comunican con sus tarjetas SIM comercializadas usando su IMSI.

Figura 5 SIM.

En la figura 5 se puede notar la **ICCID** (*International Circuit Card ID*, Identificador Internacional de la Tarjeta de Circuitos por sus siglas en inglés). Los ICC-IDs se almacenan en las tarjetas SIM y también se graban o imprimen sobre el cuerpo de plástico de las mismas en un proceso de personalización. Además, cada ICC cuenta con un número de identificación personal de 19 dígitos.

En la figura 6 se observa la lista de contactos SIM que se almacena.

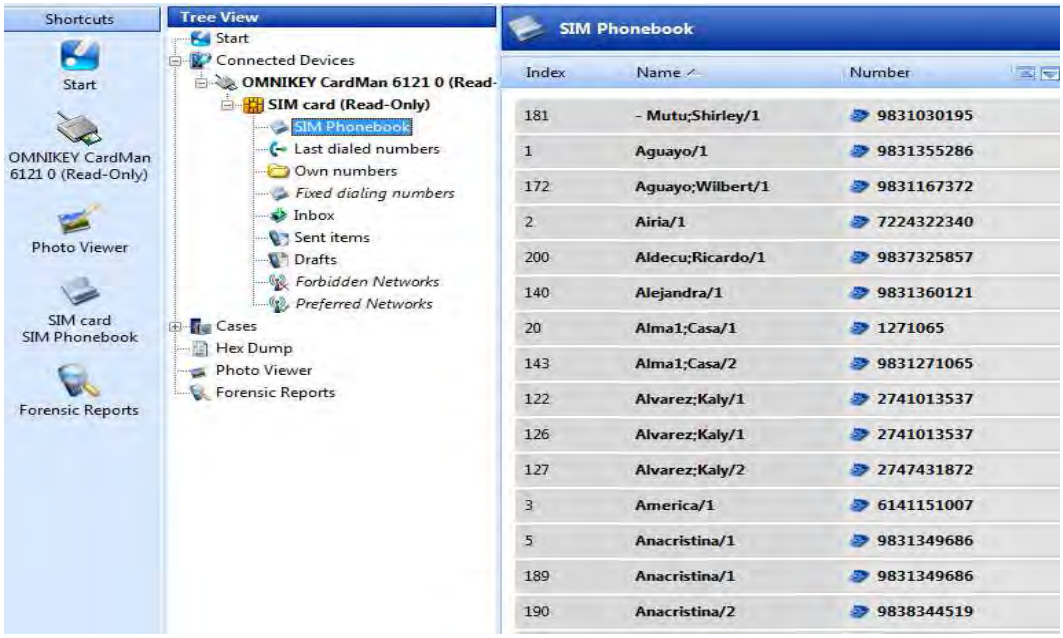

Figura 6 Contactos SIM.

En la Figura 7se identifica una lista de números de los últimos números marcados por el usuario.

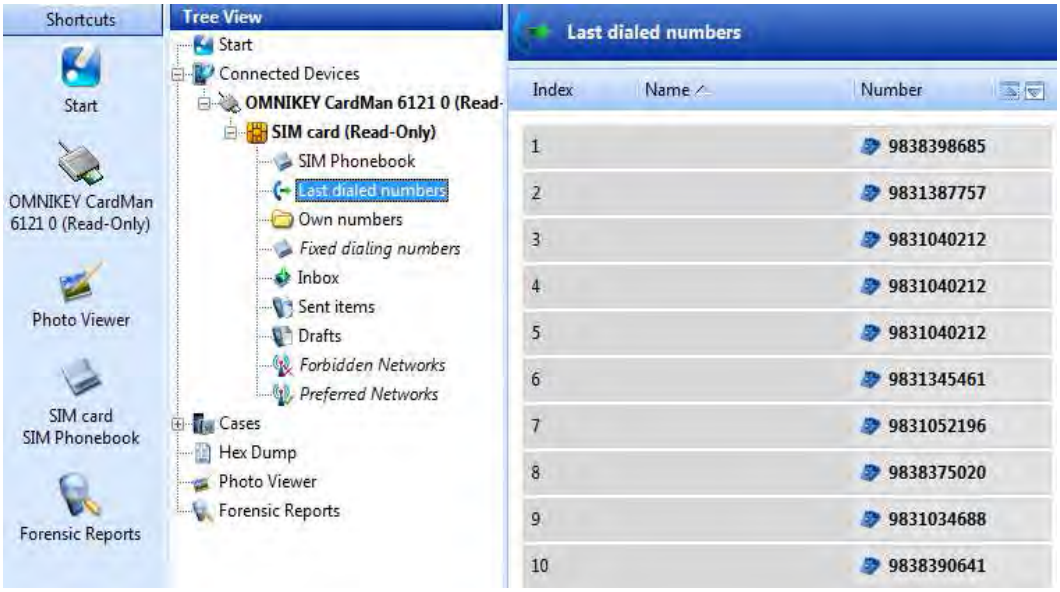

Figura 7 Números Marcados.

En la (figura 8) se identifica información recibida en la bandeja de entrada como hora y fecha del SMS de la SIM.

Figura 8 Mensajes guardados SIM.

En la (figura 9) se identifica SMS enviado por el usuario hacia otro dispositivo móvil.

Figura 9 Mensaje enviado SIM.

Nota: (este software es comercial) para generar el reporte específico y detallado del sistema se necesita activar el producto este software está considerado dentro de la gama de herramientas forenses consultados y recomendados por compañías que se dedican al trabajo del análisis forense informático esto es solo una muestra para abrir el camino al campo de la seguridad de la información. Dicha información puede ser usada para fines legales.

Conclusiones

Debido a la creciente necesidad de aportes para el campo de la informática forense en dispositivos móviles, se realizó este trabajo de investigación principalmente sobre los dispositivos que operan en redes de telecomunicaciones GSM.

La investigación realizada da a conocer las diversas metodologías que existen y las formas de estudiar un dispositivo móvil, permitiendo conocer los sistemas operativos que los rigen, la arquitectura y los dispositivos que la componen, sé observó que dichas metodologías existentes permiten la incautación de la información digital en un dispositivo móvil.

El desarrollo de esta investigación se realizó con una desventaja, la cual fué no poder adquirir el equipo adecuado por el alto costo que este representa, así se optó por adquirir herramientas más económicas que permitieran el análisis de una SmarCard, también se tomó en cuenta la disponibilidad en el mercado de ciertas herramientas y su compatibilidad con diversos software, siendo el dispositivo *SIMOMNIKEY* el más accesible.

Se priorizó estudiar la SIM's componente principal de un dispositivo GSM en donde se almacena información fundamental de registros antiguos entre los cuales destacan las llamadas y mensajes eliminados de un dispositivo móvil.

La metodología aplicada dio el resultado esperado, se obtuvo la evidencia digital, aunque no se descarta la posibilidad de utilizar otra metodología o herramienta requerida para el estudio de esta ciencia, ya que no existe un solo método para aplicación de esta ciencia, dentro del marco de análisis forense de las SIM cada método existente sugiere realizar un reporte, o informe detallado de la información recabada durante el estudio realizado, con el fin de tener la presentación de los resultados.

El método que se utilizó en esta investigación la emplean diversas organizaciones como la policía especializada en delitos informáticos, guardia civil entre otros para recuperar información eliminada de un dispositivo móvil y es recomendable acudir a estas organizaciones, ya que éstas toman en cuenta aspectos, legales y de validez ante un penal.

Durante la investigación se contactó a una empresa llamada *Cellebrite Mobile Data Secured (UFED)* la cual cuenta con una línea de productos destinados a la industria del análisis forense, está empresa maneja una de las herramientas más eficaces y altamente recomendable, ofrece un kit de herramientas forenses con los dispositivos universales, además del software adecuado para realizar la extracción de evidencia digital en un teléfono o en una tarjeta SIM , pero para esta investigación no fue posible adquirirse debido a su costo elevado, aunque no queda descartada la posibilidad de adquirir este kit de herramientas y en futuro iniciar un nuevo proyecto con nuevos retos , puesto que la tecnología móvil día a día se está innovando.

Para concluir, la tecnología no sólo debería innovar el aspecto de los teléfonos celulares o la durabilidad de estos, desde mi punto de vista deberían de brindar seguridad a los usuarios, esto es; que puedan almacenar información sin la inseguridad de que cualquier persona en alguna parte del mundo y sin conocimiento del usuario pueda acceder y crear modificaciones, los celulares

son cada vez más utilizados por la sociedad y permiten a los usuarios tener un mayor control de la información que les resulta vital, junto con las redes de telecomunicaciones posibilitan la conexión a internet y de esta manera la sociedad se beneficia, la comunicación ya paso de ser un lujo a un recurso necesario.

Bibliografía

Dispositivos móviles, análisis forense y sus futuros riesgos. (11 de abril de 2008). (Israel Becerril Sierra) Recuperado el 23 de Febrero de 2011, de http://www.revista.unam.mx/vol.9/num4/art26/art26.pdf

Revista digital Universitaria . (10 de abril de 2008). Recuperado el 2011 de marzo de 3, de Dispositivos móviles, análisis forense y sus futuros riesgos : http://www.revista.unam.mx/vol.9/num4/art26/int26.htm

streets,Office& Bullets. (13 de Agosto de 2009). Recuperado el 10 de mayo de 2011, de Análisis forenses a tarjetas SIM (Recuperando SMS's): http://acidous.wordpress.com/2009/08/13/analisis-forenses-a-tarjetas-sim-recuperando-smss/

Dragon Jar . (2011). Recuperado el 10 de mayo de 2011, de http://www.dragonjar.org/tag/analisis-forense

Análisis Forense En Dispositivos Móviles Con SYMBIAN OS. (s.f.). (Maestría en Ingeniería Electrónica, Pontificia Universidad Javeriana) Recuperado el 25 de Enero de 2011, de http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf

Andrea Ariza, J. R. (s.f.). *Un Nuevo Reto para la Informática Forense.* Recuperado el 8 de mayo de 2011, de http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion6%284%29.pdf

Ashcroft, J. (Julio de 2001). *Electronic Crime Scene Investigation:A Guide for First Responders.*Recuperado el 2 mayo de Abril de 2011, de http://www.ojp.usdoj.gov/

Carlos Andrés Castillo Londoño, R. A. (2008). Guía Metológica para el análisis Forense Orientado a Incidentes en Dispositivos Móviles GSM. Bogota.

Curbelo, D. A. (s.f.). *http://acurbelo.org/.* Recuperado el 03 de Mayo de 2011, de Telefonía Móvil: http://acurbelo.org/adof3115/cellphones-etiquette-security.pdf

Delaitre, R. A. (2007). *Cell Phone Forensic Tools: An Overview and Analysis Update.*United States Of America.

Delgado, Miguel Lopéz. (Junio de 2007). *Análisis Forense Digital*. Recuperado el 3 de Marzo de 2011, de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Forensics Project. (s.f.). (My Dizayn.) Recuperado el 7 de mayo de 2011, de http://forensics-project.org/analisis-forense-en-dispositivos-moviles-sim-card-i

Galván, I. S. (2009). Propuesta de una Metodología De Análisis Forense Para Dispositivos De Telefonía Celular. Mexico.

Juan Felix Basterretche. (2007). *Universidad Nacional del Nordeste.* Recuperado el 28 de Abril de 2011, de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/tfbasterretche.pdf

Glosario

GSM: Global System for Mobile communications (Sistema Global para las comunicaciones Móviles), es el sistema de teléfono móvil digital más utilizado y el estándar de facto para teléfonos móviles.

CDMA: Es una técnica de acceso múltiple digital especificada por la Asociación de Industria de Telecomunicaciones (TIA) como "IS-95." La TIA aprobó el estándar CDMA IS-95 en julio 1993.

CPU: Abreviatura de Central Processing Unit (unidad de proceso central), es el procesador o procesador central.

Roaming: Itineranciase refiere a la capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad.

EMS: (Enhanced Messaging Services) Nuevo estándar de mensajería que permite la descarga y el envío/recepción de mensajes de texto acompañados de melodías, imágenes y animaciones.

Forensis: proviene del latín forensis (sitio donde los tribunales juzgan las causas) e implica un ejercicio y aplicación de procedimientos.

ICC-ID: International Circuit Card ID, 'Identificador Internacional de la Tarjeta de Circuitos'). Los ICC-IDs se almacenan en las tarjetas SIM y también se graban o imprimen sobre el cuerpo de plástico de las mismas en un proceso de personalización. Además, cada ICC cuenta con un número de identificación personal de 19 dígitos.

IMSI:(International Mobile Subscriber Identify, 'Identidad Internacional del Suscriptor Móvil') único.

LCD:(acrónimo del inglés Liquid Crystal Display) es una pantalla delgada y plana formada por un número de píxeles en color o monocromos colocados delante de una fuente de luz o reflectora.

MMS: Sistema de mensajería multimedia es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos o cualquier otro contenido disponible en el futuro.

MSISDN: Mobile Subscriber Integrated Services Digital Network Number "Es Un número de identificación única de una suscripción en una red GSM o una red móvil UMTS.

PDA: (Del inglés personal digital assistant (asistente digital personal)), también denominado ordenador de bolsillo, es una computadora de mano originalmente diseñado como agenda electrónica.

PIM: (Personal Information Management) Sistema avanzado de gestión del organizador del teléfono móvil. Permite programar el calendario y sincronizarlo con Pc y PDA.

PIN:(Personal Identiffication Number) Código personal de 4 números que nos permite limitar el acceso a nuestra tarjeta SIM. Totalmente personalizable, e incluso se puede suprimir.

PUK:(Personal Unlock Key) Código de 4 números asociado a la SIM que permite desbloquearla el acceso. Se facilita con la propia SIM y no se puede variar.

RAM: Son las siglas de random access memory, un tipo de memoria de ordenador a la que se puede acceder aleatoriamente.

UTMS: Sistema Universal de Telecomunicaciones Móviles (Universal Mobile Telecommunications System) es una de las tecnologías usadas por los móviles de tercera generación.

Roaming: Se refiere a la capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad.

ROM:(Read-onlymemory) o memoria de sólo lectura, es la memoria que se utiliza para almacenar los programas que ponen en marcha el ordenador y realizan los diagnósticos.

SIM: (acrónimo en inglés de subscriber identity module, en español módulo de identificación del suscriptor) es una tarjeta inteligente desmontable usada en teléfonos móviles.

Smart Card: Una tarjeta inteligente (smartcard) son circuitos integrados que permiten la ejecución de cierta lógica programada.

SMS: son las siglas de Servicio de Mensaje Corto. Disponible en redes digitales GSM permitiendo enviar y recibir mensajes de texto de hasta 160 caracteres a teléfonos móviles vía el centro de mensajes de un operador de red.

TDMA: Acceso múltiple por división de tiempo**,** Permite a varios usuarios compartir el mismo canal de frecuencia al dividir la señal en intervalos de tiempo diferentes.