ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y ANÁLISIS DE EVIDENCIA DIGITAL EN TELÉFONOS CELULARES CON TECNOLOGÍA GSM PARA PROCESOS JUDICIALES

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

JORGE ALEXANDER MALEZA PEÑAHERRERA

(a.maleza@ieee.org)

KARINA GABRIELA SANDOVAL DUQUE

(karina_sandoval@ieee.org)

DIRECTOR: ING. PABLO HIDALGO

(phidalgo@ieee.org)

Quito, Noviembre 2011

DECLARACIÓN

Nosotros, Jorge Alexander Maleza Peñaherrera y Karina Gabriela Sandoval Duque, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Alexander Maleza Karina Sandoval

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Alexander Maleza Peñaherrera y Karina Gabriela Sandoval Duque, bajo mi supervisión.

_____

Ing. Pablo Hidalgo

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradecemos a Dios por darnos la vida, paciencia, entendimiento y perseverancia, para luchar por nuestros sueños y no desmayar en el camino.

Agradecemos de manera muy especial a nuestros padres, por brindarnos amor, comprensión y palabras precisas en los momentos difíciles, para con ello recordarnos lo importante que es culminar una actividad empezada y así poder sentir la satisfacción de una labor bien realizada.

Agradecemos al Ing. Pablo Hidalgo por su colaboración y apertura constante en el desarrollo de este proyecto, por las palabras de aliento y jalones de orejas cuando eran necesarios.

Al Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado, en especial al Dr. Santiago Acurio del Pino, por su colaboración, excelente disposición y apertura.

Al IEEE y de manera especial a la Rama Estudiantil de la Escuela Politécnica Nacional, gracias a todos quienes la conforman, por su apoyo en los momentos fáciles y difíciles en el desarrollo del Proyecto de Titulación.

A nuestro compañeros, amigos y conocidos, por las vivencias y enseñanzas compartidas, pues en cada aventura aprendimos lo importante que es tener alguien en quien confiar y trabajar en equipo.

A nuestros profesores, que durante toda la carrera nos han preparado para culminar con éxitos la misma.

Alexander Maleza

Karina Sandoval

DEDICATORIA

De manera especial a mi Madre quien con su amor me ha ayudado a sobrepasar cualquier reto que me he propuesto, y quien indirectamente estuvo conmigo en esas largas noches de estudio.

A mi Padre quien siempre está apoyándome en el camino de mi vida y quien confió en mí cuando le dije que estarían las siglas “Ing.” antes de mi nombre.

A mi hermana quien me brindó su apoyo incondicional y las palabras justas en el momento preciso.

A mis familiares, amigos y conocidos IEEE quienes me brindaron su apoyo y aliento para culminar esta meta.

Alexander Maleza

DEDICATORIA

Principalmente a Dios por su inmensa misericordia y amor. A mis padres quienes con sus enseñanzas y apoyo supieron sembrar en mí la semillita de la perseverancia. Pues “No hay que darse por vencida ni aun vencida, hay que levantarse y salir a triunfar”.

A mis hermanas y sobrinos quienes supieron brindarme su amor y apoyo incondicional.

A mis familiares quienes me brindaron su apoyo y aliento para culminar una de mis metas. Pero de forma especial a mis abuelitos Papito Flavio y Mamita Carmen, quienes con su amor, mimos y consejos me enseñaron el valor de la responsabilidad y humildad en cada logro alcanzado.

A mis amigos con quienes descubrimos las diferentes facetas de mi personalidad, pero aprendieron a tenerme paciencia, gracias por su apoyo, comprensión y locuras…

Los quiero mucho a TODOS, Dios los bendiga…

Karina Sandoval

CONTENIDO

CAPÍTULO 1

CAPÍTULO 2

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ACRÓNIMOS

ACPO	*Association of Chief Police Officers*
AND	*Abbreviated Dialing Numbers*
AGCH	*Access Grant Channel*
APDU	*Application Protocol Data Unit*
API	*Application Programming Interface*
ASETA	Asociación de Empresas de Telecomunicaciones de la Comunidad Andina
BCCHA	*Broadcast Control Channel*
BGA	*Ball Grid Array*
BS	*Base Station*
BTS	*Base Transceiver Station*
CASETEL	Colombia, Cámara de Empresas de Servicios de Telecomunicaciones
CDMA	*Code Division Multiple Access*
CDR	*Call Detail Record*
CF	*Compact Flash Card*
CHV	*Chip Holder Verification*
CINTEL	Centro de Investigación de las Telecomunicaciones
CITEL	Comisión Interamericana de Telecomunicaciones
CONATEL	Consejo Nacional de Telecomunicaciones
CPU	*Central Processing Unit*
CSI	*Computer Crime and Security Survey*
DCS	*Digital Cellular System*
DF	*Dedicated Files*
DSP	*Digital Signal Processor*
EDGE	*Enhanced Data rates for GSM of Evolution*
EEPROM	*Electrically-Erasable Programmable Read-Only Memory*
EF	*Elementary Files*
EMS	*Enhanced Messaging Service*
EXT1	*Extension1*
EXT2	*Extension2*
EXT3	*Extension3*

FDMA	*Frequency Division Multiple Access*
GPRS	*General Packet Radio Service*
GPS	*Global Positioning System*
GSM	*Global System For Mobile Communications*
HSPA	*High-Speed Packet Access*
HTTP	*Hypertext Transfer Protocol*
ICCI	*Integrated Circuit Card Identifier*
IDC	*International Data Corporation*
IEEE	*Institute of Engineers Electrical and Electronics*
IMAP	*Internet Message Access Protocol*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
IP	*Internet Protocol*
JTAG	*Joint Test Action Group*
LAC	*Location Area Code*
LAI	*Location Area Information*
LCD	*Liquid Crystal Display*
LND	*Last Numbers Dialled*
LOCI	*Location Information*
LOCIGPRS	*Location Information GPRS*
LTE	*Long Term Evolution*
MCC	*Mobile Country Code*
MDA	*Mobile Data Association*
ME	*Moblie Equipment*
MF	*Master File*
MMC	*Multimedia Card*
MMS	*Multimedia Messaging System*
MNC	*Mobile Network Code*
MS	*Mobile Station*
MSC	*Mobile Switching Center*
MSIN	*Mobile Subscriber Identity Number*
MSISDN	*Mobile Station International Subscriber Directory Number*
NGMN	*Redes Móviles de Próxima Generación*

NIST *National Institute of Standards and Technology*
NPI *Numbering Plan Identification*
OBEX *Object Exchange*
OMPT *Open Mobile Terminal Platform*
PCB *Printed Circuit Board*
PCH *Pagging Channel*
PDA *Personal Digital Assistant*
PIN *Personal Identification Number*
PM *Permanent Memory*
POP Post Office Protocol
PSTN *Public Switching Telephonic Network*
PUK *Personal Unlocking Key*
RAC *Routing Area Code*
RAI *Routing Area Information*
RAM *Random Access Memory*
RIM *Research In Motion*
RISC CPU *Reduce Instruction Set CPU*
RISC *Reduced Instruction Set Computing*
ROM *Read Only Memory*
SAT *SIM Application Toolkit*
SD *Secure Digital*
SDK *Software Development Kit*
SDN *Service Dialling Numbers*
SIM *Subscriber Identity Module*
SMS *Short Message Service*
SMT *Surface Mount Technology*
SMTP *Simple Mail Transfer Protocol*
SO Sistema Operativo
SPN *Service Provider Name*
SWGDE *Scientific Working Group on Digital Evidence*
TAC *Type Allocation Code*
TAP *Test Access Port*
TDMA *Time Division Multiple Access*

TIC	Tecnologías de la Información y de la Comunicación
TON	*Type Of Number*
TSOP	*Thin Small-Outline Package*
URL	*Uniform Resource Locator*
UTI	Unión Internacional de las Telecomunicaciones
WAP	*Wireless Application Protocol*
WiFi	*Wireless Fidelity*
WiMAX	*Worldwide Interoperability for Microwave Access*
WLAN	*Wireless Local Area Network*
WPAN	*Wireless Personal Area Network*

RESUMEN

El Estudio y Análisis de Evidencia Digital en Teléfonos Celulares con Tecnología GSM para Procesos Judiciales, se desarrolló en base a estudios de investigadores nacionales, que han venido trabajando en el desarrollo de procedimientos para la validación de evidencia digital, y organismos internacionales que han desarrollado herramientas forenses especializadas en hardware y software, que ayudan a encontrar evidencia y analizarla para procesos judiciales.

Este trabajo se divide en cinco capítulos, además de anexos en los que se incluyen formularios propuestos a utilizar en una investigación y la documentación de un caso.

En el capítulo 1 se realiza una investigación sobre la penetración de los teléfonos celulares con tecnología GSM en el mundo y cómo pueden ser utilizados éstos como evidencia digital.

En el capítulo 2 se reconoce y analiza la evidencia digital potencial que puede ser proporcionada por el teléfono celular y la tarjeta SIM. Paralelamente se investiga y analiza para la extracción de evidencia digital, técnicas de análisis lógico y físico; así mismo, se analiza cómo mantener íntegra esta evidencia digital.

En el capítulo 3, se hace un estudio de las herramientas existentes en el mercado tanto de software y hardware, para la extracción de información útil del teléfono celular y demostrar su integridad después de la extracción.

En el capítulo 4, se propone y redacta un procedimiento técnico-legal que servirá como guía para un adecuado manejo de la evidencia electrónica y digital en una investigación judicial. El mismo se acopla a la realidad Ecuatoriana y permite a las personas responsables (investigadores, técnicos y peritos) llevar un adecuado registro de la información recopilada del teléfono celular.

En el capítulo 5, se describen las conclusiones a las que se han llegado con la realización de este Proyecto de Titulación. Se mencionan además, las recomendaciones pertinentes según el caso.

PRESENTACIÓN

El presente Proyecto de Titulación tiene por objetivo proponer un sistema de análisis forense para teléfonos celulares con tecnología GSM. Este análisis permite obtener evidencias o pruebas auténticas e integras, que contribuyen a la investigación en un proceso judicial y posteriormente puedan ser validadas para el mismo; en la actualidad el teléfono celular forma parte de la vida cotidiana de las personas y es por esta razón que éstos se hallan involucrados en diferentes tipos de delitos.

Este hecho ha creado la necesidad de que tanto la Policía Judicial, Fiscalía y la Función Judicial deban especializarse y capacitarse en nuevas áreas en donde las TICs (Tecnologías de la Información y de la Comunicación) se convierten en herramientas necesarias en auxilio de la Justicia y la persecución del delito y del delincuente.

En el proyecto se establecerá qué evidencia digital potencial puede ser proporcionada por el teléfono celular, para lo cual se analizará la información del Equipo móvil y la Tarjeta SIM.

Por ello se propone y redacta un procedimiento desde el punto de vista técnico y legal, que servirá como guía para realizar un adecuado manejo de la evidencia electrónica y digital en la investigación judicial bajo la cual esté involucrado el teléfono celular. Paralelamente se analiza el marco legal y regulatorio que existe en el País acerca de evidencia digital, para abordar su importancia, pues actualmente no se tiene leyes claras al respecto.

El estudio realizado en el presente Proyecto de Titulación, ha sido desarrollado en la base a la situación actual de Evidencia Digital en teléfonos celulares con tecnología GSM en Ecuador respecto a técnicas de análisis, herramientas de extracción, leyes y procedimientos; sin embargo este procedimiento intenta ser una primera guía ya que el campo de la tecnología está en constante evolución.

CAPÍTULO I

CAPÍTULO 1

1. IMPORTANCIA DEL ANÁLISIS FORENSE DE TELÉFONOS CELULARES

La necesidad de comunicación del ser humano lo ha motivado a desarrollar sistemas altamente sofisticados, que incorporan conceptos inalámbricos y de movilidad para facilitar y mejorar la comunicación al desplazarse libremente.

Es de esta forma que el campo de las comunicaciones inalámbricas móviles representadas principalmente por las tecnologías celulares, se ha convertido en uno de los ejes más destacados de las telecomunicaciones a nivel global.

1.1 INTRODUCCIÓN

En la actualidad, y desde hace aproximadamente diez años, el empleo de dispositivos móviles se ha incrementado notablemente [1].

"El uso de sistemas de telecomunicaciones móviles en todo el mundo ha llegado a proporciones casi epidémicas", principalmente por su facilidad de uso y la propiedad de mantener en contacto permanente a sus usuarios, por lo cual se ha generado un cambio significativo en la forma en que las personas se comunican, pero también por su proliferación ha incrementado su uso en actividades de orden delictivo [1].

Los teléfonos celulares, así como todos los dispositivos móviles, son aparatos que en la actualidad utiliza la mayoría de la gente. Al igual que las computadoras, estos artefactos han dejado de ser un lujo, pues se han convertido en una necesidad.

Además de cumplir con la función básica de un teléfono, que es realizar y recibir llamadas telefónicas, cuentan con funciones especiales, entre las que se encuentran, el envío de mensajes de texto cortos (SMS, *Short Message Service*), sistema de mensajes multimedia (MMS, *Multimedia Messaging System*), correos electrónicos, navegación en Internet y administración de información personal [2].

El crecimiento de la telefonía celular en nuestras sociedades está en aumento; los avances en tecnología de semiconductores relacionados con teléfonos celulares han llevado al aumento del poder computacional de éstos, incrementado su funcionalidad, lo que ocasiona a su vez que la tendencia de compra de celulares continúe creciendo.

Para tareas ordinarias, los teléfonos celulares proveen las mismas funcionalidades que brinda una computadora de escritorio. Esto hace que los celulares se conviertan potencialmente en una valiosa fuente de evidencia en un análisis forense[1].

Existe gran variedad de dispositivos móviles, dentro de los cuales el mayor crecimiento en popularidad y uso se presenta en los dispositivos móviles inteligentes, debido a su capacidad tanto para realizar llamadas como para navegar por Internet; además, porque permiten desarrollar y ejecutar aplicaciones que no necesariamente son incluidas por el fabricante.

Los teléfonos celulares inteligentes permiten a los usuarios la instalación de ciertas aplicaciones, tales como, procesadores de texto, hojas de cálculo y aplicaciones de almacenamiento de datos.

Además proporcionan la habilidad de ver e imprimir información confidencial y/o documentos electrónicos, lo que transforma a estos dispositivos en oficinas móviles, esto sin importar el sistema operativo que utilice, la forma en la que se sincronice o cómo se conecten con las computadoras.

Según la Revista Lideres, en el año 2006 Porta [2] y Movistar en Ecuador empezaron a comercializar la marca *BlackBerry*, de la firma canadiense RIM[3] (RIM, *Research in Motion*) y cada día existen más ecuatorianos que utilizan estos

[1] *Análisis Forense* es la obtención y estudio de datos empleando métodos que distorsionen lo menos posible la información con el objetivo de reconstruir todos los datos y/o los eventos que ocurrieron sobre un sistema en el pasado. RIVAS, José L, FRAGOSO, Carlos, Análisis Forense, Auditorías y Detección de Intrusiones, 2006.

[2] *Porta*, Conecel S.A es una empresa de Telecomunicaciones que presta servicios a Ecuador, la misma que desde el 20 de Marzo del 2011 paso a llamarse Claro

[3] *RIM, Research in Motion e*s una compañía canadiense con vastos conocimientos en teléfonos inteligentes como los *BlackBerry.*

equipos. Según Eduardo Amador, gerente de Pospago de Porta, el mercado se duplicó entre los años 2009 y 2010. “Entre los clientes contamos con ejecutivos, jóvenes y amas de casa” [3].

Un estudio de la consultora de mercados tecnológicos IDC, utilizados por la firma Yellow Pepper, confirma la creciente demanda de estos equipos. El número de iPhone (Apple) vendidos en el año 2009 en Ecuador fue de 2 750; pero solo en el primer semestre del año 2010, la cifra fue de 3 770 unidades. En el caso de los equipos de la finlandesa Nokia en el año 2009 se comercializaron 32 842 equipos y entre enero y junio del año pasado fueron 32 692 unidades [3].

Un caso especial es el de *BlackBerry*, que se ha convertido en el equipo favorito de los usuarios ecuatorianos, de acuerdo a las fuentes consultadas. Según una estimación de *Location World*, en el país funcionan alrededor de 400 000 terminales *BlackBerry* [3].

El aumento de la capacidad de memoria interna, el poner *slots* para poder añadir memorias externas, colocar procesadores de texto y navegadores de Internet son pocas de las funcionalidades adicionales de los teléfonos celulares. Estas funcionalidades adicionales aumentan drásticamente el valor de la información que contienen estos dispositivos.

Además, en la actualidad los estándares para teléfonos celulares son menores que los que existen para computadoras y al igual que las computadoras, estos dispositivos se han convertido en una necesidad; esto lleva al incremento de su uso en actividades de orden delictivo y ser un portador de datos digitales con potencialidad de ser usado como evidencia.

Cuando un teléfono celular es involucrado en un crimen o en un incidente, los analistas forenses requieren de herramientas que permitan obtener una apropiada y rápida recuperación de la información almacenada en el dispositivo. La información obtenida, después de ser analizada, servirá para redactar un reporte detallado de las actividades realizadas, incluyendo fechas; esto con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó a cabo un delito

o se violó una política. En algunos casos esta información puede obtenerse, aun cuando haya sido borrada [4].

Anualmente el Instituto de Seguridad Informática CSI [4] *(Computer Security Institute)* publica una encuesta llamada "CSI *Computer Crime and Security Survey*" en la cual se realiza un análisis de la situación actual de la seguridad y del crimen digital de las organizaciones participantes, y cuyo objetivo principal es conocer si las mejores prácticas de seguridad digital implantadas producen resultados.

Dicha encuesta arrojó que por la necesidad de movilidad y disponibilidad de la información en las organizaciones, el uso de dispositivos celulares inteligentes dentro de éstas se ha incrementado notablemente, al igual que el número de incidentes.

CSI afirma que cuando un incidente se presenta, es más fácil e importante, para lograr la identificación de los involucrados, monitorear los terminales de comunicación más que la comunicación en sí misma.

En la actualidad existen gran cantidad de proveedores y fabricantes de dispositivos celulares, lo que produce heterogeneidad en todo sentido en el campo forense, especialmente en los procesos y herramientas que se utilizan para obtener evidencia digital de estos dispositivos en una investigación, esto se debe a que los fabricantes crean sus propios estándares.

A diferencia de la informática forense [5], el análisis forense sobre dispositivos móviles, es un campo relativamente nuevo; los procedimientos y normas para su análisis aún se encuentran en desarrollo, y el apoyo judicial que se tiene está relacionado con el análisis forense informático.

---

[4] *CSI (Computer Security Institute)* es una organización educativa de profesionales en seguridad de la información, con más de 30 años de experiencia en la industria, a la vanguardia de las tendencias de la seguridad y la investigación.

[5] *Informática forense* es una rama de las ciencias forenses, que involucra la aplicación de la metodología y la ciencia para identificar, preservar, recuperar, extraer, documentar e interpretar pruebas o evidencias procedentes de fuentes informáticas con el fin de facilitar la reconstrucción de los hechos encontrados en la escena del crimen, para luego usar dichas evidencias como elemento material probatorio en un proceso judicial.

1.1.1 TELEFONÍA CELULAR GSM EN EL MUNDO

GSM de las siglas en inglés *Global System For Mobile Communications* es un estándar mundial para teléfonos celulares, para el acceso emplea una combinación de TDMA[6] y FDMA[7] entre estaciones en un par de canales de radio de frecuencia dúplex; es un sistema diseñado para utilizar señales digitales, así como también, canales de voz y control digitales, lo que permite un moderado nivel de seguridad. Existen cuatro versiones principales, basadas en la banda de frecuencia que utilizan para su operación: GSM-850, GSM-900, GSM-1800 y GSM-1900.

Figura 1.1: Distribución del número de suscriptores en el mundo[8]

[6] *Acceso múltiple por división de tiempo (TDMA, Time Division Multiple Access)* divide el canal de transmisión en particiones de tiempo. Comprime las conversaciones (digitales), y las envía cada una utilizando la señal de radio por un periodo de tiempo. En este caso, distintos usuarios comparten el mismo canal de frecuencia, pero lo utilizan en diferentes intervalos de tiempo.

[7] *Acceso múltiple por división de frecuencia (FDMA, Frequency Division Multiple Access)* separa el espectro en distintos canales de voz, al separar el ancho de banda en pedazos (frecuencias) uniformes. Los usuarios comparten el canal de comunicación, pero cada uno utiliza uno de los diferentes subcanales particionados por la frecuencia.

[8] *Fuente* http://www.3gamericas.org/index.cfm?fuseaction=page&pageid=852 última consulta Septiembre 2010

En GSM, las conexiones se pueden utilizar tanto para el envio y recepción de voz, como de datos. Los casos más comunes son las imágenes que se pueden enviar y recibir, y el uso de aplicaciones a través de teléfonos móviles, tal es el caso de Internet.

Como muestra la Figura 1.1 y 1.2, la tecnología GSM es el estándar de telefonía celular más utilizado alrededor del mundo; según GSMA[9] y la Firma de Industrias Móviles *Wireless Intelligence*[10], en un reporte de Julio del año 2010, anuncia que el número de conexiones móviles globales ha sobrepasado los 5000 millones en el mercado mundial, después de que a finales del 2008 se registró 4000 millones de conexiones.

Wireless Intelligence predice que a mitad del año 2012 el número de conexiones llegarán a 6000 millones; a la vez esta misma compañía afirma que la proporción de penetración de móviles sobre la base global de 5000 millones de conexiones era del 74% comparado con el 60% en los 4000 millones de conexiones anteriores.

Para América, se tiene que el estándar GSM ocupa el primer lugar, como muestra la Figura 1.3 tomada de la fuente 3G Américas[11]

La habilidad de enviar y recibir mensajes (SMS, *Short Message Service*) ha transformado a los celulares en un centro de mensajes. Según *Mobile Data*

[9] *GSMA* (*Association GSM*) representa los intereses de la industria mundial de comunicaciones móviles, abarca 219 países, une a casi 800 operadores de telefonía móvil del mundo, así como más de 200 empresas, incluyendo fabricantes de teléfonos, compañías de *software*, proveedores de equipos, empresas de Internet, medios de comunicación y organizaciones de entretenimiento.

[10] *Wireless Intelligence* es la base de datos global de información sobre el mercado móvil, esta base de datos posee información de los más de 5 millones de puntos de datos individuales en 940 operadores (a través de 2.200 redes) además abarca operadores de redes móviles en todo el mundo a través de varias tecnologías celulares.

[11] *3G Americas* fundada en enero de 2002, reúne a operadores y fabricantes de telefonía móvil de las Américas para brindar una única voz que represente a la familia de tecnologías inalámbricas GSM - GSM, EDGE (*Enhanced Data rates for GSM of Evolution*), HSPA *(High-Speed Packet Access*) y LTE (*Long Term Evolution*). Ha suscrito acuerdos de trabajo en colaboración con la *GSM Association*, el *UMTS Forum*, la Alianza de Redes Móviles de Próxima Generación (NGMN), el Centro de Investigación de las Telecomunicaciones (CINTEL) en Colombia, la Cámara de Empresas de Servicios de Telecomunicaciones (CASETEL) en Venezuela y la Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA) entre otras.

Association[12] en junio del año 2010 en Reino Unido se enviaron 11 millones de mensajes de texto por hora, así como, el promedio de MMS (*Multimedia Messaging System*) a final del 2009 es de 601 millones.

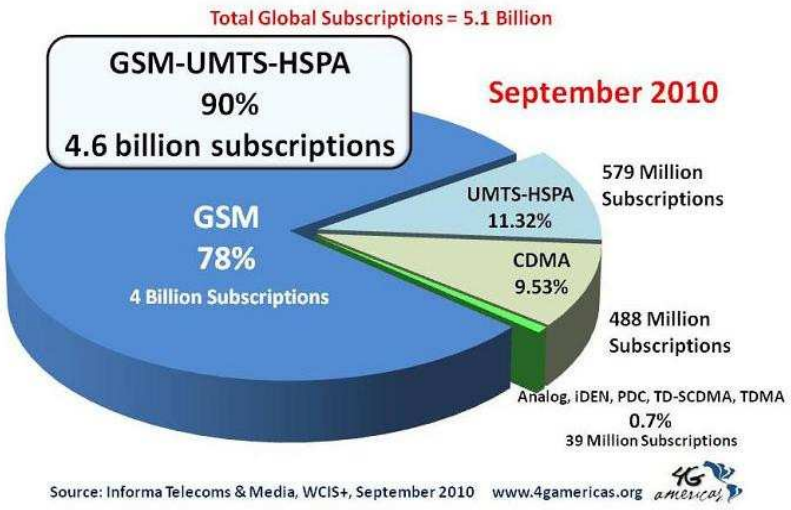


Figura 1.2: Comparación de la tecnología GSM con las tecnologías UMTS, HSPA, CDMA, entre otras tecnologías celulares en el mundo[13]

Al incluir la aplicación de *e-mail* y poder estar conectados a Internet, se agregó conveniencia en las personas y poder en las comunicaciones. Incluir el *e-mail* significó a los usuarios poder recibir notificaciones de mensajes instantáneos y la capacidad de poder descargarlos donde estén.

Cuando llega un nuevo correo, éste es transferido de forma inmediata por el servidor de correo al cliente de correo, en este caso el teléfono celular. Esto hizo al teléfono celular un dispositivo de almacenamiento y transferencia de correo electrónico muy versátil y atractivo en el mercado.

[12] *Mobile Data Association (MDA)* es una asociación sin fines de lucro dedicada a representar y promover todos los datos de las empresas móviles. Los miembros incluyen: operadores de redes móviles, desarrolladores de contenido móvil, fabricantes de teléfonos móviles, y desarrolladores de aplicaciones, contenidos, servicios de entretenimiento y *marketing* móvil.

[13] *Fuente* http://www.3gamericas.org/index.cfm?fuseaction=page&pageid=851 última consulta Septiembre 2010.

En lo que respecta a teléfonos celulares inteligentes que están ganando posicionamiento en los mercados internacionales, *Canalys*[14] realiza anualmente una investigación acerca del estado del mercado de los dispositivos móviles inteligentes y afirman que los 2 últimos años han presentado el mayor crecimiento, el uso de estos dispositivos en comparación con los años anteriores.

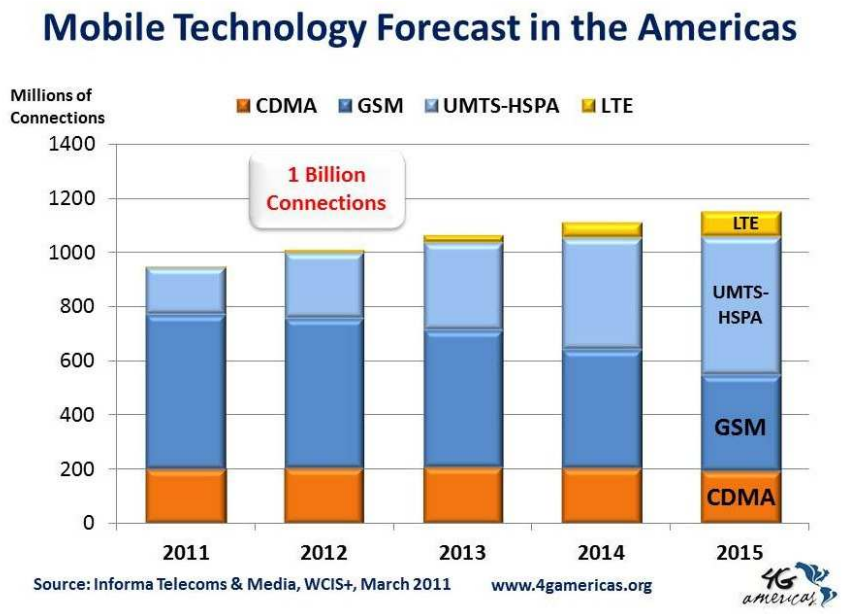


Figura 1.3: Proyección del número de abonados por tecnologías inalámbricas para el período 2011-2015[15]

De los resultados obtenidos cabe rescatar que *Apple* se introdujo en el mercado en tercer lugar con el dispositivo móvil *iPhone*, esto gracias a la innovación en cuanto a diseño e interfaz de usuario que soporta.

1.1.2 TELEFONÍA CELULAR GSM EN EL ECUADOR

En los últimos años el crecimiento del sector de las telecomunicaciones representado por la telefonía celular en Ecuador, ha tenido un importante desarrollo debido principalmente al crecimiento del número de usuarios, lo que a

[14] *Canalys* se especializa en la entrega de datos de alta calidad, análisis y asesoramiento a líderes del mundo en tecnología. Es reconocido como un proveedor clave de servicios de asesoramiento continuo y proyectos confidenciales personalizados para directores de *marketing* en telecomunicaciones, navegación y compañías de electrónica de consumo.

[15] *Fuente* http://www.4gamericas.org/index.cfm?fuseaction=page&pageid=1789 última consulta Marzo 2011.

su vez determina la demanda de nuevos y mejores servicios como consecuencia del actual estilo de vida de la sociedad contemporánea.

De esta manera la relación oferta-demanda en el mercado de las telecomunicaciones, ha impulsado su desarrollo y crecimiento de forma tal, que se ha consolidado como una de las principales actividades económicas del país, en relación a otros servicios de comunicación como la Telefonía Fija e Internet. Esto se puede apreciar en la Figura 1.4.

En Ecuador la tecnología GSM está siendo utilizada mayoritariamente por las empresas celulares que operan en el país, abarcando con su cobertura a un importante número de usuarios a nivel nacional.

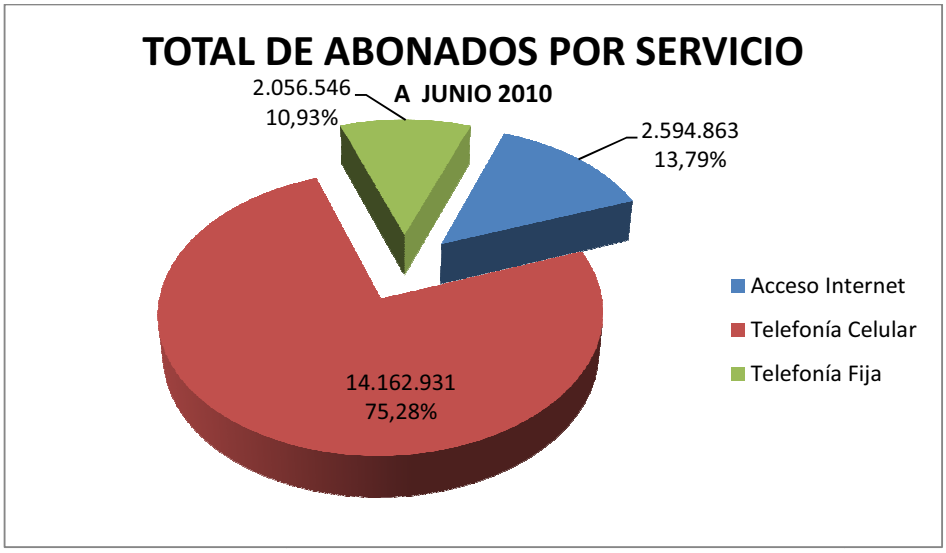


Figura 1.4: Total de abonados de Telefonía Fija, Móvil e Internet en el Ecuador

La Figura 1.5 muestra el incremento de suscriptores en los 10 últimos años en las operadoras celulares presentes en Ecuador.

Las Figuras 1.6 a 1.8 muestran el número de abonados GSM comparándolo con las otras tecnologías y el total de abonados.

Con esto queda demostrado que la telefonía celular en Ecuador está representada por el estándar GSM, el cual es utilizado mayoritariamente por la población ecuatoriana.

Según la Revista Líderes, Ecuador es uno de los países que más abonados tiene en telefonía móvil a escala mundial. En concreto, posee 12 millones 946 mil usuarios de los 14'306.876 de ecuatorianos. De ellos, 212.842 usuarios tienen contratado el servicio de *e-mail* para sus teléfonos celulares [2].

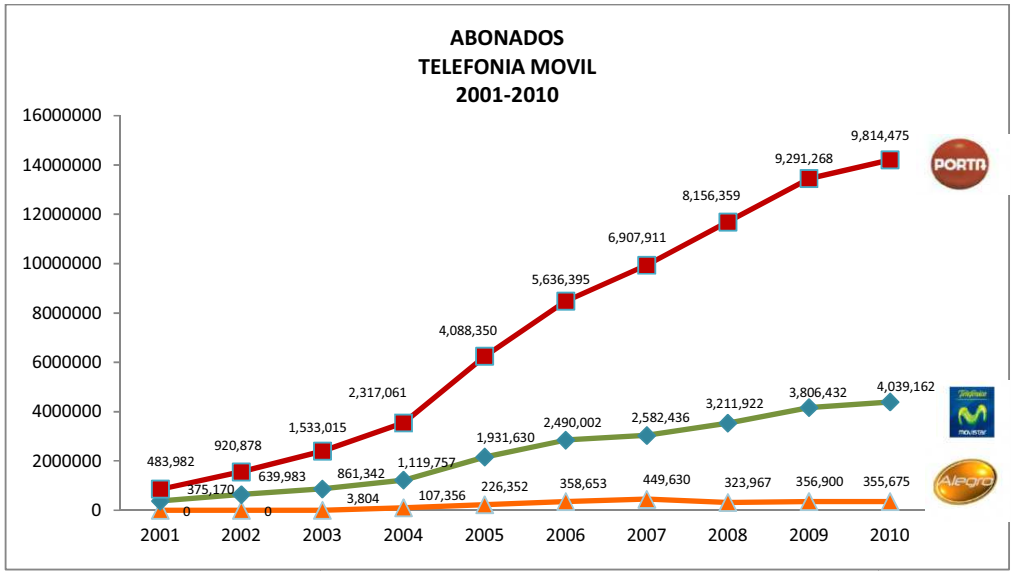


Figura 1.5: Crecimiento de los Abonados de Telefonía Celular por operadora

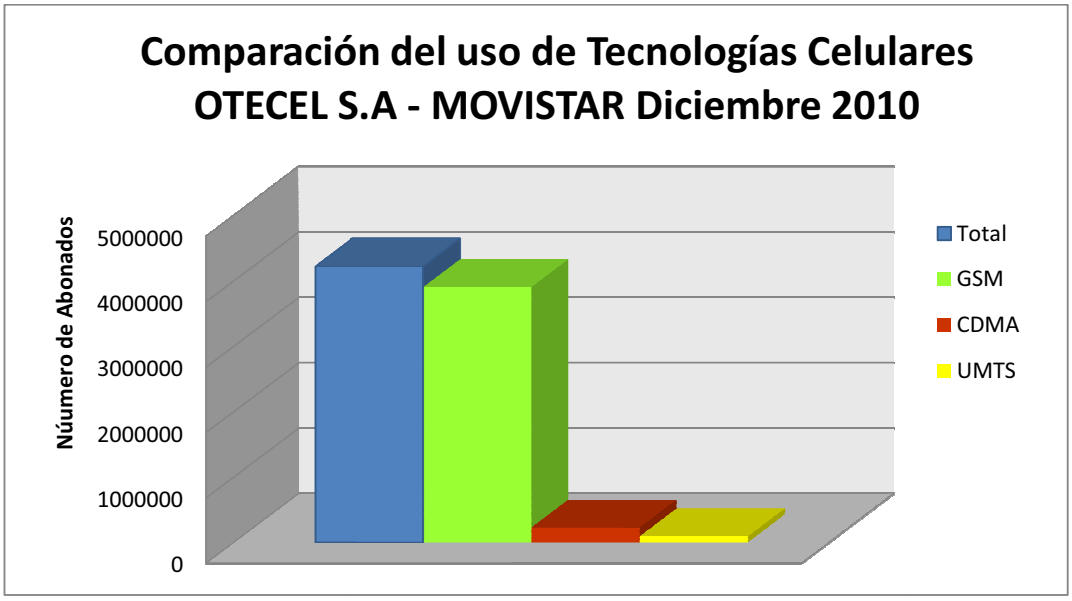


Figura 1.6: Número de Abonados de GSM comparados con el total de abonados y las otras tecnologías existentes en Otecel S.A – Movistar

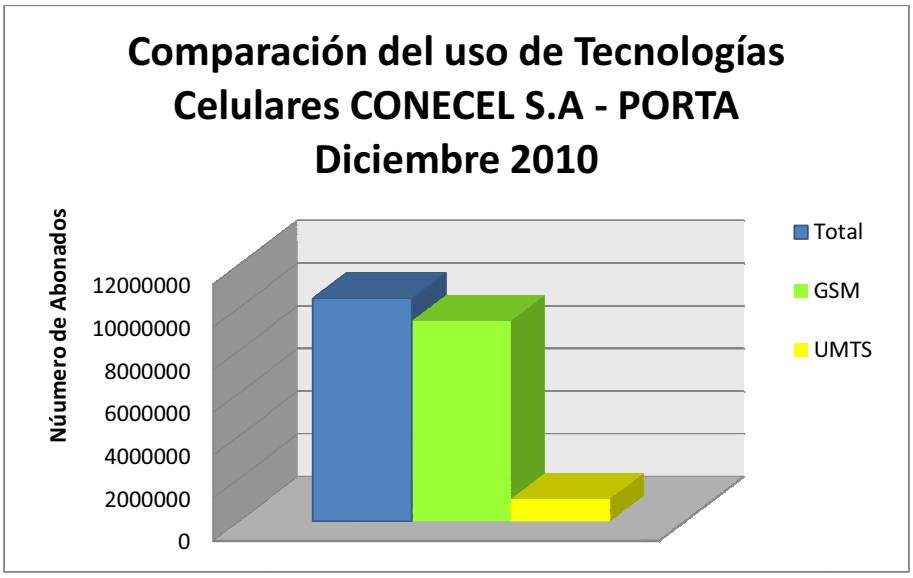


Figura 1.7: Número de Abonados de GSM comparados con el total de abonados y las otras tecnologías existentes en Conecel S.A - Porta

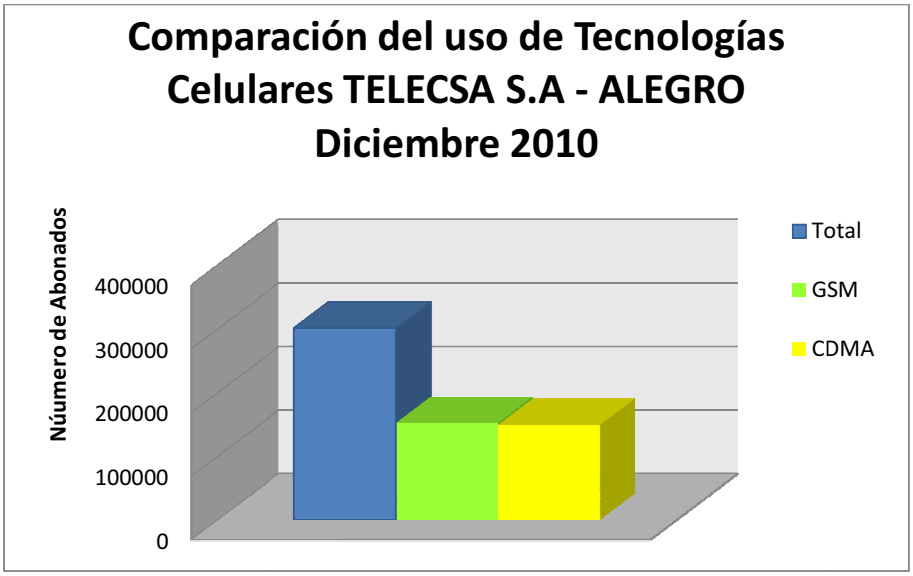


Figura 1.8: Número de Abonados de GSM comparados con el total de abonados y las otras tecnologías existentes en Telecsa S.A – Alegro

Por eso, quienes se conectan a través de un dispositivo móvil a la red representan el 38.68% del total de la población conectada en Ecuador. Estos usuarios necesitan tecnología de punta en cuanto a teléfonos inteligentes [2].

Por eso Movistar, que tiene el mayor número de abonados con servicio de *e-mail* y aplicaciones de redes sociales (112.303 usuarios), tiene como modelos más vendidos el *BlackBerry Bold* 9700 y el 8520. El primero, un teléfono que dejó atrás el molesto *scroll* para convertirse en un teléfono táctil, que brinda posibilidades de conectarse a Internet en lugares donde hay *WiFi*[16] sin necesidad de contratar un plan [2].

El crecimiento de usuarios con acceso a Internet a través de los teléfonos celulares también es muy alto. Solo en el año 2009 se registró un incremento del 22%, algo excepcional si se considera que el 40% de la población que se conecta dice que lo hace con propósitos educativos y de aprendizaje [2].

1.2 EVIDENCIA DIGITAL

Los elementos de prueba o evidencias dentro de un proceso judicial son de vital importancia, ya que mediante su investigación se puede llegar a determinar la confirmación o desvirtuación de una hipótesis o afirmación precedente de lo que corresponde a la verdad.

De esta manera, se podrá confirmar la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables; todo esto servirá para que las personas responsables alcancen el conocimiento necesario y resuelvan el asunto sometido a su criterio.

Por lo tanto, es trascendental, tener en consideración la formalidad y claridad de los procedimientos y/o técnicas de análisis utilizadas en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, frente a un hecho delictivo.

1.2.1 DEFINICIÓN DE EVIDENCIA DIGITAL

De acuerdo a la conceptualización de Eoghan Casey [4], “la evidencia digital es un tipo de evidencia física, que está construida de campos magnéticos y pulsos

[16] *WIFI (Wireless Fidelity)* es una tecnología utilizada en redes inalámbricas de área local WLAN (*Wireless Local Area Network*) para crear un entorno de red de computadoras o terminales situados a pocos cientos de metros, normalizado por el estándar *IEEE* 802.11

electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales".

Miguel López Delgado [5], define la evidencia digital como el conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencia a estos metadatos[17] que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado.

Para el Grupo de Trabajo Científico de Evidencia Digital [6] (SWGDE, *Scientific Working Group on Digital Evidence*), la evidencia digital es la información de probable valor, que es adquirida o transmitida en forma binaria.

Según Jeimy J. Cano M. [7], la evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso.

La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: es volátil, anónima, duplicable, alterable, modificable y eliminable.

Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de análisis forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia existente en una escena del delito.

Además, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado en relación a: su debido registro, valor probatorio, preservación transformación, recuperación y que sea admisible.

Con estos argumentos, la evidencia digital, es una herramienta de especial cuidado, para el proceso de investigación de delitos tecnológicos, debe ser tratada por parte de especialistas que conserven todas las medidas de precaución necesarias para no contaminarla y/o alterarla, para que ésta no sea objeto de desestimación ante un proceso legal.

[17] *Metadatos,* se refiere a datos que se refieren a otros datos o a un grupo de datos llamado recurso, lo que permite ver elementos del sistema de archivos que no se muestran habitualmente como las referencias a directorios o archivos eliminados.

Por consiguiente, la evidencia digital no solo está limitada a lo que es encontrado en las computadoras, también se puede extender a los dispositivos electrónicos tales como MP3, memorias *flash*, *Ipod*, celulares, entre otros aparatos de telecomunicaciones y multimedia. Además, la evidencia digital no está limitada a los tradicionales crímenes computacionales, se la puede extender a todas las clases de crímenes en donde la evidencia digital puede ser encontrada.

Según ZDZIARSKI [8], para que la evidencia digital pueda ser utilizada 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 y veracidad 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 ser 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, qué proceso se siguió en la investigación y cómo la integridad de la evidencia fue preservada, para que ésta sea comprensible y creíble en un proceso judicial.

1.2.2 HISTORIA DE LA EVIDENCIA DIGITAL EN EL ECUADOR

Desde 1999 Ecuador incursiona en la discusión del proyecto de “Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas” y se conforma comisiones para la discusión de la Ley. Se formulan observaciones a la misma, por parte de

los organismos directamente interesados en el tema como el CONATEL[18], Superintendencia de Bancos, Cámaras de Comercio, entre otros sectores y organismos que ven en el Comercio Telemático una gran oportunidad de hacer negocios y ayudar a que nuestro país ingrese en el boom de la llamada ‘’Nueva Economía’’.

Cuando la ley se presentó, en un principio tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal. Las infracciones a la misma, es decir los llamados Delitos Informáticos, se sancionarían de conformidad a lo dispuesto en el Código Penal ecuatoriano, situación que se comprende un tanto forzada, esto si se toma en cuenta los 70 años de dicho Código; en resumen los códigos penales ahí existentes, no tomaban en cuenta los nuevos adelantos de la Informática y la Telemática.

En abril de 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos que es de donde parte el análisis de la llamada evidencia digital.

Increíblemente en la actualidad los delincuentes utilizan la tecnología para facilitar la ejecución de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, Fiscalía y la Función Judicial deban especializarse y capacitarse en estas nuevas áreas en donde las TICs (Tecnologías de la Información y de la Comunicación) se convierten en herramientas necesarias en auxilio de la Justicia y la persecución del delito y el delincuente.

Los hábitos de las personas han cambiado con el uso de las TICs, también las formas en que los delincuentes actúan y comenten sus actos censurables; es así que el acceso universal a las tecnologías de la información y la comunicación,

[18] CONATEL, El Consejo Nacional de Telecomunicaciones es el ente de la administración y regulación de las telecomunicaciones en el Ecuador y de la administración de telecomunicaciones del Ecuador ante la Unión Internacional de Telecomunicaciones (UIT).

brinda nuevas oportunidades para que gente inescrupulosa como delincuentes, pornógrafos infantiles, entre otros, cometan actos delictivos.

Los delincuentes realizan toda clase de ataques contra la intimidad, fraudes telefónicos y cibernéticos, que atacan a la integridad de los sistemas digitales y de la red a nivel mundial; actúan de forma desmedida sin que los operadores de justicia puedan hacer algo, ya que éstos han quedado relegados en sus actuaciones por la falta de recursos tecnológicos, leyes claras y capacitación a fin de lidiar con la evidencia digital presente en toda clase de infracciones.

Las infracciones tecnológicas son unas de las causas de preocupación de los elementos de seguridad de muchos países, dado que las mismas han causado inmensas pérdidas económicas especialmente en el sector comercial y bancario.

Por esta razón es que en países con altos niveles tecnológicos como Estados Unidos, Alemania o Inglaterra se han creado y desarrollado técnicas y herramientas tecnológicas a fin de lograr tanto el descubrimiento de los autores de dichas infracciones así como asegurar la veracidad de estas pruebas.

Para ayudar en esta problemática existe el Análisis Forense, ciencia criminalística que sumada al impulso y utilización masiva de las TICs en todos los ámbitos del quehacer del hombre, está adquiriendo una gran importancia, debido a la globalización de la sociedad de la información.

A pesar de ello esta ciencia no tiene un método estandarizado para todas las ramas de las TICs, razón por la cual su validez, veracidad y admisibilidad dentro de un proceso judicial podría ser cuestionado; pero esto no debe ser un obstáculo para dejar de lado esta ciencia importante, la cual debe ser manejada en base a rígidos principios científicos, normas legales y de procedimiento.

1.3 PROPÓSITO DE LA INVESTIGACIÓN FORENSE CELULAR

El análisis forense aplicado a teléfonos celulares, es un área de investigación relativamente nueva. Es por esto que existe poca documentación sobre el tema, y más aún en lo relacionado con la atención de incidentes o crímenes.

1.3.1 CRÍMENES Y TELÉFONOS MÓVILES

Al alcanzar tanta popularidad los dispositivos móviles en el mercado y por la variedad de funcionalidades que ofrecen, también se han incrementado notablemente los delitos cometidos con éstos y el hecho de encontrarlos en escenas delictivas es más frecuente.

La tecnología no es buena ni mala, solo depende del uso que se le dé; es así que este invento que ha proporcionado grandes satisfacciones, también ha sido de gran utilidad para cometer una gran variedad de delitos, entre los más conocidos están la clonación, la intercepción de mensajes en transacciones bancarias, el secuestro, narcotráfico, la extorsión, el intercambio de imágenes de pedofilia, entre otros.

1.3.1.1 Delitos que involucran teléfonos móviles

Existen diferentes tipos de delitos, que la evidencia digital contenida en un teléfono celular puede ayudar a resolver, pues puede formar parte de la escena del hecho o escena del delito como elemento activo o pasivo y se necesita de un análisis minucioso para que sea validado como evidencia. Entre los delitos más comunes y casos hipotéticos se tiene:

1.3.1.1.1 Asesinatos

a. El asesinato de Knutby se refiere a un asesinato e intento de asesinato en el valle de Knutby al este de Uppsala en Suecia. Un pastor de una congregación pentecostés de esta comunidad fue sentenciado de por vida en prisión, por persuadir a su amante para disparar y matar a su esposa, además, de tratar de matar al esposo de otra de sus amantes. Dos días después del asesinato, la amante del pastor, Sarah S. se declaró culpable. A pesar de su declaración, la policía creía que ella tenía un cómplice. La evidencia más fuerte contra el pastor, era la comunicación extensa a través de mensajes de texto y llamadas de voz entre él y su amante, en el día del asesinato y antes de los hechos ocurridos. Ellos no sabían que aunque borraron cuidadosamente los mensajes, estos mensajes se los podía recuperar [9].

b. Mr. Bristowe dijo en las Noticias de BBC por Internet: “Que era la evidencia del teléfono celular, la que hizo que la policía analice con más detalle a Huntley como sospechoso”. La policía investigó el teléfono de Jessica una de las chicas asesinadas y descubrieron cuando y donde se había apagado; en este momento la red celular dejo de registrarlo en la radio base número 1846, el domingo cuando las muchachas desaparecieron.

   Con esto la policía proporcionó un mapa de la ruta que según ellos pensaron las muchachas habrían tomado, y el único lugar en esa ruta donde el teléfono estaba conectado y luego se desvinculó estaba dentro o justo fuera de la casa de Huntley, se cree que esta evidencia mínima fue crucial para obligar a Huntley para cambiar su historia y de repente admitir que las muchachas murieron en su baño [10].

1.3.1.1.2 Robo

El caso contra Dan Kincaid era difícil de resolver. Un propietario al norte de Boise, Idaho - USA, había identificado al Sr. Kincaid de 44 años, como la persona que había irrumpido en su casa suburbana. Pero el testimonio del testigo ocular no siempre constituye una evidencia sólida, y el Sr. Kincaid estaba negándose a hablar, la policía quiso indagar más, así que ellos investigaron el teléfono celular de marca *BlackBerry* del Sr. Kincaid, este teléfono tenía la funcionalidad de recibir y enviar correos, y así, encontraron toda la evidencia que ellos necesitaban.

Justamente cuando intentaba encontrar un camino para salir de su barrio sin ser capturado, el Sr. Kincaid escribió a su novia, poco después de que él irrumpió en la casa, el mensaje decía: “los perros ladrarán si salgo entre o detrás de las casas…… la policía sabe que yo llevo puesto una camisa azul”, el continuó “yo necesito salir de aquí antes de que ellos me encuentren”. Enfrentado con su admisión del delito, mandada electrónicamente, el Sr. Kincaid acepta un trato con fiscales [11].

1.3.1.1.3 Agresión

Era un supuesto que un muchacho hubiera dirigido un ataque serio en contra de un niño. El muchacho estaba negando todo el conocimiento de la casualidad inicialmente, hasta que la policía fue informada que había evidencia en el teléfono celular; analistas recuperaron fotos en las cuales se demostraba la agresión, siguiendo un método de análisis forense, también recuperaron un mensaje multimedia borrado enviado a otro niño con uno de las fotos que lo comprometían [12].

1.3.1.1.4 Acoso

Un empleado de una gran empresa se acerca a Recursos Humanos debido a que ha recibido mensajes y llamadas telefónicas inapropiadas de un compañero de trabajo. Para confirmar este comportamiento, se autoriza el análisis del teléfono celular *BlackBerry* del supuesto acosador, que había sido emitido por la empresa para fines comerciales entre el empleado y la empresa.

La administración no quería alertar al personal del tema en cuestión, ni que se va a proceder a la investigación. Por lo que se envió un comunicado al jefe de cada grupo explicando que se procederá a realizar actualizaciones de *firmware* a los *BlackBerry* de los empleados. Agentes nombrados por la empresa como personal de apoyo pide a cada usuario que introduzca su PIN[19] para poder realizar una copia de seguridad del dispositivo. El personal explica que la copia de seguridad es necesaria en caso de que la actualización del *firmware* no funcione correctamente.

Todas las copias de seguridad se copian en un recurso compartido de red y el archivo *.IPD archivo propio del sistema operativo de los *BlackBerry* asociado con el sujeto en cuestión se toma para el análisis y se descubre que efectivamente de este celular han sido realizados los mensajes y llamadas telefónicas por lo cual se confirmó el Acoso [13].

---

[19] *PIN*, *Personal Identification Number,* es un código numérico utilizado de seguridad para obtener acceso al teléfono celular, mientras sea habilitado por el usuario.

1.3.1.1.5 Narcotráfico

Un vehículo sospechoso es detenido por exceso de velocidad en una carretera local. El oficial que lo detuvo, se da cuenta que el conductor está actuando de manera extraña cuando se acerca el vehículo. Mientras hablaba con el conductor, se da cuenta que los ojos del hombre miraban una bolsa oculta bajo el asiento del pasajero. El oficial le pide al sospechoso salir del coche, y encuentra que la bolsa contiene una gran cantidad de drogas.

Después del interrogatorio, se cree que el sospechoso estaba simplemente actuando como un mensajero, pero no dice nada a los investigadores. La policía sospecha que está en contacto con el distribuidor, a quien la policía quiere detener. Después de colocar al sospechoso bajo arresto por posesión de drogas, se confisca el teléfono celular y se realiza una copia del mismo para determinar quién es el contacto y cuándo el conductor iba a su encuentro [11].

1.3.1.1.6 Extorsión telefónica

El tema de que los teléfonos celulares sean utilizados para la extorsión se ha incrementado por la facilidad con la que se puede adquirir el mismo, sin necesidad de que el usuario proporcione datos de identificación personal.

Cada vez que una persona mal intencionada tenga acceso a un teléfono celular que no necesariamente le pertenezca, puede utilizar la información encontrada para hacer una extorsión telefónica. La forma más común de operar de los extorsionadores telefónicos se basa en hacer llamadas al azar con los contactos telefónicos encontrados, si la llamada es contestada, el extorsionador exige grandes cantidades de dinero a cambio de la libertad de un familiar presuntamente secuestrado.

En este tipo de casos un analista forense, utilizando las herramientas correctas, podría obtener las últimas llamadas realizadas y contestadas, los últimos mensajes de texto y/o multimedia enviados y recibidos, correos electrónicos e incluso información personal, sin olvidar los archivos de imágenes que podrían ayudar a describir acciones delictivas.

El analista, al encontrar todos los eventos registrados en el dispositivo móvil, tendrá elementos suficientes para asegurar que se ha realizado un acto delictivo y culpar o exonerar al dueño del dispositivo [1].

1.3.1.1.7 Fraude en Telefonía Celular

Se entiende por fraude la acción contraria a la verdad y a la rectitud, que perjudica a la persona o a la institución contra quien se comete. Acto cumplido intencionalmente tendiendo a eludir, herir o menoscabar disposiciones legales o derechos del Estado o de terceros con el fin de obtener un beneficio.

Las telecomunicaciones al ser una base tecnológica que recorre transversalmente cualquier actividad humana, no están exentas de que a través suyo se cometan diversos fraudes. Esto afecta a todos los prestadores de servicios de telecomunicaciones y, potencialmente, a todos los usuarios. Por ende, es importante que esta temática sea tratada de manera integral por los diferentes actores del sector. [14]

El desarrollo de la Telefonía Móvil y la amplia variedad de nuevos servicios que se incorporan utilizando esas redes, han hecho que los ejecutores del fraude procuren sacar provecho económico de dichos servicios.

La Telefonía Móvil con su característica intrínseca de ubicuidad y con la modalidad del sistema prepago, resulta propicia para su uso en actividades ilícitas que se combinan con actividades de fraude. [15]

Una definición apropiada para fraude en este campo, es “el uso ilícito de acceso a la red de telefonía celular para obtener provecho o lucro”.

El fraude de la Telefonía es un fenómeno mundial. Estimaciones corrientes contabilizan pérdidas de USD 15 a 55 mil millones por año (1% a 5%) en la industria de telefonía, que mueve negocios en valores cercanos a los USD 1,5 billones [16].

Se considera que los tipos de fraude relacionados a las redes de telefonía celular son:

a. Fraude de abonado: Ocurre cuando alguien se suscribe a un servicio usando identificación falsa o información personal obtenida de manera fraudulenta. Los infractores obtienen su información personal y la usan para abrir una cuenta de teléfono celular a su nombre. A menudo se realizan consumos elevados por períodos cortos de tiempo y luego se deja de usar el servicio [17].

b. Clonación de tarjetas SIM: El módulo de identificación de abonado (SIM, *Subscriber Identity Module*) personaliza un terminal móvil GSM, el cual es totalmente genérico hasta el momento en que se inserta el SIM.

   La clonación de la tarjeta SIM ha llegado a ser una nueva forma de robo de identidad, permitiendo que sea robada a través del teléfono. En teléfonos GSM, la tarjeta SIM insertada en el teléfono mantiene asociados todos los datos del usuario con la red.

c. *Bypass*: De los tipos de fraude existentes, el que más perjuicio origina a las operadoras de telefonía y al Estado ecuatoriano, lo constituye el "*By pass*", que en los últimos años ha causado pérdidas millonarias a nuestro país.

   De forma resumida se puede decir que el "*By pass*" encamina directamente el tráfico que viene del exterior hacia las centrales locales, sin pasar por la central de tráfico internacional, es decir, se evita la tarifación de la llamada internacional, y se la convierte en una llamada local .

   El tráfico de llamadas entrantes es aproximadamente 8 veces mayor que el de las llamadas salientes y en este mismo sentido se comete el ilícito del "*By pass*".

   El "*By pass*" se muestra como una ruta alternativa para los *carriers* internacionales, presentando un costo sumamente menor que el exigido

por las compañías telefónicas locales; por este motivo deciden ingresar sus volúmenes de tráfico mediante esta vía alternativa; o, fomentar la implementación de sistemas de "*By pass*" para ingresar su tráfico a un menor costo.

Previamente, se debió equipar el local clandestino con numerosas líneas telefónicas, dependiendo del tamaño del "*By pass*". Estas líneas son conseguidas a través de cómplices en la misma empresa telefónica o con documentación falsa, adulterada o robada.

Una vez que todo el volumen de tráfico ha ingresado al local clandestino, equipos de telecomunicaciones procesan la información como una mini central telefónica; las llamadas procesadas por la mini central telefónica generan llamadas locales hacia los abonados finales en el Ecuador, completando así la llamada que se generó desde cualquier parte del mundo.

Las empresas telefónicas locales sólo perciben una llamada local, mientras la porción internacional la cobra la empresa que comete el fraude.

SIM BOX es un tipo de fraude que afecta específicamente al Sistema Celular; se define como el uso de equipos especiales que permiten la utilización simultánea de un banco de tarjetas SIM para tráfico internacional. Las tarjetas SIM son obtenidas mediante fraudes de suscripción, para importar o exportar tráfico internacional, típico fraude de "*Bypass*", la diferencia es el uso de las redes celulares. [14]

1.3.1.2 El Esfuerzo de la Ley involucrado

Por diversos que sean los dispositivos móviles, tecnológicamente se puede encontrar un camino que permita encontrar evidencia digital en ellos; pero esta diversidad acarrea consigo una desventaja al momento de crear leyes nacionales e internacionales que puedan aplicarse en cualquier país en contra de quien está haciendo mal uso del teléfono móvil.

La velocidad con la que cambia la tecnología en los dispositivos móviles es mayor comparada con la velocidad en que cambian las leyes de un país, pudiendo significar un problema si se considera que un intruso puede diseñar una estrategia de ataque, usando un dispositivo móvil desde un país donde no existan leyes que consideren la evidencia digital para ayudar a la investigación de delitos.

La brecha entre la ley y el crimen organizado sigue siendo considerable en lo que respecta a la utilización de tecnologías de Telefonía Móvil. Los teléfonos móviles se usaron en la década de los 80's por las organizaciones criminales como un instrumento para evadir la captura, así como un medio para facilitar las operaciones cotidianas.

Irónicamente, tomó décadas para convencer a las empresas legítimas que la conectividad móvil podía mejorar sus ingresos, y casi todas las personas que participan en cualquier nivel de la delincuencia ya conocían en la misma década que los teléfonos móviles pueden proporcionar un retorno de la inversión.

Por otra parte, las leyes disponibles para informática forense no pueden hacer frente en varios aspectos a la evidencia digital obtenida de los dispositivos móviles, esto se debe en parte a algunas de las siguientes razones.

a. El aspecto de la movilidad del dispositivo, requiere interfaces y *hardware* especializados, así como, medios de almacenamiento particulares.

b. El sistema de archivos reside en la memoria volátil en comparación con los equipos informáticos que residen en las unidades de disco duro.

c. La gran diversidad de sistemas operativos integrados en los dispositivos móviles.

d. El que el teléfono móvil siempre se encuentre recibiendo señales, a pesar de que se encuentre en estado inactivo o de ocio.

e. Los ciclos de producción cortos para nuevos dispositivos móviles.

Estas diferencias son algunas de las razones por lo que es importante distinguir entre el análisis forense celular y la llamada informática forense o análisis forense de sistemas informáticos.

1.3.2 DIFERENCIAS ENTRE ANÁLISIS FORENSE DE TELÉFONOS MÓVILES Y ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS

Las ciencias forenses son disciplinas que estudian la utilización de procedimientos y conocimientos científicos para adquirir, preservar, analizar y presentar las evidencias apropiadamente.

Las ciencias forenses son combinación del conocimiento científico, diferentes técnicas de análisis, y que conjuntamente con el marco regulatorio ayudan a demostrar con la evidencia recuperada la existencia del delito y sus posibles responsables.

Posteriormente con el avance de la ciencia y la tecnología, las ciencias forenses han alcanzado un desarrollo inconmensurable, pero ese desarrollo a veces no ha ido de la mano del avance de la legislación penal. Esto en razón del retraso en la incorporación de nuevos elementos de prueba y medios probatorios y sobre todo en la demora de la admisibilidad de nuevas evidencias o pruebas.

De lo anterior se puede decir que el análisis forense de teléfonos móviles es “la ciencia forense que se encarga de la identificación, preservación, evaluación, extracción y filtrado de la evidencia digital, para luego ser presentada”.

El análisis forense se basa en realizar etapas planificadas para recabar pruebas y analizarlas. Las herramientas tecnológicas utilizadas para la identificación, extracción e interpretación de la evidencia, cumplen un papel importante al momento de colectar y analizar la información y los elementos de convicción necesarios.

Las causas que explican por qué un análisis de teléfonos móviles es diferente al análisis de sistemas informáticos son:

a. La variedad de fabricantes y modelos de teléfonos que existen el mercado de telefonía móvil.

b. La heterogeneidad que se presenta tanto en la configuración de *hardware*, sistema operativo, forma de acceso y tipo de aplicaciones que manejan los teléfonos móviles.

c. La información volátil y dinámica que poseen los teléfonos móviles en lo que es información de localización e información personal.

d. En la mayoría de los casos, los fabricantes de teléfonos móviles optan por crear y aplicar sus propios protocolos e interfaces para uso de sus sistemas operativos, ocasionando que para los analistas forenses sea más difícil realizar una investigación.

e. Las herramientas que se disponen en el mercado, que se pueden utilizar para recuperar contenido son variadas, y se tiene modelos y marcas de teléfonos móviles que muchas veces no son compatibles con todas las herramientas.

f. Existe poca literatura sobre el análisis forense de teléfonos móviles y especialmente de teléfonos móviles inteligentes. Sin embargo, se han desarrollado herramientas y algunas técnicas forenses para llevar a cabo dicho proceso.

g. A diferencia de los computadores, la mayoría de teléfonos móviles no tienen discos duros, y generalmente guardan los datos en la memoria volátil los cuales se pueden perder si no hay el adecuado suministro de energía.

h. Eventualmente si el dispositivo aparece como en estado inactivo o de ocio por la característica intrínseca de movilidad, para reservar energía, puede estar sucediendo un proceso detrás de este estado, lo cual puede dar como resultado la pérdida de datos.

Es por esto, que para lograr un análisis forense confiable, y que la evidencia que se recoja logre ser admisible, auténtica, completa, fiable, entendible y creíble, es importante seguir lineamientos y un sistema transparente.

1.4 FUTURAS AMENAZAS

La actual evolución tecnológica de dispositivos móviles, hace que existan nuevas funcionalidades que los asemejan cada vez más a una computadora, del tamaño de un teléfono móvil.

Estos dispositivos presentan la capacidad de funcionar como una cámara digital que obtiene imágenes y video de alta calidad, un reproductor de música con capacidad de almacenar canciones, una agenda personal con capacidad de conectarse a Internet, de forma inalámbrica, para consultar correo electrónico o cualquier sitio *Web*, un sistema de posicionamiento global que ayude a localizar la ubicación física de quien porta el dispositivo, así como la ruta más corta para llegar a un destino.

Finalmente, un teléfono puede llevarse a casi cualquier parte del mundo, con la confianza de que el dispositivo hará lo necesario para realizar una llamada o video llamada, todo esto en un mismo dispositivo de tamaño atractivo.

Para que los nuevos dispositivos móviles puedan ser aprovechados al máximo, la mayoría de los proveedores de servicios de Internet y Telefonía están instalando y ajustando su infraestructura para que el intercambio de información sea más rápido y accesible en casi cualquier parte del mundo.

Con estos avances en la tecnología, los analistas forenses predicen que a corto plazo, los vectores de ataques estarán enfocados a apoderarse de los dispositivos móviles conectados a Internet.

Los intrusos aprovecharán el ancho de banda para infectar a los dispositivos móviles con algún virus o gusano. Una vez infectados, los intrusos podrían programar instrucciones que reporten las actividades de las víctimas, para lo cual recibirán imágenes o videos en tiempo real que detallen el lugar donde se

encuentre las víctimas, las personas que lo acompañan, la forma como viste la víctima e incluso quienes la rodean.

El intruso estará recibiendo de forma automatizada una serie de imágenes y videos en un servidor central, desde el cual podrá enviar órdenes para aumentar o disminuir la frecuencia a la que el dispositivo móvil mandará archivos multimedia. En el ataque también pueden incluirse conversaciones privadas obtenidas gracias al dispositivo móvil, que la víctima porte en la bolsa del pantalón, en la camisa o atado a la cintura.

Esta nueva forma de espionaje puede ser nombrada como "*Botphones*", haciendo alusión al término "*bot*", utilizado para nombrar un equipo de cómputo comprometido que puede ser controlado remotamente tanto de forma centralizada como descentralizada.

Siguiendo la misma línea de los "*Botphones*", otro vector de ataque puede estar basado en las conexiones de salida que realiza un dispositivo móvil. Con esto se puede pensar en una negación de servicio provocado por miles de dispositivos móviles comprometidos, que intenten hacer conexiones a un servidor al mismo tiempo, hasta lograr impactar la disponibilidad de un servicio.

Éste y otros ataques forman parte de los problemas que se sufrirá como sociedad. Mientras no existan leyes que respalden a las víctimas, se tendrá que ir inventando nuevas formas para evitar caer en manos de los intrusos y no hacer de la tecnología un instrumento que los intrusos usen para beneficiarse.

Los avances tecnológicos permiten que los dispositivos móviles soporten memorias externas, mientras que su tamaño es cada vez más pequeño, lo cual hace atractivo para que este dispositivo sea utilizado o esté presente en actos delictivos de cualquier clase.

El futuro de teléfonos móviles y sus componentes pueden ser resumidos en la velocidad del procesador y su composición, tipo de baterías y las tecnologías aplicables, y finalmente la capacidad de memoria y almacenamiento.

Todos estos componentes y su desarrollo tienen un impacto sobre el análisis forense celular, los mismos que se detallan a continuación:

a. Velocidad y Composición del Procesador: Intel ya ha demostrado el tener un procesador de 1 GHz para dispositivos móviles. Además de la velocidad de procesamiento, los teléfonos móviles inteligentes están tendiendo a usar una tecnología llamada sistema sobre chip, que permitiría al procesador incorporar un conjunto de diferentes funcionalidades en el mismo paquete, reduciendo el número de chips adicionales requeridos, incorporando así al dispositivo más capacidad de memoria.

b. Tipos de Baterías: Los teléfonos móviles típicamente usan tres tipos de baterías: NiMH (níquel-hidruro metálico), Li-ion (ion de litio), and *Lipolymer* (ion polímero de litio).

   Toshiba anunció que lanzará al mercado una tecnología de baterías de *lithiumnion* que permitirá a las baterías recargarse seis veces más rápido que cualquier otra batería convencional, lo cual significa que tomará alrededor de un minuto para obtener el 80% de la carga.

   Tecnologías inalámbricas tales como *WiFi, WiMax* [20] , y *Bluetooth* [21] descargan la batería muy rápidamente, esto representa un reto para los fabricantes de baterías mientras estas tecnologías están siendo incorporadas a los teléfonos inteligentes.

c. Capacidad de memoria y almacenamiento: Los sistemas operativos de los teléfonos móviles son pequeños en comparación con una computadora, por consiguiente, tiene más sentido almacenar el sistema operativo en la memoria RAM, ROM o Flash.

[20] *WIMAX (Worldwide Interoperability for Microwave Access)* es un grupo de la industria que se formó para promover el estándar IEEE 802.16, es una tecnología dentro de las llamadas tecnologías de última milla con un alcance de 40 a 50 km (fijo) y 5 km (para estaciones móviles)

[21] *BLUETOOTH* es una de las redes inalámbricas de área personal WPAN (*Wireless Personal Area Network*) más conocidas, no está pensada para soportar redes de computadoras, sino para comunicar un computador o cualquier otro dispositivo con sus periféricos; está normado por el estándar *IEEE* 802.15.1.

Los teléfonos actuales tienen de 64 a 128 MB de memoria RAM estática para el código de aplicación, 128 a 256 MB de memoria flash para el código del sistema y más de 128 MB de memoria flash para datos del usuario. El aumentar la capacidad a las memorias debe estar acompañado de aumento en la velocidad de acceso a los datos por lo tanto esto también mejorará.

CAPÍTULO II

CAPÍTULO 2

2. TÉCNICAS DE EXTRACCIÓN DE LA INFORMACIÓN

En este capítulo, se revisarán los elementos del Sistema Celular GSM que pueden ser evidencia, con el objetivo de entender su funcionamiento, y así discriminar qué evidencia es relevante para la investigación judicial; se enfocará en el teléfono móvil como fuente principal de evidencia. Se establecerá qué evidencia digital potencial puede ser proporcionada por este medio, por lo que se analizará la información que proporciona tanto el Equipo Móvil como la tarjeta SIM.

Así mismo se investigan y analizan cuatro técnicas de extracción de evidencia digital de un teléfono móvil, las cuales son: Extracción manual, Extracción lógica, *Hex-Dump* y *Chip off*.

Estas técnicas han sido propuestas por organismos y personas especializadas en el tema; al mismo tiempo, se analiza cómo proteger esta evidencia digital para que luego sea validada y utilizada en el campo judicial.

2.1 EVIDENCIA DIGITAL EN LA ARQUITECTURA GSM

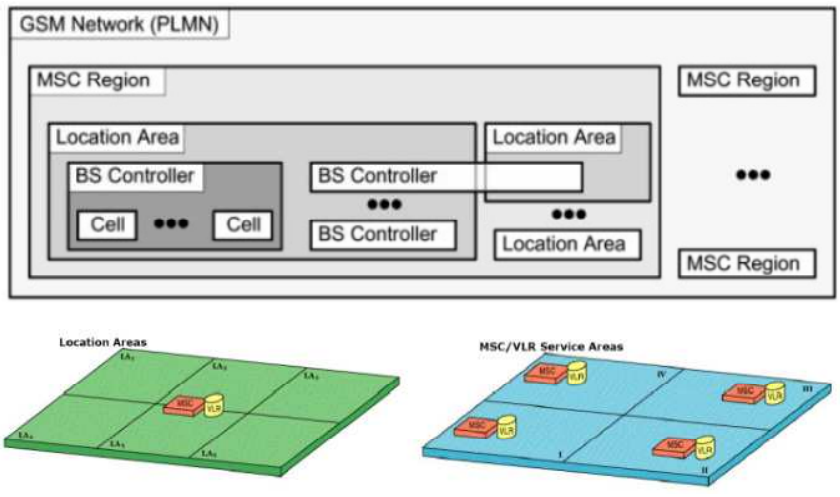


Figura 2.1: Zonas o Regiones GSM[22]

[22] Figura tomada de Diapositivas de Comunicaciones Inalámbricas, Ing Soraya Sinche, 2010

Todos los elementos dentro de la arquitectura GSM no necesariamente constituyen evidencia digital potencial ó relevante para una investigación judicial, por lo cual hay que realizar una discriminación.

Se debe recordar que el sistema GSM agrupa sus elementos en diferentes zonas o regiones, tales zonas se muestran en la Figura 2.1 y sus componentes se observan en la Figura 2.2

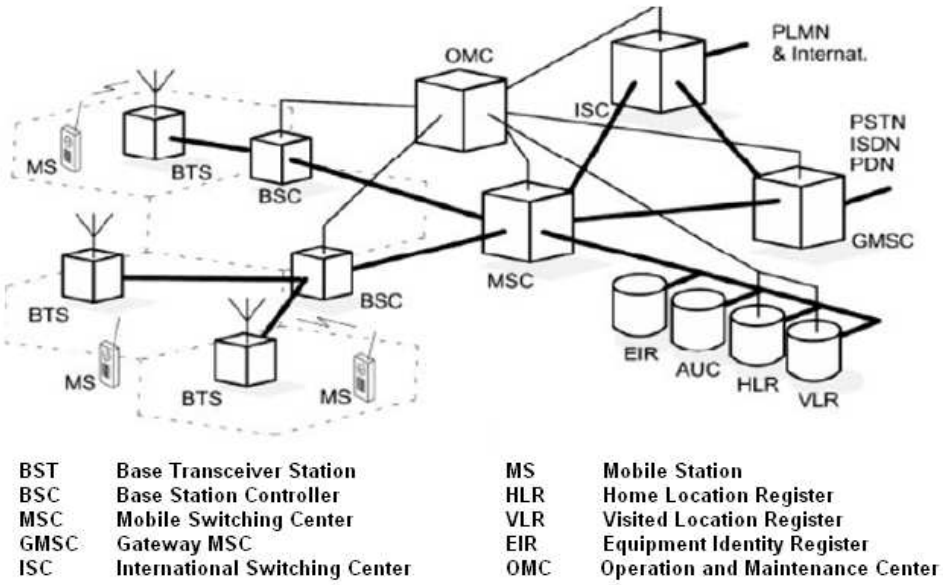


Figura 2.2: Arquitectura GSM[23]

Con el objetivo, de entender de forma general el funcionamiento de los elementos que constituyen la Arquitectura GSM y así clasificar la información que puede ser evidencia potencial, se revisará sus elementos constitutivos agrupados en la Infraestructura Instalada Fija y la Estación Móvil.

2.1.1 INFRAESTRUCTURA INSTALADA FIJA

Su parte fija puede ser dividida en tres subredes que cumplen funciones propias y que a su vez interactúan entre sí con el propósito de ofrecer a los usuarios todos los servicios de telefonía móvil que requieren; los elementos de estos Subsistemas están conectados entre sí a través de interfaces estandarizadas como lo muestra la Figura 2.3

[23] Figura tomada de Diapositivas de Comunicaciones Inalámbricas, Ing Soraya Sinche, 2010

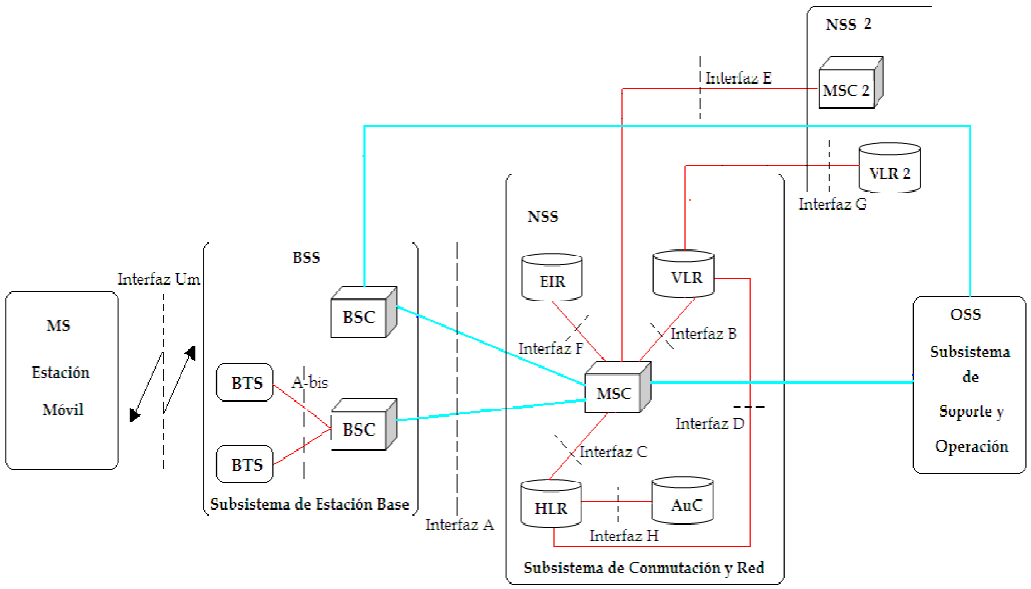


Figura 2.3: Interfaces y Subsistemas Estandarizadas de la arquitectura GSM[24]

Estos subsistemas son:

- Subsistema de estación base (BSS, *Base Station Subsystem*)
- Subsistema de Conmutación y Administración (NSS, *Network Switching Subsystem*)
- Subsistemas de Mantenimiento y Operación (OSS, *Operations and Maintenance Subsystem*)

Dentro de estos subsistemas existen elementos que son de interés para una investigación judicial; se puede afirmar que todos los elementos relacionados con registros detallados de llamadas de sus siglas en inglés CDR (*Call Detail Records*) son elementos de interés.

A continuación se citan los elementos de la Arquitectura GSM, los cuales están involucrados en la generación de CDRs:

[24] Figura tomada del Proyecto de Titulación, Estudio y Análisis del Comportamiento de RF en espacios edificados, In-Building, DITZEL, Sergio, Universidad Austral de Chile, 2008

2.1.1.1 *Mobile Switching Center* (MSC)

El Centro de Conmutación Móvil, es el elemento central de una red de telecomunicaciones móviles, la cual es llamada PLMN (*Public Land Mobile Network*) en los estándares.

Todas las conexiones entre los suscriptores son administradas y enrutadas por el MSC sobre la matriz de conmutación, mientras dos suscriptores tengan establecida una conexión de comunicación.

MSC coordina las actividades del BSS y conecta todo el sistema celular a otras redes como la PSTN[25] *(Public Switched Telephone Network).*

Es la encargada del ajuste de potencia transmitida por las Estaciones Móviles; además interviene en el proceso de *handoff* o *handover*[26]. En grandes ciudades un solo *carrier* puede utilizar varias MSC.

Las actividades de administración para establecer y mantener una conexión son parte del protocolo de control de llamada, realizado por el MSC que generalmente es responsable de las siguientes tareas:

- Registro de los suscriptores, cuando se enciende la Estación Móvil se registra en la red y entonces es visible para todos los suscriptores de la red.
- Establecimiento y enrutamiento de las llamadas entre dos suscriptores.
- Envío de SMS.

[25] PSTN (*Public Switched Telephone Network*) se refiere a la red telefónica pública conmutada, es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue.

[26] *Handover o handoff*, es un sistema en comunicaciones móviles celulares cuyo objetivo es el transferir la comunicación (el servicio prestado) de una estación base a otra cuando la calidad del enlace es insuficiente; este mecanismo garantiza y mantiene la comunicación cuando un dispositivo móvil se traslada a lo largo de su área de cobertura.

Como los suscriptores pueden moverse libremente en la red, el MSC es también responsable de la administración de movilidad de los suscriptores. Esta actividad comprende las siguientes tareas:

- Autenticación de suscriptores en el establecimiento de la conexión; esto es necesario debido a que un suscriptor no puede ser identificado fácilmente en la Red, como ocurre en una red telefónica pública por el par de cobre sobre el cual llegan las señales al usuario y a la central telefónica fija.

- Si una conexión no tiene actividad entre la Red y la Estación Móvil, el MSC tiene que reportar los cambios de localización de la Estación Móvil en la Red, para que se pueda enrutar las llamadas entrantes y los mensajes de texto. Este procedimiento es llamado A*ctualización de Localización*.

- Si el suscriptor cambia su localización mientras la conexión está establecida con la Red, el MSC es parte del proceso que asegura que la conexión no sea interrumpida y sea enrutada a la siguiente celda.

Existen diferentes nombres para el MSC, lo cual refleja la complejidad de sus funciones dentro de la Red, como cuando es llamada *Gateway* MSC definida como la interfaz que conecta a la Red Celular con otras redes.

Cada MSC está conectado a Controladores de Estaciones Base (BSC, *Base Station Controller*) de su área de influencia, pero también a su VLR (*Visitor Location Register*), y a su HLR (*Home Location Register*), así como, a los HLRs de los distintos operadores.

Un MSC controla un área geográfica que corresponde a un cierto número de *Location Area* (LA) llamado *MSC Service Area*.

2.1.1.2 *Home Location Register* (HLR)

Es una base de datos de suscriptores de la red GSM, la cual contiene un registro para cada usuario; también contiene información acerca de servicios individuales. Dentro de la Red Celular típicamente hay un pequeño número de HLRs.

El *International Mobile Subscriber Identity* (IMSI), es un número único que identifica a un suscriptor internacionalmente y se lo utiliza para tareas de señalización en la red. El IMSI es almacenado en la Tarjeta SIM del suscriptor y en el HLR; ésta es la clave para conocer toda la información acerca del usuario.

Para establecer la ruta de una llamada entrante a una Estación Móvil, el suscriptor es almacenado en el HLR con el área de servicio del MSC correspondiente.

El número de teléfono del usuario, el cual es denominado *Mobile Suscriber* ISDN *Number* (MSISDN) en el estándar GSM, está almacenado en un HLR determinado y único, que administra su operador móvil.

Al recibir una llamada, el MSC pregunta al HLR correspondiente al número llamado si está disponible y dónde está (es decir, a qué BSC hay que pedir que le avise) y enruta la llamada o da un mensaje de error.

La información almacenada contenida por cada estación móvil es:

- Identidad
- Servicios Suplementarios
- Información de su Ubicación
- Información de Autenticación

2.1.1.3 *Visitor Location Register* (VLR)

El VLR es una base de datos temporal con toda la información que un usuario necesita para poder acceder a los servicios de red. Esta información es proporcionada por el HLR con quien comparte funcionalidades; el VLR es el encargado también de mantener actualizados los datos de posición de una forma precisa.

Mientras los estándares permiten implementar al VLR como un componente independiente de hardware, gran parte de los fabricantes tienden a implementar el VLR simplemente como un componente de software en la MSC.

Cuando un suscriptor deja el área de cobertura de un MSC, el registro del suscriptor es copiado del HLR al VLR de un nuevo MSC, y es entonces removido del VLR de la MSC previa.

El VLR viene integrado con el MSC, y existirá uno por cada MSC, además en el VLR se almacena la identificación del Área de Localización del suscriptor.

Cuando un usuario se registra en la red, el VLR del MSC al que está conectado el usuario se pone en contacto con el HLR de origen del usuario y verifica si puede o no hacer llamadas según su tipo de suscripción. Esta información permanece almacenada en el VLR mientras el terminal de usuario está encendido y se refresca periódicamente para evitar fraudes (por ejemplo, si un usuario de prepago se queda sin saldo y su VLR no lo sabe, podría permitirle realizar llamadas).

Se debe tener en cuenta que el sistema GSM permite acuerdos entre operadores para compartir la red, de modo que un usuario en el extranjero por ejemplo puede conectarse a una red (MSC, VLR y recursos de radio) de otro operador.

Al encender el teléfono y realizar el registro en la red extranjera, el VLR del operador extranjero toma nota de la información del usuario, se pone en contacto con el HLR del operador móvil de origen del usuario y le pide información sobre las características de suscripción para permitirle o no realizar llamadas. Así, los distintos VLRs y HLRs de los diferentes operadores deben estar interconectados entre sí para que todo funcione.

2.1.1.4 *Short Messaging Service Center* (SMSC)

Otro elemento importante de la red es el SMSC el cual se utiliza para almacenar y enviar mensajes cortos. El servicio de mensajes cortos puede ser utilizado tanto para intercambiar mensajes entre usuarios, como con propósitos de notificación cuando una llamada es enviada al sistema de mensajes de voz.

El que envía el SMS, prepara el texto para el mensaje y entonces se transmite utilizando un canal de señalización al MSC.

Aparte del texto, el SMS contiene también el MSISDN del destinatario y la dirección del SMSC, información que la Estación Móvil extrae de la Tarjeta SIM. Cuando el MSC recibe el mensaje del suscriptor este mensaje es enviado de manera transparente al SMSC.

Cuando el mensaje es entregado, el SMSC analiza el MSISDN del receptor y extrae la localización actual utilizando el HLR. El SMS es entonces enviado al MSC correspondiente. Si el suscriptor se encuentra activo, el MSC trata de contactar a la estación móvil y si se recibe una contestación positiva, el mensaje se envía; una vez que la estación móvil confirma la recepción del mensaje, el MSC notifica al SMSC y el SMS se borra de la base de datos del SMSC.

Si el suscriptor no se encuentra activo, por ejemplo la batería de la Estación Móvil está descargada, la estación móvil no se encuentra en el rango de cobertura, o simplemente si el dispositivo está apagado, entonces no es posible entregar el mensaje. En este caso, una bandera de espera es activada en el mensaje dentro del VLR y el SMS es almacenado en el SMSC. Cuando el suscriptor se comunica con el MSC, el MSC notifica al SMSC para intentar la entrega.

2.1.1.5 *Authentication Center* (AuC)

Es una parte importante del HLR que almacena la clave individual por suscriptor (Ki), la misma que se encuentra almacenada en la tarjeta SIM del suscriptor. La clave Ki es secreta, previniendo así, que ésta pueda ser leída directamente.

AuC es una base de datos protegida, que proporciona los parámetros necesarios para autentificar a los usuarios dentro de la red; soporta también funciones de cifrado, permitiendo verificar la identidad del usuario y asegurando la confidencialidad de cada llamada; protege de fraudes al operador de la red.

2.1.1.6 *Equipment Identity Register* (EIR)

El EIR se utiliza para proporcionar seguridad en las redes GSM a nivel de equipos válidos, además contiene una base de datos con todos los IMEIs (*International Mobile Equipment Identity*) de los equipos autorizados en la Red. Es decir, que si un determinado equipo trata de hacer uso de la red y su IMEI no se encuentra

dentro de la base de datos del EIR, éste no podrá acceder a la red. La base de datos está dividida en tres secciones:

- ***White List***: Contiene las identidades de los equipos autorizados para acceso al servicio. Además contiene todos los IMEI designados a todos los operadores de las naciones con las que se tienen acuerdos de *roaming* internacional.

- ***Black List*****:** contiene todos los IMEI que se consideran bloqueados (por ejemplo los robados).

- ***Grey List*****:** En esta lista figuran las identidades de los equipos en observación, por ejemplo, aquellos en los que se ha detectado algún tipo de fallo, contiene todos los IMEI marcados como *faulty,* relativo a aparatos no homologados. Los terminales introducidos en la *Grey List* son señalados a los operadores de sistema a través de una alarma cuando solicitan el acceso, permitiendo la identificación del abonado que utiliza el Equipo Móvil y el área donde se encuentra.

2.1.1.7 *Elementos del Sistema GPRS (General Packet Radio Service)*

El sistema GPRS (*General Packet Radio Service*) se propone como una extensión del sistema móvil GSM, para envio y recepción de datos de usuario, mediante la técnica de conmutación de paquetes, a diferencia del sistema GSM que utiliza la técnica de conmutación de circuitos para el servicio de transmisión de voz.

GSM añade un conjunto de servicios complementarios y servicios de transmisión de datos a baja velocidad aprovechando su carácter digital, pero no fue concebido con intención de ofrecer de forma óptima servicios de transmisión de datos, es por ello la necesidad de un nuevo sistema llamado GPRS.

La tecnología GPRS mejora y actualiza a GSM en los siguientes servicios:

- Servicio de mensajes multimedia (MMS)

- Mensajería instantánea

- Aplicaciones en red para dispositivos a través del protocolo WAP
- Servicios P2P utilizando el protocolo IP
- Servicio de mensajes cortos (SMS)
- Posibilidad de utilizar el teléfono móvil como módem USB

Los sistemas GSM y GPRS comparten los mismos canales de radio, con un reparto de los recursos en función de la demanda de los diferentes servicios. El concepto básico detrás de la transmisión de paquetes de GPRS, radica en su habilidad de permitir que las aplicaciones seleccionadas compartan los recursos de radio, asignando los recursos de radio para transmisión solamente cuando las aplicaciones tienen datos a transmitir.

El sistema GPRS introduce dos nuevos elementos sobre la arquitectura GSM que hace posible su funcionamiento complementario como sistema de conmutación de paquetes, el SGSN (*Serving GPRS Support Node*) y el GGSN (*Gateway GPRS Support Node*).

La introducción de estos dos nuevos elementos, SGSN y GGSN, define nuevos interfaces de interconexión con el resto de elementos de red compartidos con GSM como las bases de datos HLR y VLR que añaden las informaciones de usuario para dar soporte a los nuevos servicios GPRS y los elementos de gestión de los recursos radio BTS y BSC que añaden las funcionalidades del sistema GPRS para hacer posible su uso compartido.

2.1.1.7.1 Serving GPRS Support Node (SGSN)

En GSM la funcionalidad de conmutación de circuitos la realiza el elemento MSC, mientras que para la arquitectura GPRS se añade el elemento complementario SGSN de conmutación de paquetes, que realiza entre otras las siguientes funciones:

- Opera como un *router* para los paquetes de datos de las estaciones móviles presentes en un área geográfica.

- Enruta los datos al GGSN cuando se requiere una conexión a una red externa
- Administración de la movilidad
- Realiza funciones de seguridad (autenticación y cifrado), control de acceso, facturación y estadísticas de tráfico.
- Funciones para asociarse y desasociarse (*attach/detach*) con la Red.
- Conversión de Protocolos entre el *backbone IP* y los protocolos utilizados en el BSS y en la Estación Móvil

2.1.1.7.2 Gateway GPRS Support Node (GGSN)

En GSM la interconexión con otras redes de conmutación la realiza el elemento G-MSC (*Gateway* MSC), y en la arquitectura GPRS la realiza el elemento GGSN (*Gateway GPRS Support Node*), que cumple las siguientes tareas:

- Funciona como un punto de acceso para los SGSN, provee el punto de asociación entre el dominio GPRS y otras redes de datos tales como Internet.
- Gestión de Movilidad.
- Interfaz hacia redes *IP* (*IPv4* e *IPv6*) y *X.25* especificadas en el estándar GPRS.
- Traducción de direcciones de los paquetes entrantes a direcciones GSM y de las que recibe desde el SGSN a las de la red externa.
- Encapsulación/ desencapsulación de paquetes.

2.1.1.8 *Base Station Subsystem* (BSS)

El subsistema de Estación Base, también llamado “subred de radio”, contiene todos los nodos y funciones de control de los recursos de radio, que son necesarios para la conexión inalámbrica de los suscriptores móviles sobre la interfaz de radio o “interfaz de aire” a la red.

El BSS está compuesto de una o más BTSs, que realizan funciones de nivel físico (interfaz de radio), y la BSC que efectúa la gestión de los recursos de radio.

2.1.1.8.1 Base Station Controller (BSC)

Es el responsable del establecimiento, liberación y mantenimiento de todas las celdas con las cuales se encuentra conectada. Provee todas las funciones de control y enlaces físicos entre el MSC y las BTSs, además de administrar todas las funciones de radio de la red.

Las funciones más relevantes del BSC son las siguientes:

- Gestión de los canales de radio (elección de celda y canal)
- Control de la potencia de trabajo de las estaciones móviles (MS)
- Gestión del proceso de *Handover*
- Adaptación de las velocidades de los canales de radio (inferiores a 16 Kbps) al estándar de 64 Kbps utilizado por la PSTN o ISDN.

2.1.1.8.2 Base Transceiver Station (BTS)

También llamadas estaciones base, son los elementos visibles del sistema GSM; comparada con la red telefónica pública, la estación base reemplaza la conexión cableada al suscriptor, por la conexión inalámbrica la cual es llamada interfaz de aire.

Las estaciones base son también los componentes más numerosos de la red móvil. Su función principal es la de proporcionar un número de canales de radio para su respectiva zona de servicio.

El sistema consiste en una red de radio-células, también conocida como celdas contiguas (con cobertura sobrepuesta para asegurar el *handover*) que se utilizan para cubrir una determinada área de servicio; cada celda tiene una BTS.

BTS contiene dispositivos de transmisión y recepción de señales de radio (*transceivers*), incluyendo las antenas y también el procesador de señales

necesario para el interfaz de radio, así como, equipos de comunicación con la BSC, situadas por lo regular en el centro de cada celda.

Pueden existir una o varias BTS por cada BSS y es justamente la potencia de éstas la que determina el tamaño de una celda. Dentro de las funciones que realizan las BTS se tienen:

- Sirven como interfaz física entre las estaciones móviles y los controladores de estaciones base (BSC).
- Se encargan de los aspectos de diversidad en antenas.
- Control dinámico de potencia, entre otras.

2.1.1.9 Evidencia Digital Potencial en la Arquitectura GSM

Dentro de la Arquitectura Instalada Fija de GSM, como se mencionó anteriormente, son de interés como evidencia digital, los CDRs se crean y almacenan en el MSC con el propósito de facturación e identificación de la BTS sobre las cuales fueron efectuadas llamadas y mensajes de texto, además de información de tiempo y localización del suscriptor.

Los registros o CDRs comúnmente generados son:

a. Registros de llamadas realizadas/recibidas por las estaciones móviles.
b. Registros de mensajes enviados/recibidos.
c. Registros del HLR y VLR, respecto a la Ubicación de la Estación Móvil.

Este análisis requiere de la participación en su totalidad de la Operadora de Telefonía Móvil, quien muchas veces no está dispuesta a colaborar, por razones de seguridad o medios legales; pero la combinación del análisis de los CDRs con la estación móvil puede ayudar a establecer hechos relacionados con un acto delictivo o puede ayudar a corroborar una coartada.

2.1.2 ESTACIÓN MÓVIL

Sobre el marco teórico de GSM, al teléfono móvil se lo conoce como Estación Móvil (MS, *Mobile Station*). Éste se encuentra constituido por dos partes, el Equipo Móvil (ME, *Mobile Equipment*) o también conocido como Terminal Móvil y la tarjeta SIM (*Subscriber Identity Module*).

Éstos son diseñados para obtener movilidad por parte del usuario, desarrollados en un tamaño pequeño, una batería liviana y que proporcione larga duración; usa sistemas operativos propietarios tales como RIM y una memoria flash interna.

La tarjeta SIM, almacena algunos identificadores y algoritmos necesarios para autenticar al suscriptor en la red. Un usuario puede remover la tarjeta SIM de su equipo móvil e insertarla en otro móvil compatible, y reanudar la operación del mismo sin la intervención de la operadora celular, conservando su número telefónico, plan de servicio e incluso el directorio de marcado rápido.

Los archivos dentro de la tarjeta SIM, son utilizados por los usuarios para almacenar información de la configuración de la red, contactos, enviar y recibir mensajes de texto.

Los teléfonos móviles cada vez son más avanzados y es posible desarrollar varias funciones tales como navegadores de Internet, comunicación vía *e-mail*, y almacenamiento de archivos.

Para entender dónde se puede encontrar evidencia digital se debe analizar tanto el Equipo Móvil como la tarjeta SIM.

2.1.2.1 *Mobile Equipment*

Los Equipos Móviles son dispositivos cuyo principal identificador es el IMEI (*International Mobile Equipment Identity*), que trabaja conjuntamente con la Tarjeta SIM en la arquitectura GSM, realizando una serie de funciones que van desde la de un organizador digital simple hasta la de un ordenador de gama baja.

El ME está diseñado para movilidad, tiene un tamaño compacto, con baterías recargables, y es ligero. Todos los Equipos Móviles tienen un número de

características en común, pero los fabricantes tratan de diferenciar sus productos por lo que ejecutan funciones adicionales para hacerlos más atractivos a los consumidores. Esto ha provocado gran innovación en Equipos Móviles los últimos 20 años.

La mayoría de Equipos Móviles tiene un conjunto básico de elementos y capacidades comparables entre diferentes fabricantes. Disponen de un microprocesador, memoria de sólo lectura (ROM, *Read Only Memory*), memoria de acceso aleatorio (RAM, *Random Access Memory*), un módulo de radiofrecuencia, un procesador de señal digital, un micrófono y un altavoz, una variedad de interfaces, y una pantalla de cristal líquido (LCD).

El sistema operativo (SO) del dispositivo se mantiene en la memoria ROM; con herramientas adecuadas, normalmente se puede borrar y reprogramar electrónicamente. La memoria RAM, la cual en algunos modelos se puede utilizar para almacenar datos de usuario, se mantiene activa por medio de baterías, y su daño o agotamiento hace que esta información se pierda.

Los últimos Equipos Móviles desarrollados disponen de microprocesadores cada vez más avanzados que reducen el número de chips de apoyo necesarios para las tareas de procesamiento; incluyen una capacidad de memoria considerable, se puede integrar ranuras para tarjetas de memoria extraíbles y periféricos especializados, tales como *WiFi*, *IrDA* o *Bluetooth*.

La mayoría de los modelos populares de equipos móviles en el mercado internacional son producidos por Nokia, Sony Ericsson, Motorola, Samsung y LG.

2.1.2.1.1 Estructura

Los equipos móviles son dispositivos electrónicos complejos. A medida que pasa el tiempo aumenta la tecnología, las funciones y la complejidad en su construcción. Los equipos móviles inteligentes de hoy tienen numerosas partes dentro de ellos, pero la mayoría de Equipos Móviles independiente de su tamaño y variedad de funcionalidades tienen una estructura básica común.

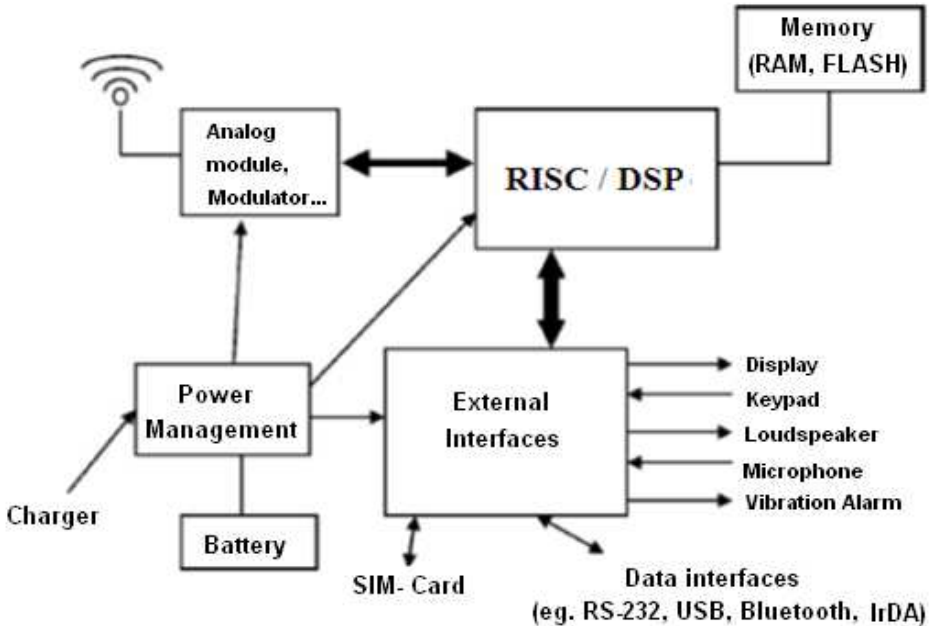


Figura 2.4: Estructura básica de un equipo móvil [18]

La Figura 2.4 presenta la estructura básica del Equipo Móvil. A continuación se describen sus componentes:

a. RISC CPU*, Reduce Instruction Set* CPU: Es un procesador que se encarga de:

- Procesar la información que recibe vía diferentes canales utilizados en la interfaz de aire, sean éstos para tráfico y control entre la BTS y la Estación Móvil.
- Establecer las llamadas.
- Procesar parte de la transmisión.
- Administrar la movilidad de procesos como *handover, location update.*
- Conexiones vía interfaces externas como *Bluetooth*, IrDA, USB.
- Controlar el Interfaz de Usuario como el teclado y el *display*.

Muchas de estas tareas tienen que ser realizadas de forma simultánea, por lo que un sistema operativo multitarea de tiempo real se usa sobre el procesador RISC.

El componente de tiempo real del sistema operativo es especialmente importante para dar prioridades; por ejemplo si el procesador tiene la función de transmitir datos sobre la interfaz de aire durante una sesión GPRS, todas las otras tareas, como el control del teclado y de la interfaz gráfica tienen una prioridad más baja de ser atendidas por el procesador.

La capacidad del procesador RISC es el factor principal que decide las aplicaciones y funciones que se puede implementar en el teléfono.

b. DSP, *Digital Signal Processor*: Su principal tarea es la compresión de voz, la misma que será transmitida y decodificada en la cadena de recepción.

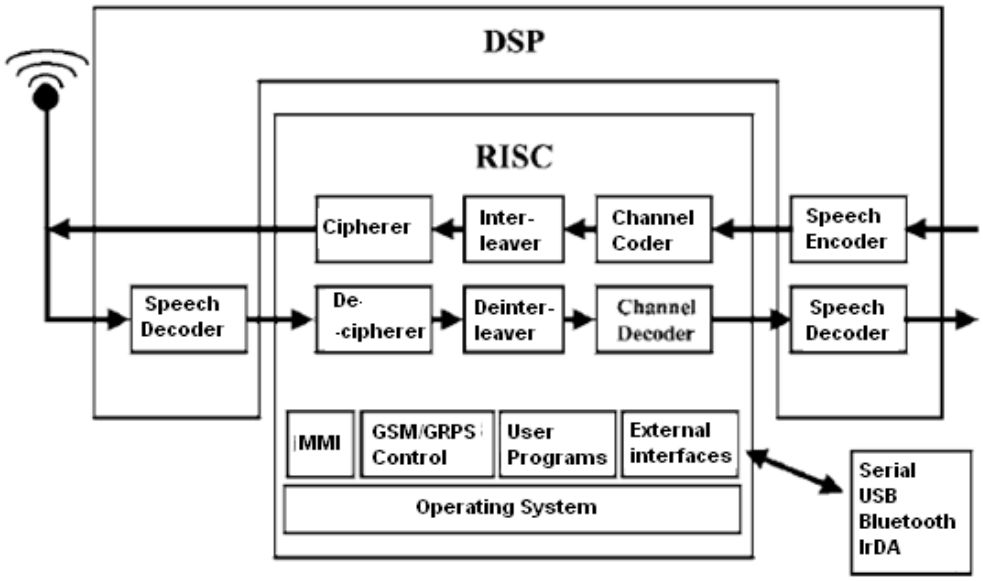


Figura 2.5: Funcionalidades realizadas por los procesadores RISC y DSP [18]

Por ejemplo el DSP 56600 con una frecuencia del procesador de 104 MHz se usa para estas tareas. La Figura 2.5 muestra las tareas realizadas por los procesadores RISC y el DSP.

c. **La placa de circuitos:** Esencialmente es el cerebro de la operación, permite que todas las partes del Equipo Móvil se comuniquen entre sí, permitiendo al móvil seguir trabajando. Sin esta placa el equipo móvil sería simplemente una colección de partes que no harían nada. Una placa de circuitos es similar a la placa madre de una computadora.

d. **Memorias**: Un equipo móvil contiene memoria volátil y no volátil sobre las cuales varias categorías de datos se pueden almacenar, como el código del sistema operativo, los controladores de dispositivos, librerías del sistema, aplicaciones del sistema operativo, aplicaciones del usuario, diversos tipos de texto, imagen, audio, vídeo y otros archivos de datos, incluyendo datos personales.

   La estructura de la memoria del teléfono móvil puede ser dividida en áreas fijas para ciertos datos, tales como las entradas de la agenda, las entradas del calendario, los registros de llamadas y mensajes SMS, o asignado dinámicamente mediante un gestor de memoria interno.

   La memoria también puede ser estructurada de forma más rigurosa como un sistema de archivos con formato. El tipo de memoria en la que cada categoría de datos se almacena y la estructura de memoria empleada varían entre los fabricantes y, a menudo se basan en las características del sistema operativo utilizado.

   Incluso para un determinado modelo de equipo móvil, la asignación de los datos para almacenamiento puede variar entre equipos móviles proporcionados por operadoras de diferentes redes, en función de las adaptaciones hechas por los fabricantes para cada operadora.

   Las actualizaciones de *firmware* enviado por un proveedor de red también pueden afectar las localizaciones de los datos. La Figura 2.6 muestra un arreglo típico, en la que residen los archivos de usuario en la memoria no volátil, tales como Flash ROM o posiblemente un micro disco duro, junto con el código del sistema operativo. Dado que el almacenamiento es persistente, los contenidos no se ven afectados si la energía se agota

completamente. La memoria volátil se utiliza para el almacenamiento dinámico y su contenido se pierde cuando se agota la batería.

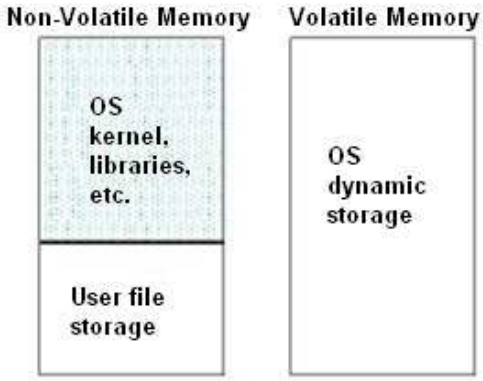


Figura 2.6: Asignación de espacios en memorias de almacenamiento [19]

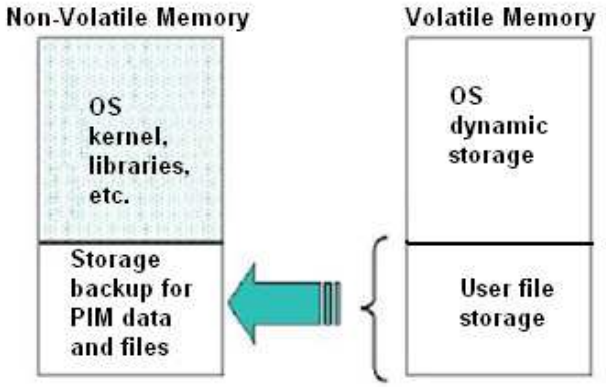


Figura 2.7: Asignación alternativa de espacios en memorias de almacenamiento [19]

Una alternativa común de un arreglo de memoria, utilizada principalmente en los teléfonos inteligentes, se muestra en la Figura 2.7. La memoria volátil se utiliza para el almacenamiento dinámico y de archivos de usuario. La memoria no volátil se utiliza principalmente para mantener el código del sistema operativo, y posiblemente información personal, sean datos o archivos a manera de copia de seguridad de la memoria volátil.

e. **Micrófono y bocina**: permiten al usuario del teléfono móvil hablar y escuchar, a la otra persona que está en la línea luego de su decodificación

respectiva en el microprocesador. Muchos de los teléfonos incluyen un segundo micrófono y bocina que se los utiliza en el altavoz.

f. Pantalla de cristal líquido (LCD): Muestra visualmente toda la información, similar al visor de una calculadora. En los últimos años se ha desarrollado la tecnología de este tipo de pantallas, permitiendo el uso de pantallas a color.

g. *Teclado/Keypad*: Proporcionan el interfaz entre el usuario y el sistema, éste es el único componente del sistema con el cual, bajo operación normal, los usuarios están involucrados.

Cualquier característica del sistema básica o mejorada, es accesible vía el teclado numérico, y una vez que se establezca una conexión, este componente proporciona la funcionalidad similar a la de cualquier teléfono convencional.

El Equipo Móvil contiene un *display* que ilumina los dígitos marcados y proporciona una ayuda navegacional a otras características. El teclado numérico permite almacenar los números telefónicos para uso futuro y proporciona el acceso a otras características que pueden variar según fabricante.

h. Antena: Es una antena de goma flexible montada en el equipo móvil, generalmente son antenas internas o antenas extensibles externas.

Las antenas y los cables que conectan a los transmisores de radio deben tener características de rendimiento adaptables a los circuitos de transmisión, frecuencia y niveles de potencia.

El uso de antenas y cables que no están optimizados para su uso pueden afectar negativamente al rendimiento. El cable incorrecto, el cable dañado, o conexiones defectuosas pueden impedir el funcionamiento de equipo móvil.

i. **Baterías:** Sin éstas no habría como alimentar de energía al teléfono móvil o Estación Móvil, pues almacena la energía necesaria para el funcionamiento del teléfono.

   La mayoría de teléfonos móviles posee una batería recargable mientras está dentro del teléfono, a menudo acompañadas de un cargador de corriente alterna.

   Actualmente existen tres tipos de baterías en el mercado según el material del que se componen: la primera de NiCd (Níquel /Cadmio), la segunda de NiMH (Hidrato Metálico de Níquel) y la tercera de Li-Ion (Iones de Litio).

   Las diferencias entre estos tipos de batería radican en la capacidad, y tiempo de vida. Las baterías NiMH poseen una gran capacidad, pero su rendimiento decae después de unos 300 ciclos (carga – descarga) lo que causa el decrecimiento de su capacidad y el crecimiento de su resistencia interna.

   Las baterías NiCd ofrecen aproximadamente un 30% menos de capacidad que las anteriores, pero su vida útil se extiende hasta los 1000 ciclos aproximadamente, con un rendimiento constante debido a que la resistencia interna permanece baja.

   En cambio, las baterías de Ion de Litio ofrecen una alta energía, bajo peso y no requieren de cargas periódicas, pero pierden su capacidad con el tiempo, aunque se use o no. Si su uso es constante, podría llegar a usarse unos 1000 ciclos.

j. **Componentes Opcionales:** Aparte de los componentes básicos anteriormente analizados, los fabricantes también agregan componentes y funciones a sus teléfonos, particularmente para teléfonos inteligentes; dos de los componentes más populares son capacidades GPS e interfaces inalámbricas para conectarse a Internet. Los fabricantes pueden crear las antenas separadas para estas capacidades, o intentan combinarlas en una sola antena.

2.1.2.2 Tipos de Equipos Móviles

Existen Equipos Móviles con diferentes características de *hardware* y *software*, por ejemplo difieren en tamaño, peso, velocidad del procesador, capacidad de memoria, sistema operativo, aplicaciones de usuario, entre otras.

	Básicos	**Avanzados**	**Inteligentes**
Procesador	Velocidad Limitada	Velocidad mejorada	Velocidad Superior
Memoria	Capacidad Limitada	Capacidad Mejorada	Capacidad Superior, Posibilidad de Disco Duro.
Display	Escala de Grises	Color	De gran tamaño color 16 bits (65536 colores) o superior
Ranuras para Tarjetas	Ninguna	*MiniSD o MMCmobile*	*MiniSD o MMCmobile*
Cámara	Ninguna	Función Fotográfica	Función Fotográfica y video
Entrada de Texto	Teclado Numérico	Teclado Numérico	Pantalla táctil, reconocimiento de escritura a mano, construido el teclado en estilo *QWERTY*
Interfaz Celular	Voz y datos limitados	Voz y datos de velocidad normal	Voz y datos de alta velocidad
Interfaz Inalámbrica	*IrDA*	*IrDA, Bluetooth*	*IrDA, Bluetooth, WiFi*
Baterías	Recargable Polímero de Ion de Litio	Removible y recargable Polímero de Ion de Litio	Removible y Recargable Ion de Litio

Tabla 2.1: Características de *Hardware*

En general, se pueden clasificar como Equipos Móviles Básicos los que principalmente sirven para la comunicación entre personas (enviar y recibir

mensajes, realizar y recibir llamadas), como Equipos Móviles Avanzados los que ofrecen capacidad adicional y servicios multimedia (enviar y recibir mensajes multimedia, cámaras fotográficas integradas), y Equipos Móviles Inteligentes los que añaden capacidad y funcionalidades superiores a las de un Equipo Móvil Avanzado (navegación por Internet, cámaras de video integradas).

La Tabla 2.1 presenta las características de *hardware* que de manera general disponen los modelos de Equipos Móviles Básico, Avanzado e Inteligente. Además muestra que los Equipos Móviles con más capacidad y mayores funcionalidades pueden capturar y retener no sólo más información, sino también información variada, a través de una amplia gama de fuentes integradas, incluidos los módulos de memoria extraíble, otras interfaces inalámbricas y *hardware* incorporado.

	Básico	**Avanzado**	**Inteligente**
Sistema Operativo	Propietario	Propietario	Linux, Windows Mobile, RIM SO, Symbian.
Información Personal	Simple Directorio Telefónico	Directorio Telefónico y Calendario	Recordatorios, Directorio Telefónico y calendario mejorado.
Aplicaciones	Ninguna	Reproductor MP3	Reproductor MP3, video y visualización de documentos Office.
Mensajería	Mensajes de Texto	Mensajes de texto con imágenes y sonidos simples	Mensajes de Texto Mejorados, mensajes multimedia.
Chat	Ninguna	Chat mediante SMS	Mensajes Instantáneos
E-mail	Ninguna	Via *Network Operator's Service Gateway*	Vía POP o servidor IMAP
Web	Ninguna	Vía WAP *Gateway*	Directo HTTP
Wireless	IrDA	IrDA, *Bluetooh*	IrDA, *Bluetooth*, *WIFI*

Tabla 2.2: Características de *Software*

Hay que tener en cuenta que los componentes de *hardware* pueden variar, de hecho la tecnología que antes se consideraba para Equipos Móviles Avanzados o Inteligentes, con el tiempo aparecen en lo que ahora se consideraría un Equipo Básico, aunque las líneas dentro de este esquema de clasificación no están bien definidas, no obstante, servirán como guía general.

Indistintamente del tipo de Equipo Móvil, todos estos dispositivos soportan llamadas, mensajes de texto, un conjunto básico para la gestión de información personal que incluye aplicaciones como agenda y directorio telefónico.

Con respecto a las características de *software* los Equipos Móviles Avanzados e Inteligentes, ofrecen la posibilidad de realizar mensajería multimedia, conectarse a Internet y navegar por la web, además ofrecen aplicaciones para la gestión de información utilizando protocolos de sincronización para el intercambio de datos con el computador, entre otras.

Los móviles inteligentes, agregan la capacidad de un computador personal y así se logra la revisión de documentos electrónicos tales como informes, diapositivas, y hojas de cálculo. La Tabla 2.2 muestra las características de *software* que de forma general se encuentran en los Equipos Móviles.

Los Equipos Móviles Básicos y Avanzados suelen utilizar un sistema operativo propietario. Mientras que los Equipos Móviles Inteligentes utilizan uno de los siguientes sistemas operativos: *Windows Mobile* (*Phone Edition*), RIM SO, Symbian SO, o Linux, estos sistemas operativos son multitarea y con funciones completas, diseñados específicamente para que coincidan con las características de *hardware* de los Equipos Móviles Inteligentes. .

Los Equipos Móviles inteligentes soportan correo electrónico con plenas funciones, utilizan *Post Office Protocol* (POP), *Internet Message Access Protocol* (IMAP), *Simple Mail Transfer Protocol* (SMTP).

Para la navegación en la web se utiliza *Hypertext Transfer Protocol* (HTTP), mientras que los Equipos Avanzados prestan esos servicios a través del Protocolo de Aplicaciones Inalámbricas (WAP, *Wireless Application Protocol*); y los Equipos Móviles Básicos no soportan estos servicios.

2.1.2.3 Evidencia Potencial en la Estación Móvil

Debido a la tasa alta de penetración de los teléfonos móviles y a sus nuevas características, como mayor capacidad de almacenamiento y aumento de aplicaciones, ha sido inevitable el incremento de actividades delictivas en las cuales este presente un teléfono celular; por lo que se debe considerar que mientras éstos contengan información digital son una fuente primaria de evidencia.

Los móviles almacenan información personal, llamadas telefónicas y mensajes de texto que proporcionan evidencia digital durante una investigación. Los examinadores forenses tienen que seguir metodologías y procedimientos claros para la recuperación adecuada y posterior examen de la evidencia encontrada en el teléfono móvil.

El conjunto de características y capacidades pueden variar, dependiendo de la época en la que se fabricó el teléfono, la versión del *firmware*, las modificaciones realizadas por un determinado prestador de servicios y las aplicaciones instaladas por el usuario; pero en general se tienen las siguientes fuentes de evidencia digital:

- ✓ Identificadores del equipo y el suscriptor
- ✓ Fechas, lenguajes, y otras configuraciones
- ✓ Directorio Telefónico
- ✓ Información del Calendario
- ✓ Mensajes de Texto
- ✓ Registros de llamadas marcadas, recibidas y perdidas
- ✓ Correo electrónico
- ✓ Fotos
- ✓ Grabaciones de audio y video

- ✓ Mensajes Multimedia
- ✓ Mensajería instantánea y navegación en internet o WAP
- ✓ Documentos electrónicos
- ✓ Información de Localización

Los elementos de pruebas o evidencias presentes en una estación móvil, no sólo dependen de las características y capacidades del teléfono, sino también de los servicios de voz y datos suscritos por el usuario. Por ejemplo, el servicio telefónico pre-pagado no suele incluir servicios de datos, y descarta la posibilidad de mensajería multimedia, correo electrónico y navegación por Internet o WAP. Del mismo modo, un contrato de suscripción selectiva puede excluir ciertos tipos de servicio, aunque el teléfono tenga la capacidad de realizar estas funciones.

En resumen los Equipos Móviles son medios electrónicos que se constituyen en evidencia electrónica, esto significa que los Equipos Móviles tienen la misma posibilidad de contener evidencia digital, tal como el disco duro de una computadora.

El contenido de un Equipo Móvil es frágil y puede ser fácilmente borrado o sobrescrito, por lo tanto debe ser cuidado de manera de no perder la evidencia que podrían contener.

La evidencia digital potencial, es la encontrada en las memorias del Equipo Móvil, ya que muchos fabricantes de teléfonos celulares usan la memoria interna del equipo móvil, para implementar nuevas funciones y almacenar cierta información que no puede ser almacenada en la tarjeta SIM, debido a que tienen especificaciones que permiten el almacenamiento de cierto tipo de información.

Los primeros modelos de teléfonos móviles usaban una memoria no volátil interna EEPROM (*Electrically-Erasable Programmable Read-Only Memory*); con el crecimiento de la demanda de memoria, se comenzó a implementar memorias flash dedicadas para el almacenamiento del *software* del Equipo Móvil, este tipo

de memoria no necesita de energía permanente, y no está integrada al procesador.

La memoria interna RAM se usa para almacenar datos durante la comunicación e interacción del usuario, esta memoria puede ser implementada como un circuito separado o puede estar integrado en el procesador del Equipo Móvil.

Las computadoras generalmente usan un disco duro, en tanto que un equipo móvil utiliza una memoria flash, por eso no se puede afirmar que un equipo móvil sea una computadora; esta diferencia es importante de entender para los analistas forenses.

Es común encontrarse con memorias externas, debido a que los Equipos Móviles tienen ranuras para éstas, por sus funcionalidades tales como cámaras fotográficas y de video o reproductores de MP3. Se utilizan memorias externas como: SD (*Secure Digital*), MMC (*Multimedia Card*), CF (*Compact Flash Card*), *MicroSD* entre las más comunes.

Debido a su naturaleza, las memorias externas pueden ser analizadas por herramientas utilizadas para el análisis de sistemas informáticos, ya que existen adaptadores USB.

En general la evidencia digital lo constituye:

a. **IMEI (*International Mobile Equipment Identity*) :** El equipo móvil está asociado al código IMEI como identificativo en la red GSM, el cual se lo puede presentar como NNXXXXXXZZZZZZA, en la Tabla 2.3 se puede apreciar su significado.

b. **Directorio Telefónico:** Guarda información de diferentes contactos utilizados por el suscriptor; con la ayuda de éste es posible hacerse una idea de la red social sobre la cual se desenvuelve la persona sospechosa, se podría asociar al sospechoso con la víctima.

c. **Historial de Llamadas:** Ofrece una visión más profunda en cuanto a la actividad del propietario antes de que su teléfono celular sea encontrado en

la escena del crimen y puesto a disposición de los analistas forenses para su investigación. Se pueden ver las últimas llamadas entrantes y salientes, así como su duración. Esta información puede ser útil para obtener supuestos y conclusiones que pueden llevar a la solución del caso.

NN	XXXXXX	ZZZZZZ	A
TAC - *Type Allocation Code*		*Serial Number*	*Check Digit*
Reporting Body Identifier	*Type Identifier defined*	*Number range allocated but assigned to individual mobile stations by the manufacturer.*	*Defined as a function of all other digits (calculated by the manufacturer).*

Tabla 2.3: Campos constitutivos del IMEI

d. Mensajes cortos, Mensajes multimedia, buscadores Web/WAP y correos electrónicos: Los mensajes, buscadores y correos electrónicos pueden ofrecer información concreta en contraste con el historial de llamadas y el directorio telefónico que sólo ofrecen información indirecta. Pueden contener palabras reales escritas por el propietario o destinados al propietario, lo que puede servir como prueba.

e. Calendario: Ofrece una visión general sobre las actividades pasadas y previstas del propietario. Puede ser utilizado para conectar con el propietario determinado lugar y momento, así como indicaciones sobre posibles testigos

f. Otros dispositivos: Por ejemplo memorias externas, es posible que un sospechoso haya tomado una imagen como un trofeo de su acto delictivo; los datos se pueden utilizar para determinar la fecha exacta en la que la foto fue tomada en algunos casos, incluso la ubicación. Algunos teléfonos móviles están equipados con un receptor GPS. Este receptor puede almacenar información sobre lugares y horarios de forma independiente de las aplicaciones que se ejecutan en el teléfono celular. Así se puede

vincular al propietario del teléfono celular o sospechoso con la escena del crimen o para desechar posibles coartadas.

2.1.3 SIM

El módulo de identidad del suscriptor o tarjeta SIM es un elemento fundamental estandarizado en la red GSM, contiene toda la información concerniente al suscriptor, utilizada en los Equipos Móviles de tecnología GSM.

Los parámetros más importantes sobre la tarjeta SIM son el IMSI[27] y la Ki[28], los cuales son usados en la autenticación y la generación de las claves de cifrado. Una tarjeta SIM es mucho más que una simple tarjeta, contiene un microprocesador y memorias que pueden ser usadas para propósitos adicionales.

La tarjeta SIM adicionalmente provee el almacenamiento de información personal, tal como directorio telefónico, mensajes de texto.

Las tarjetas SIM se clasifican de acuerdo a la fase de las especificaciones que se aplicaron, la cual es grabada en un elemento del sistema de archivos. Las tres fases definidas son fase 1, fase 2 y fase 2+, las últimas dos fases corresponden a redes celulares de segunda generación (2G y 2.5G).

Una tarjeta SIM es un tipo especial de tarjeta inteligente que típicamente contiene un procesador y una memoria programable, borrable electrónicamente (EEPROM) con capacidad que va de 16 KB a 256 KB; también incluye la memoria RAM para la ejecución del programa, y la memoria ROM para el sistema operativo, autenticación de usuarios, algoritmos de cifrado de datos y otras aplicaciones.

El sistema de archivos está organizado jerárquicamente en la tarjeta SIM, reside en la memoria persistente y almacena diversos datos como entradas de nombres y números telefónicos, mensajes de texto y configuración de la red de servicios.

---

[27] *IMSI* (*International Mobile Subscriber Identity),* es un número único de identificación almacenado en la tarjeta SIM del teléfono.

[28] *Ki,* Clave de autenticación del suscriptor entre la tarjeta SIM y BS.

Dependiendo del teléfono, alguna información que se almacena en la tarjeta SIM puede coexistir en la memoria del teléfono, como mensajes de texto y directorio telefónico. Por otra parte, la información puede residir en su totalidad en la memoria del teléfono en lugar de la memoria disponible en la tarjeta SIM.

La autenticación del teléfono celular a una red segura es una función vital realizada a través de la tarjeta SIM. La información de clave de cifrado y algoritmos dentro del encapsulado, proporcionan los medios para que el dispositivo participe en un diálogo de pregunta-respuesta en la red y responder correctamente, sin exponer material clave y otra información que podría utilizarse para clonar la Tarjeta SIM y tener acceso a los servicios de un suscriptor. La tarjeta SIM además admite el cifrado de la trama para proteger contra las escuchas no autorizadas en la interfaz de aire.

2.1.3.1 Estructura Física

La Tarjeta o Módulo SIM tiene un ancho de 25 mm, una altura de 15 mm y un espesor de 0.76 mm, la cual es similar a una huella digital o estampilla postal como se muestra en la Figura 2.8.

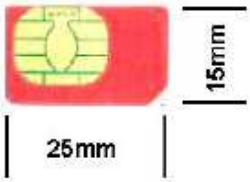


Figura 2.8: Diagrama de una tarjeta SIM

Las tarjetas SIM tienen un conjunto de especificaciones con diferentes características, sus 8 pines de conexión no son alineados a lo largo del borde como se muestra en la Figura 2.9, en cambio hay un contacto de forma circular en la almohadilla de la tarjeta inteligente, la cual está incluida en un marco plástico.

La ranura para la tarjeta SIM normalmente no es accesible en el exterior del teléfono celular lo que facilitaría la frecuencia de inserción y el poder removerla como una tarjeta de memoria; en cambio, típicamente se la encuentra en un compartimiento debajo de la batería.

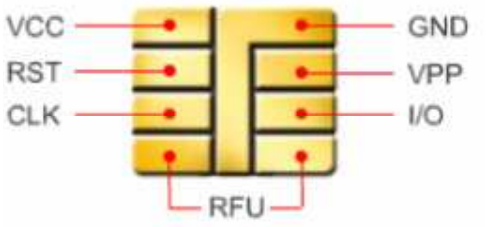


Figura 2.9: Pines de una tarjeta SIM

Cuando una tarjeta SIM se inserta en un terminal telefónico y los pines hacen contacto, una interfaz serial se usa para la comunicación entre ellos. Una tarjeta SIM puede quitarse de un Equipo Móvil y puede leerse usando un lector y software especializado a través de la interfaz serial.

La tarjeta SIM, es una tarjeta inteligente que consta de las siguientes partes:

- CPU de 8 o 16 bits
- Memoria de Programación o ROM de 40 a 100 *Kbyte*
- Memoria de Trabajo o RAM de 1 a 3 *Kbyte*
- Memoria de datos (EEPROM) de 16 a 64 *Kbyte*
- Entradas/Salidas de control.

Estos 5 módulos deben estar unidos dentro de un circuito integrado, para que su seguridad no se vea amenazada, ya que las conexiones pueden ser violentadas y se tendría un acceso ilegal y/o una malversación de parámetros importantes de la tarjeta SIM.

Una tarjeta SIM no es una simple tarjeta de almacenamiento, se encarga de los procesos de cifrado, almacena información del usuario, como se muestra en la Figura 2.10. El Equipo Móvil no puede acceder directamente a la información de la EEPROM, para ello tiene que hacer una petición al microprocesador, con lo que se prohíbe el acceso a información sensible, por esto se constituye en un sistema de microprocesamiento.

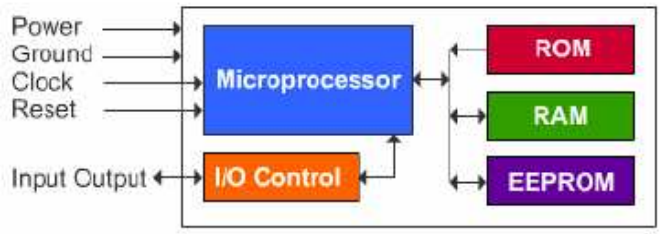


Figura 2.10: Esquema en bloques de las partes internas una tarjeta SIM

El sistema de microprocesamiento de la tarjeta SIM, puede ejecutar programas instalados por el proveedor de servicios, esto es posible vía *SIM Aplication Toolkit* (SAT) interfaz especificada en los estándares GSM; con esta interfaz los programas sobre la SIM pueden acceder a funcionalidades del teléfono celular, se podría añadir iconos o menús.

2.1.3.2 Mecanismos de Seguridad

La tecnología GSM define dos procedimientos, en los que interviene la tarjeta SIM, implementando mecanismos de seguridad; éstos son:

a. Autenticación del usuario, dentro de esta área se identifican dos formas de autenticación, la primera local y la segunda ante la red.

1. Autenticación local, se refiere a cómo el usuario se autentica ante el Teléfono Celular utilizando los mecanismos de seguridad de la tarjeta SIM, para lo cual el usuario tiene que ingresar a través del *Keypad*, los códigos PIN (*Personal Identification Number*) ó PUK (*Personal Unlocking Key)* y así autenticarse, desbloquear y obtener la información almacenada en la tarjeta SIM, cabe resaltar que estos mecanismos de seguridad deben ser previamente habilitados por el usuario.

   Para la utilización de estos códigos se debe tener presente lo siguiente:

   - El código PIN bloquea la tarjeta SIM hasta que el código correcto es introducido; puede existir dos códigos PIN (PIN1 y PIN2).

- Cada Operador de Telefonía Móvil, fija el PIN en un número predeterminado estándar, el cual puede ser modificado por el usuario.
- El código PUK es brindado por el Operador.
- Se tienen tres intentos para introducir el código PIN; después de estos intentos se tiene que usar obligatoriamente el código PUK, para desbloquear la Tarjeta SIM.
- El introducir el código PUK correctamente, restablece el contador para introducir el código PIN.
- Después de 10 intentos erróneos de introducir el código PUK, se bloquea la SIM de manera permanente.
- Se puede introducir la Tarjeta SIM en otra Estación Móvil, y los códigos PIN y PUK siguen habilitados.
- Varios modelos de teléfonos celulares utilizan los códigos PIN y PUK como mecanismos de seguridad al momento de ingresar a la información contenida tanto en el Equipo Móvil y la tarjeta SIM.

2. Autenticación con la red, se trata de la habilidad que tiene el teléfono celular de demostrar que tiene acceso a usar los recursos de la Red de Telefonía Móvil, para lo cual utiliza:

   - IMSI (*International Mobile Subscriber Identity*), es un número único de 15 dígitos decimales, almacenado en la tarjeta SIM, para cada suscriptor en el mundo, el cual especifica en sus 5 o 6 primeros dígitos el País y la Operadora del usuario.
   - Clave secreta Ki, es una clave individual por usuario de 128 bits, la cual es almacenada en el AuC y de manera especial en la tarjeta SIM, previniendo que ésta pueda ser leída directamente a través del Equipo Móvil.

- Algoritmo de Cifrado A3, utilizado en el proceso de autenticación.

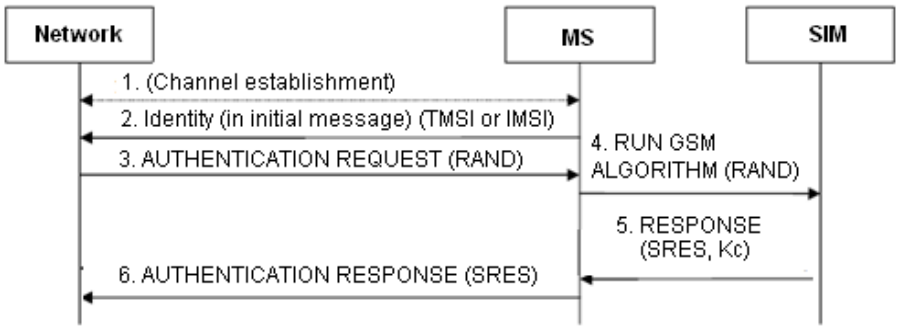


Figura 2. 11: Procedimiento de Autenticación del usuario con la Red Celular.

El proceso de autenticación como se puede apreciar en la Figura 2.11, comienza cuando se establece la conexión, seguida por el envio del IMSI por la Estación Móvil a la Red, la cual contesta con un número aleatorio (RAND), después de lo cual la Tarjeta SIM procesa este número RAND y conjuntamente con la Ki pasan por el Algoritmo A3 y se genera la respuesta de la autenticación (SRES) como muestra la Figura 2.12.

Ya que tanto la Ki, el Algoritmo de cifrado A3 y el RAND son conocidos por la Red se puede descifrar el SRES y así autenticar al usuario dentro de la Red.

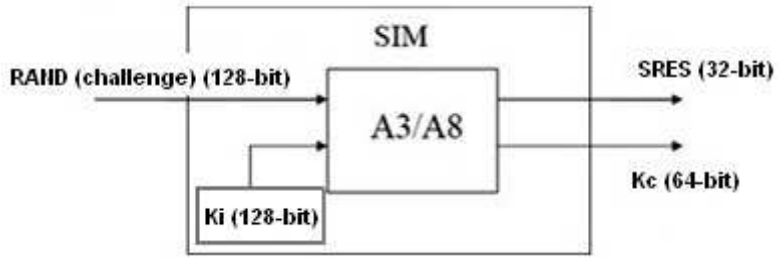


Figura 2. 12: Creación de la respuesta de autenticación

b. Confidencialidad de datos y señalización: se requiere que la señalización y los datos de usuario (tales como mensajes de texto y voz) sean protegidos

contra la interceptación y escuchas no autorizadas, lo cual se realiza con el cifrado de la información del usuario, para lo cual se utiliza:

- Algoritmo de Cifrado A8, el cual es utilizado para generar la clave cifrada Kc.

- Clave cifrada (Kc,C*ipher Key*), utilizada para dar confidencialidad a la información del usuario.

- Algoritmos de Cifrado A5, diferentes algoritmos de cifrado se encuentran en las especificaciones de GSM, éstos son los llamados A5/0 algoritmo de no cifrado, A5/1 algoritmo A5 original usado en Europa, A5/2 algoritmo de cifrado débil, A5/3 algoritmo de cifrado fuerte creado como parte del proyecto de tercera generación (3GPP, 3rd *Generation Partnership Project*); durante el establecimiento de una conexión la Estación Móvil informa a la red cuáles algoritmos soporta.

  Para el proceso de confidencialidad de datos y señalización primero se calcula la Clave cifrada Kc con la utilización de la Ki, el número RAND y el Algoritmo A8, como los muestra la Figura 2.13, luego la Kc y el número de trama se usan como entradas al Algoritmo de Cifrado A5 para luego pasar por una operación XOR conjuntamente con los datos del usuario y de ahí se transmiten a la interfaz de aire los datos del usuario cifrados.

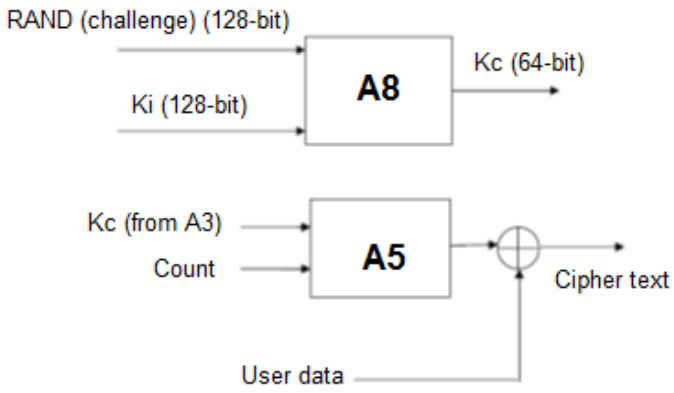


Figura 2. 13: Algoritmos de Cifrado A8 y A5

Debido a que la Ki, el número RAND y los Algoritmos de Cifrado son conocidos por la Red y la Estación Móvil o teléfono celular se puede cifrar y descifrar los datos intercambiado por la Estación Móvil y la Red, manteniendo la confidencialidad de datos y señalización del usuario.

Dentro de la Tarjeta SIM todas las medidas necesarias son tomadas para garantizar que los algoritmos A3, A5, A8 y la clave de autenticación del suscriptor (Ki) no puedan ser leídos, modificados, manipulados o anulados de tal manera que revelen información secreta, además todos los procesos que requieren el uso de la clave de autenticación de usuario serán realizados internamente por el SIM.

Los códigos de seguridad relacionados con el suscriptor podrían ser mantenidos dentro del ME durante la ejecución, usando una interfaz SIM/ME apropiada, pero deben ser eliminados del ME inmediatamente después de la finalización del procedimiento.

Pero, en realidad, un ME puede retener los datos de seguridad menos críticos cuando se remueve la tarjeta SIM o se desconecta el equipo móvil. Estos datos, cuando se almacena en el ME, sólo podrán leerse o recuperarse si la misma tarjeta SIM es reactivada.

2.1.3.3 Sistema de Archivos

El sistema de archivos de la Tarjeta SIM reside en la memoria permanente y está estructurado jerárquicamente. Dispone de tres componentes principales que son: el Archivo Principal MF (*Master File*) o la raíz del sistema de archivos, los Archivos Dedicados DF (*Dedicated Files*) que sirven como directorios, y los Archivos Elementales EF (*Elementary Files*) que almacenan los datos.

Dentro de la memoria el espacio es limitado por tal razón los archivos no son identificados por el nombre, aunque el estándar los asigna, sino por 4 dígitos hexadecimales que tienen una extensión de 2 bytes; por ejemplo el directorio principal se identifica por el código 0x3F00, el archivo que contiene el IMSI es identificado vía el código 0x6F07, entre otros.

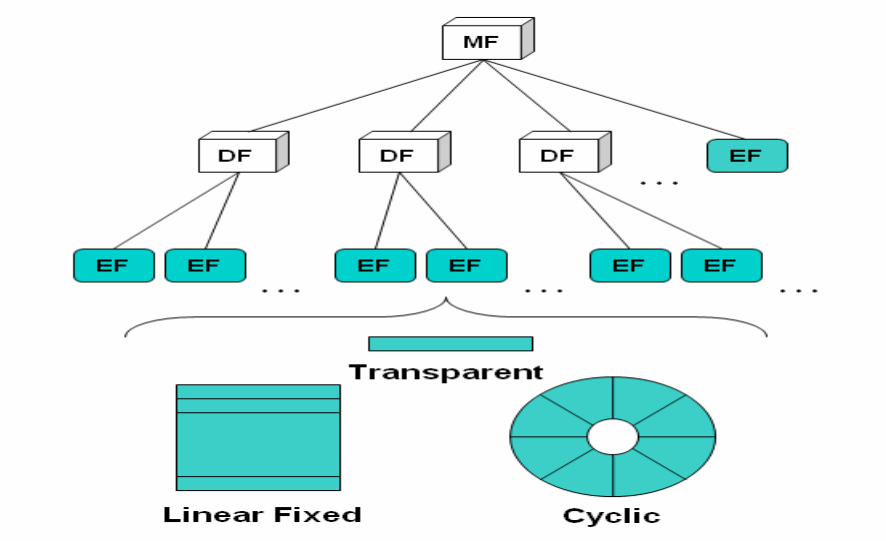


Figura 2.14: Sistemas de Archivos y formas de los archivos elementales [19]

Los Archivos Elementales pueden almacenar sus datos en tres formatos: primero como una secuencia de bytes que forman un registro (Formato Transparente), segundo como un arreglo unidimensional de registros (Formato Linear) y por último una cola de registros último en entrar primero en salir (Formato Cíclico).

Por ejemplo, el registro que contiene el IMSI se almacena en Formato Transparente, los registros telefónicos en Formato Linear, y el archivo que almacena los últimos números llamados en Formato Cíclico.

Diferentes atributos se usan para el acceso, con la finalidad de proteger los archivos de la tarjeta SIM; con estos atributos el fabricante puede controlar si un archivo puede ser leído ó escrito cuando se accede a través del Equipo Móvil a la tarjeta SIM; el mismo concepto de atributos permite a los Operadores, cambiar los archivos enviando mensajes especiales.

El Equipo Móvil puede acceder a la tarjeta SIM solamente si el usuario ingresa el código PIN cuando el teléfono es encendido; pero muchas veces los Operadores desactivan este mecanismo de seguridad.

Para la comunicación entre el Equipo Móvil y la Tarjeta SIM existen comandos y respuestas que han sido especificados en GSM, los cuales en general se los

conoce como APDU (*Application Protocol Data Units*), y dependiendo de su función llamados APDU comando y APDU respuesta.

La tarjeta SIM tiene un rol pasivo en esta comunicación, solo puede enviar respuestas si existe una petición previa hecha por el Equipo Móvil, y el acceso es permitido para lo cual la Tarjeta SIM responde con uno o más APDU dependiendo del comando enviado.

El APDU comando en su estructura contiene un *Header* y un *Body*. La cabecera tiene los campos CLA, INS, P1, P2y P3.

CLA es la clase de instrucción (la cual es siempre 0xA0 para GSM), el campo INS es el identificador del comando a ser ejecutado, los campos P1 y P2 usados para parámetros adicionales del comando y P3 contiene la longitud del campo de datos a ser escritos en la tarjeta SIM. La Figura 2.15 muestra la estructura de un APDU Comando.

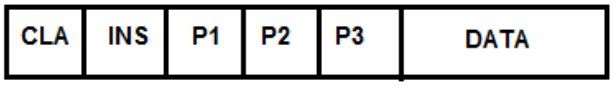


Figura 2.15: Estructura APDU Comando [18]

La estructura del APDU respuesta se puede observar en la Figura 2.16, formado por el *Body* y el *Trailer*. El *Trailer* contiene dos campos llamados SW1 y SW2, estos campos son utilizados por la tarjeta SIM para informar al equipo móvil si el comando fue ejecutado correctamente o se generó un error.

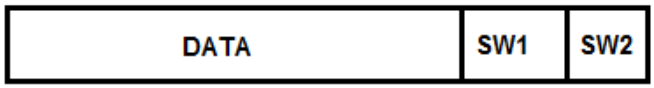


Figura 2.16: Estructura APDU Respuesta [18]

Las normas GSM definen varios DF importantes que son subordinados del MF, éstos son: DFGSM, DFDCS1800 [29] y DFTELECOM, y varios EF que son subordinados y obligatorios para todas las Operadoras de Telefonía Móvil.

[29] *Digital (DCS, Digital Cellular System)* es una variante de la norma GSM que utiliza la frecuencia de 1800 MHz.

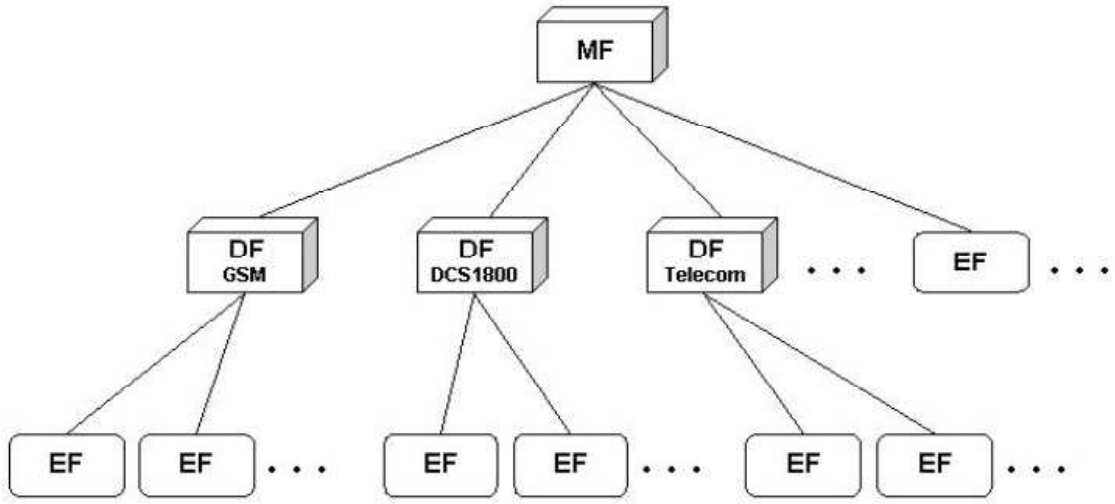


Figura 2.17: Estructura jerárquica de archivos dedicados estandarizados [19]

Los EFs debajo de DFGSM y DFDCS1800 contienen principalmente información relacionada con las diferentes bandas de frecuencia para la operación de la Red Celular. Los EFs subordinados del DFTELECOM contienen información relacionada con los servicios que ofrece la Red. La Figura 2.17 muestra la ubicación de estos archivos.

Aunque el sistema de archivos de la tarjeta SIM es altamente estandarizado, las normas permiten flexibilidad, tal que su contenido puede variar entre los Operadores de Redes.

Por ejemplo, un Operador de Red no puede utilizar un elemento opcional del sistema de archivos, pero puede crear un elemento adicional en la tarjeta SIM para su uso en sus operaciones, o puede instalar una función integrada para proporcionar un servicio especializado.

2.1.3.4 Evidencia digital potencial en la Tarjeta SIM

La tarjeta SIM que físicamente constituye evidencia electrónica, almacena información que debe ser discriminada por el examinador o analista forense, con el objeto de encontrar evidencia digital potencial.

A breves rasgos la tarjeta SIM es una tarjeta inteligente que contiene un procesador y una memoria. En los teléfonos celulares, la tarjeta SIM se utiliza

como dispositivo de almacenamiento de datos del suscriptor. El procesador se utiliza para implementar los mecanismos de acceso a la red y las características de seguridad.

El nombre del proveedor del servicio está usualmente visible, acompañado de un número único que puede ser usado para conseguir información del proveedor, tal como nombre, dirección y número asociado con la tarjeta SIM.

Las tarjetas SIM pueden ser protegidas para el acceso por el código PIN, conocido también como CHV (*Chip Holder Verification*) y en algunos casos tienen dos códigos PIN que pueden ser habilitados o deshabilitados por el usuario, lo que se convierte en un problema al extraer la evidencia digital dependiendo de la técnica utilizada.

El código PIN es usualmente requerido para acceder a la tarjeta SIM, como fue antes mencionado si un usuario falla al ingresar el código PIN por tres intentos, la tarjeta SIM se bloquea y un código de 8 dígitos llamado PUK debe ser introducido, se tiene ahora 10 intentos para introducir el código PUK válido antes de que la tarjeta SIM quede permanentemente deshabilitada.

Una buena noticia para el analista forense es que el código PUK no puede ser cambiado por el usuario; este código es proporcionado por el Operador de la Red, por lo tanto, una analista forense puede ingresar a la tarjeta SIM manteniendo un contacto con el proveedor de la Red.

Varios tipos de evidencia digital pueden existir en los Archivos Elementales (EF) ubicados en archivos dispersos por todo el sistema, que a su vez son identificadores del suscriptor en la red.

Se puede acceder a la tarjeta SIM colocándola en un lector de tarjetas inteligentes, el análisis posterior se haría en base a la imagen obtenida del equipo celular. Se debe tener cuidado en todo momento para garantizar que el contenido de la tarjeta SIM no se altere de ninguna manera. La Tabla 2.4 muestra los elementos evidencia digital útil para el examinador forense.

El IMSI es el número de identificación del suscriptor que permitirá conjuntamente con el proveedor identificar al cliente que compró el teléfono celular.

Categoría	EF	Descripción
INFORMACIÓN RELACIONADA CON LOS SERVICIOS	**ICCID**	***Integrated Circuit Card Identifier***, Identificador Integrado de la tarjeta de circuitos, es un identificador numérico único para la tarjeta SIM que puede ser de hasta 20 dígitos. Se trata de un prefijo identificador (89 para las telecomunicaciones), seguido de un código de país, un número de identificación del emisor, y un número de identificación de cuenta individual. Aparte de los prefijos, los componentes de un ICCID son variables.
	IMSI	***International Mobile Subscriber Identity*****,** Identificador Internacional del Suscriptor Móvil, es un único número de 15 dígitos asignado al abonado. Su estructura es similar a la del ICCID, tiene un código de país MCC (*Mobile Country Code*), un código de red móvil MNC (*Mobile Network Code*), y un Número de Identificación del suscriptor móvil MSIN (*Mobile Subscriber Identity Number*). El MCC es de 3 dígitos, el MNC puede ser de 2 o 3 dígitos, y el MSIN asignado por el operador ocupa el resto.
	MSISDN	***Mobile Station International Subscriber Directory Number***, Número Telefónico Internacional del Suscriptor y la Estación Móvil, tiene por objeto expresar el número de teléfono asignado al suscriptor para la recepción de llamadas en el teléfono, pero es actualizable por el suscriptor, a diferencia de la ICCID y el IMSI, el MSISDN es una EF opcional.
	SPN	***Service Provider Name*****,** Nombre del Proveedor de Servicios**,** es una EF opcional que contiene el nombre del proveedor de servicios. Si está presente, sólo puede actualizarse por el administrador u operador de servicios.
	SDN	***Service Dialling Numbers*** es un EF opcional que contiene los números de servicios especiales, tales como atención al cliente.
	EXT3	***Extension3*** es un EF que contiene datos adicionales sobre las entradas SDN.

INFORMACIÓN DE DIRECTORIO TELEFÓNICO Y LLAMADAS	**ADN**	***Abbreviated Dialling Numbers***, los números de marcación abreviada, EF que conserva una lista de nombres y números de teléfono introducido por el suscriptor. El tipo de número TON (*Type Of Number*) y la identificación de plan de numeración NPI (*Numbering Plan Identification*) también se mantienen en este EF. También puede tener un índice a un registro de EXT1 EF de datos de desbordamiento.
	LND	***Last Numbers Dialled***, Últimos Números Marcados, EF que contiene una lista de los números de teléfono recientemente llamados por el dispositivo. Un nombre del directorio telefónico también puede estar asociado y se almacena con el número llamado. También tiene un índice a un registro de EXT1 EF de datos de desbordamiento.
	EXT1	***Extension1***, registro de EFs, se utiliza para mantener un desbordamiento de dígitos para EFs tales como ADN, LND, y otras entradas.
	FDN	***Fixed Dialling Numbers*****,** Números de Marcación Fija, es similar al ADN, contiene una lista de nombres y números de teléfono, pero se restringe a marcar los números prescritos en la tarjeta SIM. Si la capacidad de almacenamiento del FDN no es suficiente para contener la información de una entrada, se puede utilizar un índice a un registro de Extension2 (EXT2) EF utilizado para almacenar datos de desbordamiento.
	EXT2	***Extension2***, es un registro de EFs usado para mantener cifras de desbordamiento de FDN y otras entradas.
INFORMACIÓN DE LOCALIZACIÓN	**LOCI**	***Location Information***, información de localización, EF que contiene información del Área de Localización LAI (*Location Area Information*) para comunicaciones de voz. El LAI está compuesto por el MCC y MNC de la zona de ubicación y el código de área de localización LAC (*Location Area Code*).

	LOCI GPRS	**GPRS Location Information**, GPRS Información de Localización, EF que contiene información del área de enrutamiento RAI (*Routing Area Information*) para las comunicaciones de datos a través de *General Packet Radio Service* (GPRS). El RAI está compuesto por el MCC y MNC de la zona de enrutamiento y el LAC, así como un código de área de enrutamiento RAC (*Routing Area Code*), un identificador del área de enrutamiento dentro del LAC.
INFORMACIÓN DE MENSAJES	**SMS**	***Short Message Service***, servicio de mensaje corto, EF que contiene el texto y los parámetros asociados para los mensajes recibidos y enviados a la red. Las entradas de SMS contienen texto e información de encabezado, como la hora en que fue recibido un mensaje o fue enviado según lo registrado por la red de telefonía móvil, el número de teléfono del remitente, la dirección del centro SMS, y el estado de la entrada. El estado de una entrada puede ser designado como el espacio desocupado libre u ocupado por un mensaje recibido para ser leído, un mensaje recibido que ha sido leído, un mensaje de salida para ser enviado, o un mensaje de salida que se ha enviado. Los mensajes eliminados son generalmente marcados como espacio libre y puede estar sin cambios en la tarjeta SIM hasta que sobrescriba en su espacio.

Tabla 2.4: EFs que contienen evidencia digital de la tarjeta SIM

El LAI es un identificador de la localización actual del teléfono celular, este valor es retenido por la tarjeta SIM cuando el teléfono celular es apagado; esta información en ciertos casos es útil para determinar la localización en la cual se utilizó por última vez el teléfono celular, cuando éste se encontraba operando.

En mensajes de texto, normalmente hay un espacio en la tarjeta SIM donde se muestran los últimos 12 mensajes de texto que fueron enviados; tener en cuenta, que existe la posibilidad de guardarlos en la memoria interna del equipo móvil.

Una configuración por defecto del teléfono celular permite almacenar todos los mensajes entrantes y salientes en la tarjeta SIM, y se puede cambiar por petición del usuario. La mayoría de los teléfonos celulares usa primero la memoria SIM antes de la memoria interna del equipo móvil.

Cada una de las ranuras para mensajes de texto almacenados en la tarjeta SIM tiene la estructura de 1 byte para el estado y de 2 a 176 bytes para el PDU.

Los bytes de estado pueden ser:

00000000	No usado
00000001	Mensaje leído
00000011	Mensaje no leído
00000101	Mensaje enviado
00000111	Mensaje no enviado

Tabla 2.5: Bytes de Estado

En mensajes eliminados, el primer byte se establece en cero, esto significa que los mensajes eliminados pueden ser recuperados a excepción del primer byte, siempre y cuando un nuevo mensaje no sea sobrescrito sobre los antiguos mensajes.

No se pueden recuperar porciones de mensajes en los *slots* de memoria, ya que cuando un mensaje ocupa la ranura, el espacio que no haya sido ocupado por este nuevo mensaje dentro de la ranura es llenado con 0xFF.

El PDU consiste de los siguientes elementos:

- El MSISDN del centro de servicio
- El MSISDN del suscriptor que envía o recibe el mensaje, depende de la SIM analizada

- Día y fecha de recepción del mensaje
- Información del directorio telefónico
- El mensaje propiamente dicho

El mensaje propiamente dicho puede ser codificado el esquema común que es GSM-7 bits, es decir, 7 bits por caracter; estos bits son transformados en una secuencia y luego arreglados en bytes para almacenar en la tarjeta SIM, es por esta razón que al ser recuperados no pueden ser leídos usando un editor hexadecimal normal.

En relación al directorio telefónico y a los números de marcación abreviada de los Archivos Elementales ADN y FDN, la mayoría de los teléfonos tienen la capacidad de almacenar cerca de 100 números marcados y dependiendo del directorio telefónico con un nombre asociado.

El último número marcado del teléfono celular se encuentra almacenado en el Archivo Elemental LND; se debe considerar que la mayoría de Tarjetas SIM sólo almacenan 5 de los últimos números telefónicos marcados del teléfono celular, y los demás se almacenan en la memoria interna del mismo dependiendo del modelo.

2.2 TÉCNICAS DE ANÁLISIS FÍSICO Y LÓGICO PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL DE TELÉFONOS CELULARES

Se pueden definir dos técnicas con las cuales se puede extraer evidencia digital de un teléfono celular, la una mediante un análisis físico y la otra empleando un análisis lógico.

El análisis físico implica una copia bit a bit de una entrada física de almacenamiento (chip de memoria); mientras que el análisis lógico implica una copia bit a bit de los objetos lógicos (archivos) que residen sobre un almacenamiento lógico (partición de archivos del sistema).

La diferencia radica, entre una memoria vista como un proceso, mediante la instalación de un sistema operativo (punto de vista lógico), versus una memoria formada por un procesador y otros componentes relacionados con el *hardware* (punto de vista físico).

Las técnicas de extracción física tienen ventajas sobre las técnicas de extracción lógica, ya que permiten analizar archivos eliminados y algunas porciones de archivos (por ejemplo, la memoria sin asignar del sistema), que de otra manera no se lo haría.

Extraer evidencia digital del dispositivo a ser analizado, así como descifrar y traducir para descubrir los datos actuales, es un trabajo tedioso y requiere mucho tiempo para ser llevado a cabo manualmente.

Figura 2.18: Pirámide de niveles de análisis de teléfonos celulares

El contenido obtenido de un análisis físico del dispositivo, se puede importar en una herramienta para automatizar el examen y presentar informes; sin embargo, sólo hay unas pocas herramientas disponibles actualmente.

Una adquisición lógica, aunque más limitada que una adquisición física, tiene la ventaja de que las estructuras de datos del sistema son normalmente más fáciles de extraer por una herramienta y ofrece una organización más natural para entender y utilizar los elementos adquiridos.

De ser posible se recomienda hacer los dos tipos de adquisición, aunque es preferible una adquisición física antes de una adquisición lógica.

Existen niveles de análisis como una división de las técnicas de análisis físico y lógico ya descritos, los cuales proponen una metodología más técnica y que va de acuerdo con un análisis forense; al mismo tiempo necesita de personal capacitado para poder aplicar estos niveles, éstos se pueden apreciar en la Figura 2.18, la cual muestra una pirámide en la que se representan los diferentes niveles de análisis que se pueden aplicar.

2.2.1 TÉCNICAS DE ANÁLISIS LÓGICO PARA LA EXTRACCIÓN DE LA EVIDENCIA DIGITAL

Las técnicas de análisis lógico generalmente implican utilización de *software* para romper o eludir los mecanismos de autenticación, y así obtener información almacenada. Mientras algunas técnicas de uso general pueden aplicarse a una clase de teléfonos móviles, la mayoría de las técnicas se especializan para un modelo específico dentro de una clase.

Cuando una técnica especializada se desarrolla, normalmente es programada y probada en un dispositivo de ensayo. Las técnicas de análisis lógico realizan lo siguiente:

a. Explotar las debilidades conocidas en la autenticación: si un mecanismo de autenticación es débil, es posible aprovecharse de estas debilidades para ingresar al sistema de archivos.

   Algunos dispositivos permiten intentos ilimitados de autenticación sin ser cancelados, lo que permite un ataque de contraseñas de uso común; también existen dispositivos que pueden tener una contraseña de reserva o contraseña maestra en el mecanismo de autenticación, lo que permite el acceso sin restricciones, sin pasar por el bloqueo del teléfono establecido por el usuario.

   Por ejemplo, el código de seguridad maestro para reemplazar el mecanismo de bloqueo del teléfono en ciertos teléfonos Nokia se puede calcular directamente desde el equipo.

Algunos teléfonos móviles GSM permiten el análisis lógico, a pesar que el código PIN esté habilitado, y si esto no funciona existe la posibilidad de crear un sustituto de la tarjeta SIM para ciertos modelos de teléfonos y así permitir el acceso al Equipo Móvil.

b. **Acceder a través de una puerta trasera (*backdoor*):** Los fabricantes a menudo suelen construir un *test* de ensayo u otro *software* de *backdoor* que el examinador puede aprovechar para obtener información.

   Se debe considerar que muchos fabricantes no permiten el uso de protocolos de diagnóstico y depuración, que no pasan por el mecanismo de autenticación, para obtener información del teléfono celular.

   La exploración del contenido de la memoria puede revelar información de autenticación, tales como contraseñas del teléfono celular. Algunas aplicaciones de *software*, en algunos teléfonos móviles soportan funciones, que permiten la lectura de la memoria.

   Por ejemplo, algunos modelos de teléfonos inteligentes soportan una aplicación llamada *parrot*, llamada así por el ave que aparece en la pantalla. Cuando se dispara una combinación de claves específicas y se proporcionan comandos apropiados a través del puerto serial, la aplicación devuelve el contenido de la memoria o lo copia en una tarjeta de memoria externa.

c. **Explotar las vulnerabilidades conocidas del sistema:** Los sistemas móviles pueden poseer las vulnerabilidades del sistema dentro de un protocolo de interfaz estándar, que un examinador puede aprovechar para eludir la autenticación y obtener acceso a la información.

   Por ejemplo, el acceso al dispositivo puede ser posible a través de una red defectuosa de servicios, una falla en un protocolo de red estándar compatible con el dispositivo, o un error en la aplicación del protocolo que lo hace susceptible a un método de ataque. Interfaces de comunicación posibles para

la explotación incluyen la interfaz serial, *USB, IrDA, Bluetooth, WiFi* y GSM/GPRS.

Dentro de las técnicas de análisis lógico de teléfonos móviles, se tiene ya sea la extracción manual o la extracción lógica de los datos que se llevarán a cabo por los examinadores forenses.

La extracción lógica del teléfono celular se utiliza cuando el dispositivo es compatible con uno o más elementos de *software* forense y la extracción manual generalmente es necesaria cuando no existe el *software* compatible.

La extracción lógica de la tarjeta SIM se utiliza cuando el teléfono móvil es compatible con un elemento o más de *software* forense. Una verificación manual también puede ser requerida para confirmar que los datos extraídos son completos y correctos.

Cualquiera que sea la técnica de análisis lógico utilizada se debe tratar de obtener los elementos citados como evidencia digital potencial, tanto de la tarjeta SIM como del Equipo Móvil.

2.2.1.1 Extracción Manual

Generalmente se utiliza cuando no se encuentra elementos compatibles para la extracción de la evidencia, y debe ser utilizada como último recurso ya que con esta técnica el analista corre el riesgo de cambiar la información. Se utiliza por lo general en teléfonos fabricados recientemente, en los que los fabricantes de herramientas forenses no tienen la actualización para soportar estos teléfonos celulares.

Esta técnica de análisis requiere que los examinadores forenses realicen una grabación de cada una de las pantallas que se van mostrando al momento del análisis, usando el *Keypad* y los menús del teléfono celular; esto también podría incluir una grabación de audio, y así producir un reporte con todo el material grabado, por ejemplo el IMEI en la mayoría de teléfonos celulares puede ser mostrado en pantalla digitando *#06#.

El personal responsable debe estar familiarizado con el tipo de teléfono en particular a ser analizado para no cometer errores. Se requerirá el conocimiento de manuales descargados del portal del fabricante; si esto no se realiza se corre el riesgo de presionar botones equivocados y eliminar evidencia.

2.2.1.1.1 Ventajas

- Es rápido
- Se puede realizar en la mayoría de dispositivos, mientras se tenga conocimiento
- No se requiere cables
- Fácil de usar

2.2.1.1.2 Desventajas

- No se adquieren todos los datos y tampoco los datos borrados.
- Es propenso a errores
- Barrera de idiomas
- Si el teclado está dañado no se puede realizar
- Desperdicio de tiempo

2.2.1.2 Extracción Lógica

En general, usa protocolos propietarios de los fabricantes, con modificaciones para el no intercambio de información y se basa solo en la lectura de datos; los teléfonos móviles requieren cables y controladores para establecer una conexión, complicando aún más el proceso de adquisición.

Sistemas operativos propietarios requieren el uso de métodos de adquisición potencialmente inseguros porque el acceso directo a la memoria del teléfono móvil es limitada, lo que impide que se aplique un punto de vista forense al

duplicar la unidad como un disco duro normal de una computadora de escritorio o portátil.

Usando el sistema operativo del teléfono para adquirir datos desde el teléfono significa que la memoria está siempre activa y siempre cambiante, esto puede dar lugar a incoherencias en la adquisición de los Códigos *Hash* de la memoria del teléfono utilizado para proteger y validar la evidencia digital.

Los comandos AT[30], *Sync* ML, y otros protocolos mencionados son de uso común en la extracción lógica de teléfonos celulares, como se muestra en la Figura 2.19. Debido a que los teléfonos pueden soportar múltiples protocolos, una herramienta puede emplear varios de ellos en la sucesión de adquirir la más amplia variedad de datos disponibles. Incluso si una herramienta utiliza varios protocolos para un teléfono particular, todos los datos disponibles no pueden ser recuperados.

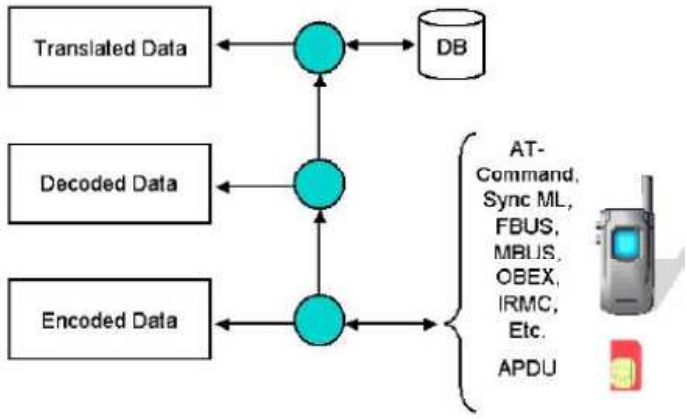


Figura 2.19: Adquisición de datos, decodificación y traducción [19]

Diferentes herramientas, pueden utilizar diferentes protocolos, para adquirir el mismo dato. La tabla 2.6 ilustra los protocolos de intercambio utilizados por diferentes herramientas para adquirir el IMEI de un teléfono celular Nokia 6101.

La primera herramienta enlistada usa los comandos AT estandarizados, mientras que las otras dos herramientas usan protocolos propietarios.

[30] *Los comandos AT,* son instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal modem. Aunque la finalidad principal de los comandos AT es la comunicación con *modems*, la telefonía móvil GSM también ha adoptado como estándar este lenguaje para poder comunicarse con sus terminales. De esta forma, todos los teléfonos móviles GSM poseen un juego de comandos AT específico que sirve de interfaz para configurar y proporcionar instrucciones a los terminales.

Mientras muchos de los protocolos son estandarizados y de conocimiento público, algunos tales como el MBUS y el FBUS[31] son propietarios de Nokia. Incluso protocolos estandarizados a menudo incluyen extensiones de fabricante o variantes.

Herramienta	Solicitud/Respuesta (Hex)	Solicitud/Respuesta (ASCII)
GSM.XRY	41 54 2B 43 47 53 4E 0D	A T + C G S N
	0D 0A 33 35 36 36 36 31 30 30 35 37 30 34 30 39 32 0D 0A 0D 0A 4F 4B 0D 0A	. . 3 5 6 6 6 1 0 0 5 7 0 4 0 9 2 . . . . O K . .
Phone Base	1E 00 0C 7F 00 02 D2 01 C0 7C 1E 00 10 1B 00 07 00 01 00 00 41 01 41 00 0E 1C	. . . . . Ò . À | . . . . A . A . . .
	1E 10 00 7F 00 02 1B 01 05 6C 1E 10 00 1B 00 1C 01 39 00 01 00 01 41 14 00 10 33 35 36 36 36 31 30 30 35 37 30 34 30 39 32 00 01 42 5B 50	. . . . l . . . . 9 . . . . A . . . 3 5 6 6 6 1 0 0 5 7 0 4 0 9 2 . . B [P
Secure View	55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 551E 00 10 1B 00 07 00 04 00 00 41 01 60 00 2F 19	U U U U U U U U U U U U U U U U U U U U U U U U U U U U …. . . . . A . ` . / .
	1E 10 00 7F 00 02 1B 00 05 6D 1E 10 00 1B 00 1C 04 39 00 01 00 01 41 14 00 10 33 35 36 36 36 31 30 30 35 37 30 34 30 39 32 00 01 45 5E 57	. . . . m . . . . 9 . . . . A . . . 3 5 6 6 6 1 0 0 5 7 0 4 0 9 2 . . E ^ W

Tabla 2.6: Ejemplo de Adquisición del IMEI [19]

La tarjeta SIM sigue normas a diferencia de los Equipos Móviles y el protocolo de aplicación de datos de la unidad APDU (*Application Protocol Data Unit*) es el protocolo de interfaz que se utiliza para la comunicación entre el Equipo Móvil y la Tarjeta SIM.

[31] MBUS/*FBUS*, es una norma ANSI/IEEE de bus de datos, orientado a placas de circuitos y teléfonos celulares. La norma específica una forma de varias piezas de *hardware* electrónico para comunicarse, generalmente una pieza actúa como maestro (envía una petición), y otro que actúa como esclavo (envía una respuesta).

Los datos adquiridos lógicamente desde un teléfono o SIM están a menudo codificados de una manera poco convencional, tal como con el texto representado en el alfabeto GSM de 7 bits, y difícil de interpretar.

Otras codificaciones que se pueden encontrar incluyen código binario decimal (BCD, *Binary Coded Decimal*) y Unicode. Para facilitar la interpretación, la mayoría de herramientas descifran los datos del operador, como se ilustra en la Figura 2.19.

Algunas herramientas van un paso más allá y, en su caso, descifran los datos como los códigos numéricos que representan un país y un operador de red, en las formas más significativas como nombres del país y el operador de red, utilizando una base de datos.

La característica más importante de una herramienta forense es su capacidad para mantener la integridad de la fuente de datos original que es adquirida y también la de los datos extraídos.

Lo primero se realiza mediante el bloqueo o la eliminación de las solicitudes de escritura para el dispositivo que contiene los datos. La segunda se realiza mediante el cálculo de un *hash* criptográfico de los volúmenes de archivos de evidencia creado, y verificando recurrentemente que este valor permanece inalterado a lo largo de la vida de esos archivos.

Preservar la integridad no sólo mantiene la credibilidad de un punto de vista jurídico, sino que también permite que cualquier investigación posterior pueda utilizar la misma línea base para replicar el análisis.

2.1.1.1.1 Ventajas

- Rápido
- Fácil de usar
- Bloques de información para la investigación
- Soporte de varios idiomas

- Reportes en formato estándar
- Repetible

2.1.1.1.2 Desventajas

- Datos pueden ser escritos en el Equipo Móvil
- Acceso a los registros de archivos (limitado)
- Necesita comprensión por parte del usuario final
- Se puede no disponer de todos los cables
- Se pueden borrar archivos

2.2.2 TÉCNICAS DE ANÁLISIS FÍSICO PARA LA EXTRACCIÓN DE LA EVIDENCIA DIGITAL

Son técnicas de análisis que incluyen una combinación de *software* y *hardware* para romper o eludir los mecanismos de autenticación y así obtener acceso e información del dispositivo.

Por ejemplo, el valor de un código de autenticación del teléfono celular puede ser fácilmente recuperado de un volcado de memoria, admitido en ciertos modelos de teléfonos celulares, lo que permite que posteriormente se realice el análisis lógico.

Pocos métodos de propósito general se aplican a una clase general de teléfono móvil. La mayoría de las técnicas de análisis físico son especializadas para un modelo específico dentro de una clase.

Al igual que con las técnicas de análisis lógico, cuando una técnica especializada se desarrolla, ésta es probada en un dispositivo de ensayo. En esta técnica el analista forense se debe apoyar en las especificaciones técnicas facilitadas por el fabricante del teléfono celular, que puede proporcionar información útil para la extracción de datos.

Las técnicas de análisis físico basadas en *hardware* realizan:

a. **Obtener acceso a través de una puerta trasera (*backdoor*) de *hardware***: Está constituido por interfaces usadas por el fabricante para la depuración y pruebas de producción o mantenimiento, las cuales se pueden utilizar para acceder a la memoria del teléfono celular.

   Por ejemplo algunos teléfonos móviles tienen activos puntos de prueba de *hardware* en la placa de circuitos que se pueden utilizan para probar el dispositivo.

   Los teléfonos celulares en la actualidad son compatibles con el estándar JTAG (*Joint Test Action Group*) nombre común del estándar *IEEE 1149.2 Test Access Port and Boundary-Scan Architecture*, concebido para realizar pruebas de las placas de circuitos impresos usando *Boundary Scan*[32]*.*

   JTAG define una interfaz de prueba común para el procesador, la memoria, y otros chips integrados, en sus teléfonos celulares.

   Los examinadores forenses pueden comunicarse con un componente de JTAG compatible mediante la utilización de *software* y *hardware,* a través de un dispositivo programador con un propósito especial e independiente para los puntos de prueba.

   La unidad de prueba JTAG puede enviar comandos y datos para los componentes JTAG compatibles además de devolver los resultados a la unidad para el almacenamiento y entrega.

   JTAG da a los especialistas forenses otra vía para obtener información de teléfonos celulares bloqueados o con daños menores y que no pueden ser conectados de otra manera.

b. **Examinar la memoria, independiente del dispositivo:** Un analista forense experimentado puede ser capaz de examinar los chips de memoria, de forma directa en el dispositivo o desoldando sus componentes y así extraer evidencia.

[32] *Boundary Scan es* un método para probar las interconexiones sobre placas de circuitos impresos o sub-bloques dentro de un circuito integrado. Es también ampliamente usado como un método para depuración del estado de los pines de circuitos integrados.

Por ejemplo, el Instituto Forense de los Países Bajos ha desarrollado una herramienta de propósito general para examinar una amplia gama de chips de memoria.

Una vez conectado físicamente a la placa de circuitos, la herramienta es capaz no sólo de leer y almacenar el contenido de la memoria, sino también de sobrescribir en la misma.

La memoria también puede ser adquirida por el desmantelamiento del Equipo Móvil, calentando la placa de circuito lo suficiente como para desoldar los chips de memoria, y usar un lector de chips de memoria para acceder a su contenido.

c. **Encontrar y explotar las vulnerabilidades:** Las vulnerabilidades del teléfono celular pueden ser descubiertas a través de un estudio detallado de protocolos de bajo nivel y en base a la experimentación, que en ciertas ocasiones se publican en la Web.

   También pueden ser descubiertos a través de ingeniería inversa. La ingeniería inversa consiste en recuperar el código del sistema operativo de la ROM de un equipo móvil idéntico al que se está examinando y así analizar el código con el fin de entender su uso en el *hardware* del teléfono celular.

   Con el conocimiento adquirido, cualquier vulnerabilidad encontrada puede ser probada sistemáticamente para determinar una técnica de ataque. Por ejemplo, para un mecanismo de autenticación por contraseña, puede ser posible usar una inyección en la memoria para sobrescribir la contraseña con un valor conocido o sustituir el programa de autenticación con una versión que siempre se autentique con éxito.

   Del mismo modo, se pueden mover dos bits en una estructura de datos, lo cual determina si la contraseña de inicio está activa y configurada, esto puede desactivar el mecanismo por completo.

d. **Inferir información por el monitoreo de las características físicas del dispositivo:** Los especialistas forenses informan que las contraseñas de

algunos teléfonos celulares, han sido descubiertas por la determinación y/o monitoreo de la dirección del bus de datos de dicha contraseña en la memoria.

Una simple observación de los datos sobre una interfaz puede revelar información. Por ejemplo, el diálogo entre el Equipo Móvil y la tarjeta SIM o de memoria protegida con contraseña pueden ser monitoreados para revelar la contraseña proporcionada por el equipo para desbloquear la tarjeta, que puede ser utilizado en un examen externo para acceder al contenido de la tarjeta.

e. **Usar un ataque de fuerza bruta automático:** Si un mecanismo de contraseña no tiene restricciones sobre el número de intentos manuales realizados y el examinador tiene tiempo, se puede intentar un ataque de fuerza bruta.

Equipado con una cámara de vídeo y un brazo robótico, la unidad sistemática puede introducir contraseñas hasta que la entrada correcta sea detectada; en el peor de los casos las teclas se dañan.

Hay un número de técnicas disponibles para que el analista pueda recuperar los datos del teléfono celular entre las cuales se destacan *Hex Dump* o también conocida como Volcado de Memoria y *Chip Off* que considera la utilización de la placa de circuitos y sus elementos para la extracción de evidencia.

Hex Dump es una técnica, que utiliza una combinación de *hardware* y *software* empleando ciertas interfaces disponibles en el teléfono celular. Se pueden utilizar cajas desarrolladas por los fabricantes para desbloquear y reprogramar el teléfono, añadiendo métodos forenses.

Chip Off consiste en acceder físicamente a la placa de circuitos, mediante la conexión a la placa de circuitos o desoldar el chip de memoria y así recuperar los datos directamente.

La conexión a la placa de circuitos se la realiza utilizando los puntos de prueba JTAG que se encuentran sobre la placa de circuitos; sin embargo, éstos no siempre están disponibles en cada placa de circuitos y así en ocasiones está técnica no está disponible para el analista.

Desoldar el chip de memoria, implica tener una estación para desoldar y un lector de chip de memoria, éstos equipos especializados son diferentes para cada modelo de teléfono celular.

Cualquier técnica que se utilice entrega un archivo binario conocido como archivo PM (*Permanent Memory*) o Archivo de Memoria Permanente. Este archivo debe ser traducido a un formato que sea fácil de reconocer y de leer. Este proceso no sólo recupera los datos visibles, sino también todos los datos eliminados del teléfono celular.

2.2.2.1 *Hex Dump*

Este proceso se refiere a realizar "*flashing*" del teléfono celular; *flashing* se interpreta como un *dump* o volcado de la memoria del teléfono, en el que se obtiene un formato hexadecimal, para una verdadera adquisición física. El objetivo es obtener el contenido total de la memoria del equipo móvil incluyendo datos ocultos y eliminados.

En esta técnica se utiliza *flashers box*, éstos son elementos electrónicos utilizados por fabricantes y/o operadores de teléfonos celulares para actualizar o reemplazar el *software* que se almacena en la memoria interna del teléfono móvil. Este *software* es comúnmente conocido como *firmware* y está por lo general preinstalado en el teléfono celular; además se tiene la posibilidad de recuperar datos de los usuarios de celulares defectuosos, bloqueados o dañados almacenados en su memoria interna.

Las *flashers boxes* son una combinación de *hardware* y *software*, existen gran variedad de éstas en el mercado, desarrolladas por los fabricantes o empresas dedicadas a telefonía celular, por falsificadores, por empresas o analistas forenses para realizar la extracción de evidencia digital; por lo tanto hay que escoger una caja adecuada, para la marca y/o modelo del teléfono celular.

La obtención de esta imagen forense o volcado hexadecimal es importante para el examinador forense, debido a que la mayoría de las aplicaciones de *software* llamadas forenses, dan como resultado de la extracción una copia de seguridad que se concentran en los datos de usuario.

El examinador debe ir más allá de los datos del usuario, como son los contactos, registros de llamadas y mensajes de texto. El uso de un volcado hexadecimal permite al examinador sondear la memoria para conocer registros de tarjetas SIM insertadas con anterioridad y la recuperación de evidencia borrada.

En algunos teléfonos celulares inteligentes se permite el uso de un *BootLoader*[33] dentro de la memoria y así realizar el volcado de memoria.

En muchos casos no se tiene disponible la herramienta forense que cumpla con esta técnica, por lo tanto se utilizan *flashers boxes* no forenses, en las cuales hay que considerar ciertos criterios forenses para su ejecución.

Por ejemplo, se puede monitorear el puerto USB de la computadora a la cual se conecta la *flasher box*, y así controlar que se ejecute únicamente la lectura y no exista intercambio de información que varíe la evidencia a ser obtenida.

Actualmente, ésta es la técnica de mayor crecimiento que utiliza las herramientas de análisis forense en teléfonos celulares del mercado.

En esta técnica la tarjeta SIM debe estar insertada en el Equipo Móvil, para obtener toda la información del teléfono celular, por lo cual es de importancia recoger el concepto de “substituto de la tarjeta SIM”.

Ocasionalmente, una tarjeta SIM no podrá ser recuperada en un teléfono celular, o puede ser que intencionalmente sea dañada y no se podrá utilizar con el teléfono, pero es necesario para la adquisición de la evidencia del Equipo Móvil.

Uno de los errores más comunes que un especialista forense puede cometer es insertar otra SIM disponible en el teléfono para obtener los datos, lo que genera una pérdida de los datos almacenados en la memoria del teléfono, como por ejemplo los registros de llamadas pérdidas, recibidas, realizadas, marcadas y los mensajes ya que está información está vinculada a la última tarjeta SIM utilizada.

[33] *Bootloader (Cargador de Arranque)* es un programa sencillo que no tiene la totalidad de las funcionalidades de un sistema operativo, diseñado exclusivamente para preparar todo lo que necesita el sistema operativo para funcionar.

La inserción de una tarjeta SIM diferente causa que los datos se borren o se copien los datos de la nueva SIM insertada, a la memoria del teléfono.

Una solución es crear un sustituto de tarjeta SIM por combinación de *software* y *hardware* para que su uso con el teléfono celular imite las características claves de la SIM original, engañando al teléfono celular para que la acepte como la SIM original.

Un substituto de SIM, a veces referido como tarjetas de acceso, puede ser útil en diversas situaciones:

- Si la tarjeta SIM de un teléfono se pierde o está dañada y es necesario para la adquisición de los datos de un Equipo Móvil con una herramienta forense, un sustituto SIM permite que los datos del teléfono sean recuperados.

- Si la tarjeta SIM para un teléfono está presente, pero se requiere un código PUK, un sustituto SIM permite la adquisición para proceder de inmediato sin tener que ponerse en contacto con el proveedor de servicios para obtener el código PUK.

- En lugar de realizar el aislamiento de las señales de radio para prohibir las comunicaciones y adquirir la evidencia de un teléfono celular, evitando las llamadas o mensajes entrantes que alteraran o modifican la evidencia, un sustituto SIM puede ser utilizado.

- Si la herramienta forense utilizada para examinar un teléfono celular accede a la información almacenada en éste utilizando un sustituto SIM en el teléfono celular, se elimina la posibilidad de que la tarjeta SIM original se altere durante el examen.

Los valores por los cuales el teléfono celular recuerda la tarjeta SIM previamente insertada en el mismo son el ICCID y el IMSI. A menudo, sólo uno de estos valores se utiliza. Ambos identificadores son únicos y se utiliza para autenticar al usuario en la red.

Si estos valores son conocidos por un teléfono específico (por ejemplo, ya sea indirectamente a través de los registros del proveedor de servicios o directamente mediante la lectura de la memoria del teléfono), puede ser posible preparar un sustituto SIM con los valores correctos necesarios para engañar al teléfono y que la acepte.

2.2.2.1.1 Ventajas

- No se borran los datos de manera automática.
- Extrae los datos ocultos del Equipo Móvil.
- Se puede extraer evidencia aunque el teléfono celular esté bloqueado, con daños menores o defectuoso.

2.2.2.1.2 Desventajas

- Requiere conversión de los datos.
- Formato para el reporte es complejo, se necesita de interpretación por parte del analista.
- Difícil de usar, se necesita de personal calificado.
- Se necesita cables y controladores especializados.
- El código fuente no está disponible, por ser propietarios.
- Limitado a algunos fabricantes.

2.2.2.2 *Chip-Off*

Esta técnica consiste básicamente, en obtener evidencia directamente de la memoria del dispositivo celular; se lo puede hacer desoldando los componentes de memoria y leerlos en un lector o utilizando las conexiones o puntos de prueba dentro de la placa de circuitos conocido como JTAG.

Después de leer la memoria utilizando las técnicas de desoldar o JTAG, el contenido de la memoria flash está disponible como un archivo binario, que se lo

puede analizar, con una herramienta especial para este propósito o con un editor hexadecimal general.

A través de este análisis, se pueden encontrar datos de interés, tales como las imágenes en formato GIF o JPG, números de teléfono, elementos de calendario mensajes de texto en el formato TPDU en sí, información considerada como evidencia digital. Parte del contenido es reconocido como contenido del sistema operativo del teléfono.

Se encuentran limitaciones al momento de leer la memoria ya que se depende del *hardware* y *software* con especificaciones del fabricante no masivamente encontradas. Otra dificultad es la falta de una herramienta de *software* para hacer la identificación e interpretación de los mensajes TPDU o de los diferentes registros encontrados.

Se ha demostrado que existen complicaciones, durante la búsqueda de mensajes de texto eliminados realizando análisis consecutivos; se observó que las áreas de memoria en donde se encontraron los mensajes en un primer análisis, se trasladaron a otra zona distinta.

Esto es probable debido a la existencia de un administrador de memoria que reasigna dinámicamente la memoria durante el uso del teléfono a fin de garantizar la óptima organización de la memoria y la utilización en todo momento.

Aunque no es particularmente sorprendente, la existencia de los administradores de memoria, tiene repercusión para el manejo forense de teléfonos móviles.

2.2.2.2.1 Uso de Interfaz de prueba (JTAG)

La mayoría de los sistemas construyen mecanismos de prueba incorporados. La razón es que la fabricación de dispositivos electrónicos es un proceso complejo en el que muchas cosas pueden salir mal.

A menos que el fabricante tenga una forma automática de realizar las pruebas de la funcionalidad del dispositivo, los elementos y las interconexiones, la calidad del producto resultante no puede ser garantizada.

JTAG hace referencia al estándar *IEEE 1149.1 Test Access Port and Boundary-Scan Architecture;* éste es un estándar para la utilización de puertos de prueba presentes en la placa de circuitos de Equipos Móviles.

El estándar JTAG especifica una interfaz y comandos, los cuales pueden ser utilizados para probar y depurar los componentes de *hardware* en los dispositivos electrónicos.

Boundary-Scan se refiere a una prueba de los pines de entrada y salida de un componente para determinar el correcto funcionamiento y la adecuada interconexión entre componentes.

Los puertos JTAG sobre la placa de circuitos pueden ser utilizados para acceder a la memoria *flash* usando el modo de depuración o el modo de prueba, lo cual se puede realizar para Estaciones Móviles con placas de circuitos que soporten JTAG, y debido a los diferentes fabricantes del mercado, la implementación del estándar es diferente para cada modelo.

Los chips de memoria *flash* en sí no soportan JTAG, sin embargo, están conectados con otros componentes como el procesador que puede ser utilizado para acceder a la memoria flash, suponiendo que el procesador tiene JTAG habilitado.

El estándar JTAG define un Puerto de Prueba de Acceso o también llamado TAP (*Test Access Port*) que permite la conexión a la placa de circuitos para la implementación de los *tests* de funcionalidad de los circuitos integrados. Las señales definidas se aprecian en la Tabla 2.7, y son vistas como pines externos sobre la placa de circuitos.

Además el estándar establece que los dispositivos de la placa de circuitos deben tener los pines señalados en la tabla 2.7, y deben estar interconectados entre sí como muestra la Figura 2.20.

Señal	Descripción
TCK	*Test Clock Input*
TMS	*Test Mode Select Input*
TDI	*Test Data Input*
TDO	*Test Data Output*
TRST	*Test Reset Input* (no obligatorio)

Tabla 2.7 Señales del estándar JTAG

El puerto JTAG se encuentra normalmente en el borde de la placa de circuitos, pero no siempre es así, y muchas veces resulta difícil determinar cuáles son los pines de determinada señal, ya que la disposición de los pines depende de los fabricantes y éstos usualmente no publican los esquemas de la placa de circuitos. Sin esta información puede ser extremadamente difícil aplicar este método, sin contar que después de encontrar los pines hay que conectar un programador JTAG específico para el tipo de memoria del cual se quiere extraer los datos.

Es importante entender que JTAG no es un estándar para bus, sino más bien especificaciones de la estandarización de puertos de acceso para prueba de cada componente, lo que permite la interconexión entre componentes sobre la placa de circuitos.

Está enteramente en manos del fabricante de cada circuito integrado decidir sobre la configuración y el funcionamiento de los pines en el *chip*. Por otra parte, corresponde al diseñador del circuito impreso decidir si los puertos JTAG se interconectan y son accesibles.

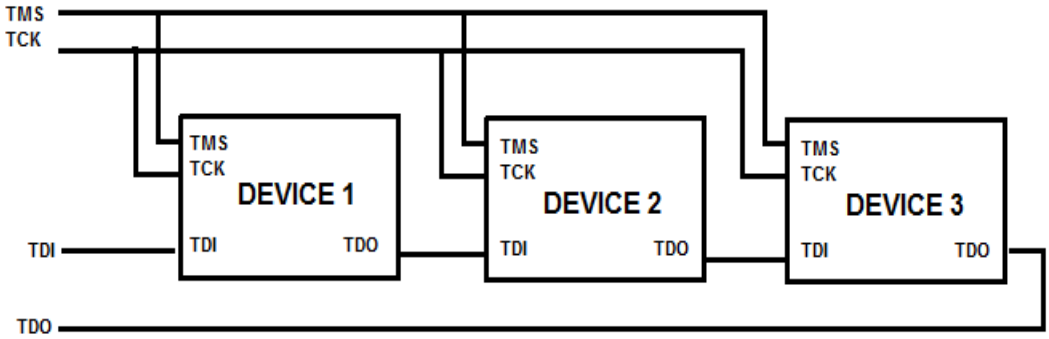


Figura 2.20: Pines y conexión de los elementos en el estándar JTAG[34]

El diseñador puede decidir no utilizar JTAG para todos los componentes, dejando los puntos de prueba en circuitos integrados no conectados. Antes de intentar usar JTAG para leer la memoria, se debe considerar lo siguiente:

- Hay que saber qué procesador y circuitos de memoria se utilizan y cómo están conectados al bus del sistema.
- Hay que encontrar los puntos de prueba para el JTAG en la placa de circuito impreso y determinar qué punto de prueba pertenece a qué señal.
- Hay que saber el protocolo de lectura-escritura para la memoria.
- Hay que determinar el voltaje correcto, si se utiliza un voltaje demasiado alto se puede dañar los circuitos.

El voltaje puede en la mayoría de los casos ser determinado mediante la medición en la placa de circuitos activa. El protocolo de memoria en la mayoría de los casos está disponible mediante la descarga de información sobre un chip de memoria en la página *web* del fabricante.

Estas dos consideraciones, sin embargo puede ser un desafío importante, ya que en la práctica es muy difícil y tedioso realizar esta tarea, sin la documentación del sistema completo, incluyendo esquemas.

[34] Figura tomada del paper "Forensic Analysis of Mobile Phone Internal Memory", WILLASSEN, Norwegian University of Science and Technology,

Cuando se trata de teléfonos móviles, tal documentación en la mayoría de los casos no está disponible. En cualquier caso, la aplicación de un sistema de lectura de la memoria a través de JTAG será diferente de un teléfono a otro. Incluso dentro de un modelo específico, los pequeños cambios de configuración (como el uso de un chip de memoria diferente) pueden llegar a requerir otra implementación de JTAG.

Para conectar el TAP a una computadora se necesita una interfaz JTAG, que puede ser construida o también existen soluciones comerciales.

2.2.2.2.2 Desoldar Componentes.

El primer propósito de esta técnica es desoldar el chip de memoria, dado que el contenido almacenado en el interior del teléfono móvil reside generalmente en una memoria flash; la técnica aparentemente obvia para acceder a los contenidos es desoldar el chip y leer el contenido. Aunque parece una solución simple, el enfoque tiene algunos conceptos que deben abordarse.

a. Desmantelar e Identificar: Antes de desoldar, las unidades deben ser desmanteladas. La mayoría de los teléfonos móviles pueden ser fácilmente desmontados con las herramientas adecuadas y la atención necesaria.

   Un juego de destornilladores TORx se necesita en la mayoría de los casos; el desmantelamiento debe hacerse en un entorno seguro electrostáticamente dado que los componentes expuestos son sensibles.

   En algunos casos, también es necesario usar herramientas especiales del fabricante, y obtener las guías de servicio en las cuales se dan instrucciones para el desmontaje de diversos modelos.

   Para varios modelos de teléfonos inteligentes se utiliza los dos lados de la placa de circuitos para reducir espacio, con lo cual se tiene algunos componentes electrónicos montados, por lo cual no es fácil realizar un reconocimiento directo de sus componentes de ahí la necesidad de las guías de servicio.

Los circuitos integrados se pueden identificar mediante el texto escrito en cada uno, por los tanto se debe anotar cuidadosamente el texto escrito y buscar los *datasheets* del fabricante.

b. Ensamblado en la placa de circuitos: Se consideran dos métodos *Through-Hole (TH)* y *Surface Mount Technology* (SMT).

Through-Hole es un método de ensamblado de placas de circuito impreso en la que los circuitos integrados se colocan sobre la placa, que está provista de agujeros, de forma que sus patas (pines) pasan al otro lado de la placa.

SMT o llamado montaje de superficie es un método de ensamblado de placas de circuito impreso, en la que los circuitos integrados se colocan sobre la placa sin que sus patas pasen al otro lado ésta.

De esta forma se pueden montar componentes a ambos lados del PCB (*Printed Circuit Board*) o placa de circuito impreso. El montaje se realiza mediante la aplicación de una pasta de soldadura que se funde al introducir el PCB en un horno especial.

Figura 2.21: Through-Hole, SMT-BGA y SMT-TSOP

Los componentes SMT no poseen pines y, si los tienen, son más cortos que los componentes *Through-Hole*; por lo que SMT en la actualidad es el más utilizado para ensamblar placas de circuitos impresos en teléfonos celulares.

SMT utiliza dos componentes, el primero denominado *Ball Grid Array* (BGA) que utiliza bolitas de estaño en la parte inferior, el segundo denominado TSOP

(*Thin small-outline package*) que utiliza pines extendidos a los lados del componente electrónico; estos componentes son conectados en la superficie del PCB. Ejemplos de estos circuitos integrados *Through-Hole*, SMT-BGA y SMT-TSOP se pueden apreciar en la Figura 2.21 de izquierda a derecha respectivamente.

Desde la perspectiva del investigador forense, el uso de métodos SMT presenta dificultades. Con *Through-Hole*, sería posible conectar cables a los pines, leer y analizar el chip sin tener que desoldar, de este modo se podría leer el contenido de la memoria sin destruir la unidad. Esto no es posible con el uso de SMT-BGA debido a que el chip está unido directamente a la PCB a través de bolas de soldadura fundida; con SMT-TSOP los pines están muy cercanos, por lo que no es posible o resulta muy difícil unir las puntas de prueba individuales a cada conexión.

El chip de memoria por lo tanto debe ser desoldado antes de que se pueda leer. Desoldar un chip presenta nuevos desafíos para el investigador forense. El desoldar debe realizarse con mucho cuidado para no dañar el circuito de memoria. Después de desoldar, se deben quitar residuos de soldadura para no producir cortocircuitos.

Con SMT – BGA en muchas ocasiones se debe restaurar a su estado original las bolitas de estaño para poder ser puesto sobre el lector de memorias, esto proceso es llamado *reballing*, para lograr esto generalmente se usa una plantilla recomendada por el fabricante.

c. Desoldar elementos: Existe una gran cantidad de equipos diferentes para la realización de soldadura y desoldadura. Estos equipos por lo general calientan la soldadura a través de la conducción del calor, convección o radiación.

Estos equipos van desde el uso de simples cautines a hornos de reflujo masivos para su uso en equipos de producción.

Lo más importante para el investigador forense es considerar las posibilidades de dañar la unidad. Los factores más importantes para evitar daños son la

temperatura correcta y el máximo gradiente de temperatura soportada por el elemento.

Considerar que en placas de circuitos que utilizan el ensamblado *Through-Hole* solo es necesario calentar los pines para desoldar, mientras que en SMT todo el chip tiene que ser calentado, lo cual añade dificultad al momento de desoldar elementos que utilizan el ensamblado SMT.

El gradiente se debe tomar en cuenta para que la temperatura se eleve lo suficientemente lento para evitar daños, al igual que la humedad puesto que si se produce vapor el dispositivo electrónico puede ser dañado; esto podría ser especialmente importante para los circuitos en los teléfonos móviles, ya que estas unidades deben asumir que han estado en condiciones de alta humedad.

Por estas razones el desoldar, como técnica forense no se debe realizar con herramientas manuales de desoldar, se debe emplear una estación de soldadura automática con posibilidades para la programación del gradiente de temperatura y para remover automáticamente los componentes.

Los equipos más comunes para desoldar dentro de una estación de soldadura deben usar una combinación de calentamiento por convección a través de aire caliente y calentamiento por radiación a través de una fuente de luz infrarroja.

La estación tiene un controlador de temperatura del inyector de aire caliente, y puede ser programado para seguir una curva de calentamiento específico, que permite al operador programar la unidad para especificar correctamente la pendiente y la temperatura máxima.

d. Leer la memoria: Para este propósito existen varios programadores tales como EPROM, EEPROM Flash en base a microcontroladores con memoria interna.

Un programador es un dispositivo electrónico hecho especialmente para la lectura y la programación de microcontroladores y dispositivos de memoria. El dispositivo se conecta a un computador, permite la lectura y la programación de una amplia gama de chips de memoria mediante el uso de adaptadores.

Un adaptador puede ser de carácter general (tales como un adaptador para todos los paquetes DIP, como el microcontrolador ATmega 16) o específicos (tales como un adaptador para el 28F640 Intel).

Además del adaptador físico, el *software* adecuado para la lectura de un chip específico es necesario, ya que la configuración de pines puede variar mucho entre los paquetes con la misma disposición física.

Fabricantes de programadores por lo general ofertan *software* con sus programadores y el programa contiene una amplia gama de dispositivos. Muchos programadores tienen capacidades integradas de control, que permiten la detección de inconsistencias en la lectura de un dispositivo.

Para muchos chips de memoria no existen programadores comerciales, por lo cual se vuelve un reto el construir tanto el *software* como el *hardware* para los analistas forenses. Muchas veces no se puede diagnosticar si en la lectura datos existen errores, debido a daños causados al momento de desoldar el componente.

La operación de lectura resulta en un fichero del mismo tamaño que el chip, este archivo pueden ser utilizado para el análisis forense de los contenidos de la memoria.

2.2.2.2.3 Ventajas

- Funciona para extraer todos los datos del equipo móvil.
- Se tiene una mejor idea de lo que está sucediendo de manera integral en el teléfono.

2.2.2.2.4 Desventajas

- Difícil de entender y convertir.
- No se tiene un formato de reporte.
- Difícil de usar, se necesita de personal calificado.

- Se necesita equipos especializados.
- El código fuente no está disponible, por ser propietarios.

2.3 PROTECCIÓN DE LA INFORMACIÓN

2.3.1 TÉCNICAS *HASH*

Una función o algoritmo matemático *Hash* es un proceso que toma un bloque arbitrario de datos y devuelve una cadena de bits de tamaño fijo (valor *hash*) de tal manera que cualquier cambio en los datos modificaría este valor *hash*.

Un *hash* forense se utiliza para mantener la integridad de una adquisición por el cómputo de algoritmos criptográficos fuertes, el valor no es reversible en los datos adquiridos.

Después de la adquisición, los cambios realizados en los datos pueden ser detectados, ya que un nuevo valor de *hash* calculado sobre los mismos datos será incompatible con el valor anterior.

Para las herramientas no forenses, los valores *hash* se deben crear manualmente usando una herramienta como *sha1sum* o *md5sum* y retener su integridad. Incluso las herramientas etiquetadas como herramientas forenses no puede calcular un *hash* criptográfico, y este valor *hash* se debe calcular manualmente.

Hay que tener en cuenta que los dispositivos móviles están constantemente activos, por lo que se pueden dar procesos de actualización, y en nuevas adquisiciones de valores *hash* en un dispositivo, estos valores serán ligeramente diferentes cuando se calculan sobre todos los datos.

Sin embargo, los valores *hash* calculados sobre las porciones seleccionadas de los datos, como archivos y directorios, por lo general se mantienen constantes. Sólo unas pocas herramientas forenses ofrecen el cálculo del valor *hash* más granular de archivos y directorios.

Algunas herramientas forenses tampoco notifican al usuario de forma automática acerca de las inconsistencias del valor *hash*, poniendo la responsabilidad en el especialista forense para comprobar el valor *hash* manualmente.

Los valores *hash* son beneficiosos porque proveen a los examinadores la capacidad de filtrar archivos de datos, y demostrar que la integridad de datos se mantiene intacta.

Con la creciente popularidad y los avances tecnológicos de los dispositivos móviles, surgen nuevos retos para los examinadores forenses y fabricantes de herramientas. Los datos recuperados de los dispositivos móviles han demostrado ser útiles en la solución de incidentes y la investigación de actividades delictivas.

Las funciones criptográficas *hash* proporcionan a los examinadores forenses la capacidad de verificar la integridad de los datos adquiridos. El valor *hash* resultante, una cadena de bits de tamaño fijo, a menudo se utiliza para identificar los archivos conocidos y pone de manifiesto que los datos no se han modificado. Las dos funciones *hash* comúnmente utilizadas son las funciones MD5 y SHA-1.

Cabe destacar que los valores *hash* de la memoria del teléfono han demostrado ser inconsistentes en algunos casos; sin embargo estas diferencias no deben tener un impacto en la integridad de los archivos estáticos en la memoria, como imágenes, sonidos, listas de contactos, entre otros.

El Instituto Nacional de Estándares y Tecnología NIST (*National Institute of Standards and Technology*) define una adquisición consistente como dos adquisiciones consecutivas que producen diferentes *hashes* generales de la memoria, mientras que los valores *hash* de los archivos individuales siguen siendo consistentes.

Técnicas de análisis para teléfonos celulares pueden proporcionar éxitos en las investigaciones en función de los datos y la forma en que fueron adquiridos.

Sin embargo, dado que 10 *hashes* de la memoria completa se espera sean inconsistentes, éstos no tienen peso en la verificación del contenido individual del

mismo teléfono, ya que no se dispone de estándares para los teléfonos móviles, también faltan las normas para la realización de una adquisición.

Hay varias prácticas generalmente aceptadas, y cada uno tiene sus propias consecuencias negativas.

CAPÍTULO III

CAPÍTULO 3

3. HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL

3.1 INTRODUCCIÓN

Al surgir el análisis forense, donde se trata de prevenir, estudiar y evaluar las conductas de incidencia criminal, ilegal e inapropiada que ciertos ciudadanos pueden tener, es de gran ayuda el usar el análisis forense en las siguientes áreas:

a. Para facilitar investigaciones de actividades criminales usando metodologías, técnicas y modelos de investigación forense.

b. Para preservar, recopilar, analizar y proporcionar las evidencias científicas y técnicas a un tribunal civil o penal de la ley.

c. Para preparar la documentación apropiada para el cumplimiento de la ley.

El análisis forense en dispositivos móviles, podría considerarse hasta cierto punto similar al análisis forense informático, sin embargo sus diferencias se las mencionó anteriormente. Cabe recalcar que los dos análisis convergen, principalmente en la falta de un procedimiento de validación de herramientas forenses que ayuden a determinar su efectividad.

Al realizar un análisis forense a teléfonos celulares, los investigadores requieren de conocimientos y herramientas (*software* y *hardware*) especiales que ayuden a entender cómo trabajan estos dispositivos, y saber dónde se encuentra información importante que podrá ser utilizada como evidencia y si fue obtenida de forma adecuada.

En este capítulo, se presenta una perspectiva general de varias herramientas de análisis forense en teléfonos celulares, que han sido utilizadas basándose en los niveles propuestos en el capítulo 2.

Varias de las herramientas forenses para dispositivos móviles abordan el problema de mantener la integridad de los datos; sin embargo varios sistemas operativos propietarios de los teléfonos móviles, crean ciertas contradicciones.

Generalmente el *software* forense debe comunicarse con el sistema operativo del teléfono, a través de una conexión abierta, accediendo así a los datos. Dado que la memoria del teléfono móvil y el sistema operativo se mantienen activos en la adquisición de datos, es casi imposible evitar modificaciones en la memoria del teléfono, sobre todo cuando se realizan varias adquisiciones.

Principalmente se evidencian estas modificaciones, cuando se tiene un único sistema de archivos, pero los datos estáticos del usuario, como imágenes permanecen sin cambios. Sin embargo, algunos de los cambios pueden ser significativos, por mencionar alguno, si tales cambios alteran el estado de un mensaje SMS de entrada durante su adquisición.

La herramienta a utilizar depende del teléfono y se basa realmente en el *software* propio del teléfono, lo que conlleva a las siguientes situaciones:

a. La adquisición de datos a través de la interfaz del *software*, puede ser limitada.

b. Datos importantes pueden ser omitidos en teléfonos que responden a determinado comando o protocolo.

c. Los comandos utilizados exitosamente con un dispositivo móvil, no necesariamente serán satisfactorios en otro dispositivo móvil.

Además existen herramientas de *hardware* que realizan un análisis de Volcado de Memoria obteniendo información específica de las localidades de memoria del teléfono móvil, que son de gran utilidad, siempre y cuando se conozca qué y dónde se encuentra esa información.

Por otro lado también se manejan herramientas forenses de hardware que realizan un análisis de cada uno de los componentes del dispositivo móvil, principalmente en las memorias internas de los mismos; este tipo de

procedimiento generalmente se lo realiza cuando es difícil ingresar y obtener información del dispositivo móvil a través de los medios convencionales (USB, *Bluetooth*, IrDA).

3.1.1 ADMINISTRADORES DE TELÉFONOS

Los administradores de teléfonos son herramientas reconocidas como de "*software* no-forense", diseñado para llevar a cabo una serie de tareas dirigidas por el usuario como son por ejemplo la lectura y la actualización de los contenidos del teléfono, usando uno o más protocolos de comunicaciones compatible con el teléfono.

Los administradores de teléfonos son utilizados circunstancialmente por los investigadores forenses para recuperar datos de un teléfono celular, cuando no existe una herramienta forense adecuada para su respectivo análisis.

Si bien es posible tomar precauciones para preservar la integridad de los datos en un teléfono celular, existen riesgos inherentes. La aplicación de un filtro forense a los protocolos de intercambio de los administradores de teléfonos, se propone como un medio para reducir el riesgo de errores.

Un tema clave es el tiempo transcurrido entre que un modelo de teléfono esté disponible para el público y la existencia de una herramienta forense compatible con ese equipo.

Cuando aparece un nuevo modelo, el fabricante de la herramienta forense debe decidir si debe adaptar su herramienta al nuevo modelo. Se compran ejemplares de este modelo para su estudio, y se prueba la actualización que se crea para el modelo, y por último se comunica la actualización de la herramienta al examinador forense.

Los factores de decisión para realizar esta actualización se basan en la popularidad del modelo de teléfono, los requisitos de la base de clientes, entre otras. El tiempo requerido para que las actualizaciones de la herramienta lleguen al usuario y los examina, puede ser muy largo, creando insatisfacción para los examinadores forenses.

Además, la validación de la actualización para su uso en un caso judicial aumenta la demora, poniendo a los especialistas forenses detrás en la curva en que el modelo sale al mercado y de tener un medio propicio para la recuperación automática de evidencia digital. La Figura 3.1 ilustra la situación.

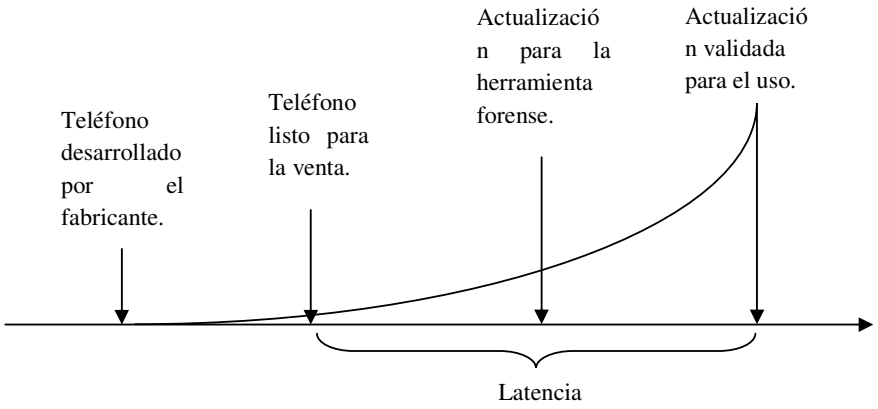


Figura 3.1: Línea de Tiempo de la Herramienta Forense [35]

Los administradores de teléfonos se vuelven en varias ocasiones la única herramienta y camino para recuperar datos, cuando no existe una herramienta forense que lo pueda realizar. Los administradores de teléfonos generalmente suelen estar disponibles por el fabricante del teléfono móvil y mantenerlo actualizado con soporte técnico para modelos recientes; además permiten diversas operaciones, incluyendo la recuperación básica de datos de usuarios como directorio telefónico.

La validez de las herramientas forenses que no están diseñadas específicamente para propósitos forenses es cuestionable. Sin embargo los administradores de teléfonos tienen la capacidad de leer y escribir datos en un teléfono; esto es un problema desde el punto de vista forense, ya que el análisis forense garantiza que la información no debe ser modificada, por lo tanto se debe utilizar este administrador con controles de procedimiento y la aplicación de pruebas adecuadas.

[35] Figura tomada del libro "Forensic Filtering of Cell Phone Protocols", JANSEN y DELAITE, NISTIR 7516, 2008

Se debe buscar otras formas de reducir la latencia existente entre un nuevo modelo y la herramienta forense existente. Por ejemplo, fabricantes de herramientas podrían mejorar sus relaciones con los fabricantes de teléfonos o con las operadoras de la red de telefonía móvil para obtener una ventaja y la herramienta pueda estar habilitada antes de que los teléfonos estén disponibles para el público.

Otro enfoque para reducir la latencia, sería el Filtrado de Protocolos en el administrador de teléfonos. La idea sería en aprovechar la funcionalidad de los administradores de teléfonos disponibles, añadiendo un filtro de protocolos, que límite su funcionalidad permitiendo un intercambio seguro, sin que se transgreda la evidencia que se pueda encontrar en el teléfono celular.

Los fabricantes de teléfonos celulares como Nokia, Motorola y Samsung normalmente mantienen su *software* de administración de teléfonos al día para modelos nuevos y al mismo tiempo ofrecen actualizaciones; los productos forenses han reconocido desde hace tiempo la posibilidad de que los administradores teléfono se puedan usar para la recuperación automática de datos básicos de usuario.

Los administradores de teléfonos no son herramientas forenses, por lo cual se deben seguir pasos adicionales y así poder usarlas para recuperar datos. Estos pasos incluyen la validación de la operación del administrador de teléfono, probar y verificar los procedimientos que deben seguirse para la adquisición de datos, a fin de proteger contra la alteración de los mismos, a través de un *hash* criptográfico.

Lamentablemente, ni siquiera un especialista con experiencia forense toma todas las precauciones, y accidentalmente puede escribir datos en un teléfono con un administrador de teléfono. El filtrado de protocolos en administradores de teléfonos ayuda a proteger los datos contra modificaciones accidentales en el teléfono y proporciona una medida provisional hasta que una herramienta forense admita el teléfono en cuestión.

Las herramientas forenses de *software* para teléfonos celulares, a menudo recuperan los datos empleando los mismos protocolos utilizados por los administradores de teléfonos. Para evitar el problema de alterar los datos en un teléfono, las herramientas de forenses restringen los protocolos usados para comunicarse con el dispositivo a solo las funciones que son bien conocidas por ser seguras.

La mayoría de los administradores de teléfonos se ejecutan bajo el sistema operativo Windows. Las comunicaciones con los teléfonos celulares se producen sobre los puertos serie COM o puerto USB.

La técnica utilizada para el prototipo de filtro consiste en interceptar la llamada del administrador del teléfono a la interfaz de programación de aplicaciones (API[36], *Application Programming Interface*), para mediante esta función capturar los datos, interpretar el contenido, y devolver una respuesta adecuada al administrador de teléfonos.

3.1.2 HERRAMIENTAS FORENSES ANALIZADAS Y UTILIZADAS EN TELÉFONOS CELULARES Y TARJETAS SIM

La variedad de herramientas forenses para teléfonos celulares es amplia, existen un número considerable de herramientas de *software* y *hardware*, pero la gama de dispositivos sobre los que operan normalmente se reduce a plataformas distintas de la línea de productos de un fabricante, una familia de sistemas operativos, o un tipo de arquitectura de *hardware*.

Las herramientas forenses de *software* son el medio preferido para la recuperación de evidencia digital en teléfonos celulares que sean compatibles con las mismas. La recuperación de datos se realiza generalmente a través de un análisis lógico y no de un análisis físico, usando uno o más protocolos soportados por el dispositivo, estos protocolos incluyen protocolos estándar, de diagnóstico, de sincronización propietarios y comandos de la interfaz.

[36] *API* (*Application Programming Interface*) es el conjunto de funciones y procedimientos que ofrecen ciertas bibliotecas para utilizarlos por otro software como una capa de abstracción.

Las herramientas de análisis lógico utilizadas en el análisis forense para teléfonos celulares, típicamente son protocolos de comunicaciones que ayuden a adquirir datos, como por ejemplo, los comandos AT, FBUS, OBEX[37].

Por otra parte, las herramientas requieren que el examinador tenga acceso completo al dispositivo (por ejemplo, el dispositivo no está protegido por algún mecanismo de autenticación o el examinador puede adaptarse a cualquier mecanismo de autenticación encontrado).

Aunque la mayoría de herramientas ofrecen una amplia gama para la adquisición, examinación y reporte de funciones, algunas herramientas se centran en uno de estos subconjuntos. Del mismo modo, diferentes herramientas pueden ser capaces de utilizar diferentes interfaces (infrarrojo, *Bluetooth* o cable serial) para adquirir el contenido del dispositivo.

Los tipos de información que una herramienta puede adquirir varían ampliamente e incluyen información personal como el directorio telefónico, los registros de llamadas telefónicas, mensajes SMS/EMS/MMS, correo electrónico, mensajería instantánea, URLs, el contenido de la visita sitios *Web*, audio, video, contenido de imagen y contenido de la tarjeta SIM.

Adquirir la información en un teléfono celular, puede variar dependiendo de factores como:

- 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 a los que se suscribe el usuario.
- Las modificaciones introducidas en el teléfono por el usuario.

Independientemente de la interfaz utilizada, se debe considerar que la capacidad de adquirir el contenido que reside en la tarjeta SIM, puede no ser compatible con

---

[37] *Object Exchange (OBEX)* es un protocolo de comunicaciones que facilita el intercambio de objetos binarios entre dispositivos. OBEX es similar en diseño y funcionalidad a HTTP, protocolo en el que el cliente utiliza un transporte fiable para conectarse a un servidor y así recibir o proporcionar objetos.

algunas herramientas. La Tabla 3.1 muestra herramientas disponibles que ofrecen facilidades para determinados tipos de teléfonos celulares.

Herramienta Forense	**Alcance**	**Características**
ZRT 2	Adquisición, examinación y reporte	- Herramienta manual, permite extraer información por medio de un analizador fotográfico encriptado.
Device Seizure	Adquisición, examinación y reporte	- Teléfonos RIM SO y modelos de GSM, TDMA, CDMA. - Soporta el recopilar información del dispositivo
Oxygen Phone Manager **(Version Forense)**	Adquisición, examinación y reporte	- Teléfonos GSM - Soporta solo la adquisición de la información del dispositivo.
UFED ***Universal Forensic Extraction Device***	Adquisición, examinación y reporte	- Windows Mobile, teléfonos RIM SO y modelos de GSM, TDMA, CDMA. - Soporta el recopilar información del dispositivo

Tabla 3.1: Herramientas Forenses para Teléfonos Celulares

Debido a que en el estándar GSM el teléfono celular se encuentra dividido en dos partes, que son el teléfono móvil (ME) y la tarjeta SIM, surgen herramientas de *software* forense que analizan exclusivamente las tarjetas SIM, de forma independiente de las actividades de los teléfonos móviles. La tarjeta SIM debe ser removida desde el teléfono y se inserta en un lector apropiado para la adquisición de información. Las herramientas forenses para tarjetas SIM requieren de un lector especializado que acepta una tarjeta SIM. La tabla 3.2 enumera algunas herramientas forenses para Tarjetas SIM.

Las herramientas adquieren los datos del dispositivo usando técnicas de análisis físico o lógico, como se mencionó en el capítulo anterior, por lo que de ser posible, se deben utilizar los dos tipos de análisis.

Herramienta Forense	Función	Características
SIM Card Seizure	Adquisición, examinación y reporte	- Recupera la información de la tarjeta SIM. - Requiere un lector de SIM.
SecureView	Adquisición, examinación y reporte	- Recupera la información de la tarjeta SIM. - Soporta lector PC/SC[38]
UFED	Adquisición, examinación y reporte	- Recupera la información de la tarjeta SIM a través del puerto propietario de la herramienta.

Tabla 3.2: Herramientas Forenses para Tarjetas SIM

Las herramientas no diseñadas específicamente para propósitos forenses, son cuestionables y deben ser cuidadosamente evaluadas antes de su uso. Aunque ambas herramientas de *software* forense y no forense, generalmente usan los mismos protocolos para comunicarse con un dispositivo, las herramientas forenses no permiten un flujo bidireccional de información con el fin de administrar el funcionamiento del dispositivo.

Por lo general, en las herramientas no forenses, no considera la adquisición de valores *hash* del contenido para fines de integridad. La documentación también puede ser limitada y el código fuente no está disponible para su revisión, aumentando la probabilidad de error y disminuyendo la confiabilidad de los resultados.

Se debe considerar sin embargo que las herramientas no forenses, pueden ser el único medio para recuperar la información que podría ser evidencia relevante. Por otro lado, se podría sobrescribir, añadir, o causar pérdida de información, si no se utiliza con cuidado.

[38] PC/SC (Personal Computer/ Smart Card) es un conjunto de especificaciones para la integración de tarjetas inteligentes en ordenadores personales. En particular se define un API de programación que permite a los desarrolladores trabajar de forma uniforme con lectores de tarjetas de distintos fabricantes, que cumplan con la especificación

A continuación se describen brevemente cada una de las posibles herramientas que se utilizarán en el desarrollo de este proyecto.

3.1.2.1 *Device Seizure* y SIM *Card Seizure (Paraben)*[39]

Device y SIM *Seizure* versión 3.0 pertenece a las herramientas de *Paraben*. Es un conjunto de herramientas de *software* forense que permite a los examinadores forenses adquirir, buscar, examinar, y reportar los datos relacionados con teléfonos celulares que operan con tecnología CDMA, TDMA y GSM. Además permite analizar las tarjetas SIM a través de un lector. *Device* y SIM *Seizure* permiten realizar una adquisición de datos lógica y física.

3.1.2.2 *Oxygen Phone Manager (OPM)*[40]

La versión forense de OPM permite a los examinadores adquirir los datos desde el dispositivo y exportar los datos adquiridos en múltiples formatos (html, pdf, entre otros). El *software* de OPM se adapta a teléfonos móviles y/o teléfonos inteligentes fabricados por Nokia, Sony Ericsson, Siemens, Panasonic, entre otros. Permite adquirir datos de los teléfonos móviles a través de interfaces físicas estandarizadas, *Bluetooth* o una conexión *IrDA*.

3.1.2.3 *UFED (Cellebrite)*[41]

Está diseñado para obtener los datos de tarjetas SIM y teléfonos celulares que operan con tecnología GSM, TDMA y CDMA. UFED proporciona la capacidad de conectarse a través de un cable, *Bluetooth* o *IrDA*. El terminal UFED contiene un SO embebido con pantalla táctil, cables de datos para varios fabricantes de teléfonos, un lector de tarjetas SIM protegido contra escritura.

---

[39] *Paraben*, es una compañía que se estableció rápidamente como líder en programas informáticos especializados en ciencias forenses, además lanzó al mercado la primera herramienta comercial para realizar análisis forense de teléfonos celulares.

[40] *Oxygen Software*, es un equipo de desarrolladores de software profesionales. Se encargan del desarrollo de software para la gestión de la información, datos y configuración de los teléfonos móviles y teléfonos inteligentes.

[41] *Cellebrite*, es productor y distribuidor de herramientas forenses para analizar dispositivos electrónicos, trabaja directamente con fabricantes de teléfonos móviles para garantizar la compatibilidad de sus productos con el público.

3.1.2.4 *Secure View (Susteen)*[42]

Secure View es un conjunto de herramientas de *software* forense que adquiere y extrae datos de los dispositivos móviles que funcionan con tecnología GSM, CDMA, TDMA; además analiza los datos de tarjetas SIM. *Secure View* proporciona un entorno seguro de sólo lectura, lo que elimina la manipulación accidental o supresión de datos críticos. *Secure View* adquiere datos de los teléfonos móviles a través de interfaces físicos estandarizados, *Bluetooth* o una conexión IrDA.

3.1.2.5 *FERNICO*[43] *ZRT 2*

El examinador de teléfonos celulares FERNICO ZRT 2 es una herramienta de reporte de información y examinación manual para teléfonos celulares y/o dispositivos electrónicos. ZRT permite a los investigadores extraer datos de un dispositivo móvil cuando todas las otras herramientas no funcionan.

3.2 ANÁLISIS DE HERRAMIENTAS FORENSES PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL

Las herramientas forenses están destinadas a facilitar el trabajo de los examinadores, las cuales son las que les permiten realizar la adquisición y análisis de forma oportuna y estructurada, y así mejorar la calidad de los resultados.

Las herramientas forenses de *software* y *hardware* se esfuerzan para hacer frente a una amplia gama de dispositivos y manejar las situaciones más comunes de investigación con modestos requisitos de nivel de conocimiento.

Estas herramientas suelen realizar adquisiciones lógicas de información utilizando protocolos comunes para la sincronización, la depuración, y las comunicaciones.

---

[42] Susteen Inc. es un proveedor internacional de soluciones de diseño, especializada en el área de comunicaciones de datos y computación móvil.

[43] *Fernico,* es una compañía informática que trabaja en estrecha colaboración con los principales servicios digitales en el mundo forense en la aplicación de la ley, los sectores militares y comerciales.

Situaciones más complicadas, tales como la recuperación de datos borrados, a menudo requieren herramientas basadas en *hardware* altamente especializado.

Si se considera que cada teléfono posee diversas características en relación a su fabricante, esto dificulta la adquisición de datos; ocasionando que los fabricantes de herramientas forenses mantengan una lista de teléfonos y características compatibles con su *software*.

3.2.1 ESCENARIOS BAJO LOS CUALES SE ANALIZAN Y SE COMPARAN LAS HERRAMIENTAS FORENSES A UTILIZAR

Una metodología sencilla, para comprender y medir las capacidades de las herramientas forenses, se describe a continuación. Los pasos principales se ilustran en la Figura 3.2.

Primero se debe elegir un conjunto limitado de dispositivos meta[44] (que van desde teléfonos celulares básicos a inteligentes), a los que se los someterá a un análisis basado en diversos escenarios, que se explicarán posteriormente en detalle.

Después de analizar los dispositivos meta y adquirir información del teléfono celular y/o de la tarjeta SIM mediante una herramienta forense, se procede a examinar la información obtenida, con la finalidad de determinar si esta información puede ser utilizada como evidencia de una actividad delictiva ante un juzgado.

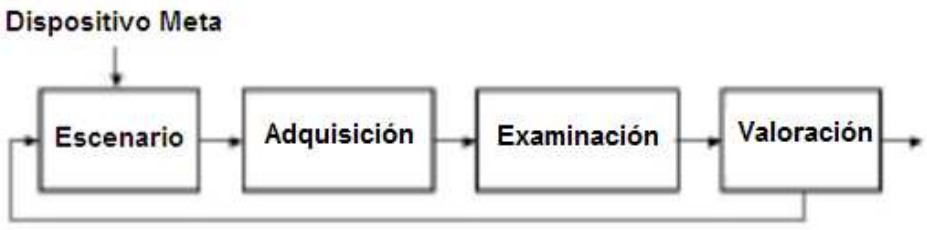


Figura 3.2: Capacidades de las Herramientas Forenses [45]

[44] Dispositivo meta, dispositivos móviles celulares a ser analizados

[45] Figura tomada del libro "Cell Phone Forensic Tools: An Overview and Analysis Update", JANSEN y DELAITE, NISTIR 7387, 2007

Por último se debe realizar una retroalimentación del proceso considerando las herramientas que se utilizaron en el análisis de los diferentes escenarios.

Para los teléfonos GSM, dos conjuntos de escenarios fueron aplicados: uno para los teléfonos que contienen una tarjeta SIM asociada, y otro para tarjetas SIM removidas de sus teléfonos y examinadas de forma independiente.

Los dispositivos meta han sido seleccionados en base a información comercial obtenida de OTECEL y de teléfonos elegidos al azar del mercado estadounidense y europeo, que son de fácil adquisición para el usuario.

La lista aunque no es extensa, abarca una amplia gama de sistemas operativos, tipos de procesadores y componentes de *hardware*. Estas variaciones fueron destinadas para descubrir las sutiles diferencias en el comportamiento de las herramientas forenses en la adquisición y el examen. La Tabla 3.3 muestra las principales características de cada dispositivo que es analizado:

Dispositivo Móvil	**Ancho de Banda**	**Características Generales**		**Nominación**
		Físicas	**Lógicas**	
Nokia 1208b	GSM 900/ 1800	- Display a color - Batería: *Stand-by* hasta 365 horas; 7 horas tiempo de conversación.	- Agenda telefónica - Registro de llamadas - SMS	Básico
Nokia 5130c *Xpress Music*	GSM 850/ 900/ 1800/ 1900	- Display a color - MicroSD max. 8GB - Cámara de 2MP - *Bluetooth*/ MicroUSB - Batería: *Stand-by* hasta 288 horas, tiempo de conversación 6 horas.	- Agenda telefónica SMS, MMS, *e-mail* - Reproductor MP3/ MP4/ eAAC+ - *Browser* WAP2.0/ xHTLM	Medio

Nokia E5	GSM 850/ 900/ 1800/ 1900	- Display a color QVGA - MicroUSB/ *Bluetooth* - Interfaz de conexión inalámbrica *WiFi* - MicroSD max 32 GB. - Cámara de 5MP - Batería: *Stand-by* hasta 696 horas, tiempo de conversación 18h30 minutos.	- SO Symbian - SMS, MMS, *e-mail*, *Push E-mail*, IM	Avanzado
Nokia N8	GSM 850/ 900/ 1800/ 1900 HSDPA 850/ 900/ 1700/ 2100/ 1900	- Display AMOLED *touchscreen* - Sensor de proximidad para auto apagado - Interfaz de conexión inalámbrica *WiFi* - MicroSD max. 32Gb - Cámara de 12MP - *Bluetooth*/MicroUSB 2.0 - Batería: *Stand-by* 390 horas, tiempo de conversación 12h30 min.	- Registro de llamadas máx. 30 días. - SMS, MMS, IM, *e-mail*, *Push e-mail* - SO *Symbiam*3 - *Browser* WAP2.0/ xHTML, lector RSS - Reproductor MP3/ MP4/ WAV/ WMA/ AAC/ eAAC+ - Salida de Television - Varias Aplicaciones (visor de documentos, editor de fotos y videos)	Avanzado

LG CU920	GSM 800/ 900/ 1800/ 1900 GPRS/ EDGE/ HSPDA 850	- Display a color - MicroSD - USB/ *Bluetooth* - AT&T wireless - Cámara de 2 MP - Batería: *Stand-by* 200 horas, tiempo de conversación 6 horas.	- Agenda telefónica (500 entradas) - *Browser*: HTML - SMS, MMS - Reproductor MP3/WMA	Medio
Motorola SLV L7	GSM 850/ 900/ 1800/ 1900	- Display a color - MicroUSB/ *Bluetooth* - Cámara VGA - MicroSD max. 512 MB - Batería: *Stand-by* 140 horas, tiempo de conversación 4 horas.	- Agenda telefónica (1000 entradas) - SMS, MMS, *e-mail*, IM - Reproductor MP3/ MPEG4	Medio
Motorola V3	GSM 900 / 1800 / 1900	- Display a color - Cámara 1.3 MP - MicroSD max. 512 MB - Mini USB/ *Bluetooth* - Batería: *Stand-by* 280 horas, tiempo de conversación 7 horas.	- Agenda Telefónica (1000 entradas) - SMS, EMS, MMS, *E-mail*, IM - Reproductor MP3/ AAC/ MPEG4	Medio
Samsung SGH J-700	GSM 900 / 1800 / 1900	- Display a color - Cámara 1.3 MP - MicroSD/USB - *Bluetooth*	- SMS, EMS, MMS - *Browser*: WAP 2.0/ xHTML, HTML - Reproductor MP3/ MP4/ WAV	Medio

Sony Ericsson W205a	GSM 800/ 900/ 1800/ 1900	- Display a color - MicroSD máx. 2 GB - Cámara de 1.3 MP - *Bluetooth*/USB - Batería: *Stand-by* 425 horas, tiempo de conversación 9 horas	- SMS, MMS - *Browser*: WAP2.0/HTML - *Walkman player* - Radio - Agenda telefónica - Registro de llamadas	Medio
Sony Ericsson W20i Zylo	GSM 850 / 900/ 1800/ 1900 HSDPA 900/ 2100	- Display a color - Cámara: 3.15 MP - Memoria: hasta 16 GB - *Bluetooth*/USB - microSD, hasta 16 GB - Batería: *Stand-by* 340 horas, tiempo de conversación 4 horas	- SMS, MMS, *E-mail*, Push *E-mail*, IM *Browser*: WAP 2.0/ HTML - Agenda telefónica - Registro de llamadas - Reproductor MP3/MP4	Avanzado
BlackBerry Curve 8520	GSM 850/ 900/ 1800/ 1900	- Display a color - Teclado *QWERTY* - Cámara de 2 MP, video QVGA. - *Bluetooth*/MicroSD - Interfaz de conexión inalámbrica *WiFi* - Batería: *Stand-by* hasta 408 horas, tiempo de conversación hasta 4h30 min.	- Agenda telefónica - *Browser* HTML - SMS, MMS, *e-mail*, IM - Reproductor MP3/ MP4/ eAAC+ - SO *BlackBerry*	Avanzado

Tabla 3.3: Características de los dispositivos móviles analizados [46]

[46] Referencia de la pág. www.smart-gsm.com analizando los diferentes dispositivos móviles enlistados. Última consulta mayo 2011.

Como información adicional, no todas las herramientas forenses soportan todos los dispositivos móviles, de hecho ocurre lo contrario, una herramienta específica normalmente sólo admite un número limitado de dispositivos.

La determinación de qué herramienta utilizar para qué dispositivo se basa inicialmente en la lista de teléfonos celulares soportados por la herramienta, obtenida de sus respectivas páginas web. La Tabla 3.4 resume los dispositivos soportados por cada herramienta. El cuadro no incluye las herramientas forenses de la tarjeta SIM.

Dispositivo Móvil	**Herramientas Forenses**				
	Device Seizure	**Oxygen Phone Manager**	**UFED**	**Secure View**	**ZRT 2**
Nokia 1208b	-	-	X	-	X
Nokia 5130c *Xpress Music*	-	X	X	-	X
Nokia E5	X	X	X	-	X
Nokia N8	X	X	X	-	X
LG CU920	X	-	X	X	X
Motorola L7	X	X	X	-	X
Motorola V3	X	X	X	-	X
Samsung SGH J-700	X	X	X	X	X
Sony Ericsson W205a	-	-	X	-	X
Sony Ericsson W20i Zylo	-	X	X	-	X
***BlackBerry Curve* 8520**	-	X	X	X	X

Tabla 3.4: Dispositivos móviles vs Herramientas Forenses

En general, herramientas forenses de SIM, no recuperan todos los elementos posibles de una tarjeta SIM. Si bien algunas herramientas tienen como objetivo recuperar la mayor cantidad de información, la mayoría de ellas se concentra en un subconjunto considerado más útiles para las pruebas forenses. En la Tabla 3.5

se muestra una visión general de los elementos recuperados, basados en información obtenida en la página web del fabricante.

Los escenarios definen un conjunto de actividades prescritas utilizadas para medir las capacidades de la herramienta forense, para recuperar información de un teléfono, a partir de la conectividad y adquisición progresiva de información en aplicaciones comunes, formatos de archivos y la configuración de dispositivo.

		Herramientas Forenses			
Información		**SIM *Card Seizure***	**UFED**	***Secure View***	***ZRT 2***
Agenda Telefónica		-	X	X	X
IMSI – *International Mobile Subscriber Identity*		X	X	X	X
ICCID – *Integrated Circuit Card Identifier*		X	X	X	X
MSISDN – *Mobile Subscriber ISDN*		X	X	X	-
SPN – *Service Provider Name*		X	X	X	-
ADN - *Abbreviated Dialing Numbers*		X	X	X	-
LDN – *Last Numbers Dialed*		X	X	X	-
SMS – *Short Message Service*	***Leidos/ No Leidos***	X	X	X	X
	Borrados	X	X	X	-
LOCI - *Location Information*		X	X	X	-
LOCI GPRS - *Location Information* GPRS		X	-	X	-
SDN –*Service Dialling Number*		X	X	X	-
EXT1 – Extension 1		X	-	X	-
EXT2 – Extension 2		X	-	X	-
EXT3 – Extension 3		-	-	X	-
FDN – *Fixed Dailling Numbers*		X	-	X	-

Tabla 3.5: Información de identificadores con tarjetas SIM vs. Herramientas Forenses

Los escenarios no tienen la intención de ser exhaustivos o de servir como una evaluación formal del producto. Sin embargo, su intento de cubrir una amplia

gama de situaciones comúnmente encontradas en el examen de un dispositivo (por ejemplo, datos ocultos, depuración de datos) es útil para determinar las características y funcionalidad que ofrece la herramienta.

La tabla 3.6 ofrece una visión general de estos escenarios que se analizaran para todos los dispositivos meta. Para tener en claro cada escenario de la lista, se realiza una breve descripción de su objeto, método de ejecución, y los resultados que se espera al ejecutar los mismos. Por lo que consideramos:

Escenario	Descripción
HEX DUMP/ Extracción Lógica	Determinar si la herramienta puede realizar una extracción lógica o volcado de memoria. - Analizar el sistema de archivos de la información recopilada de la memoria interna del dispositivo móvil o de la tarjeta SIM. - Analizar bit a bit la información recopilada de la memoria interna del dispositivo móvil o de la tarjeta SIM.
Conectividad y Recuperación	Determinar si la herramienta puede conectarse correctamente al dispositivo y recuperar el contenido del mismo. - Habilitar la autenticación del dispositivo del usuario, antes de la adquisición y requerimientos (PIN, contraseña y/u otra autenticación de información) para limitar el acceso. - Conectar el dispositivo y adquirir el contenido, comprobar que los resultados sean consistentes con las características conocidas del dispositivo. - Esperar que el mecanismo de autenticación sea exitoso sin afectar a la herramienta, y que la información del dispositivo pueda ser recuperada.
Aplicaciones PIM (Personal Information Manager)	Determinar si la herramienta puede encontrar información aunque ésta se haya eliminado, además que encuentre aplicaciones PIM (Administración de Información Personal), por ejemplo, la agenda telefónica. - Crear diferentes tipos de archivos PIM en el dispositivo. - Esperar que toda la información PIM relacionada al dispositivo, se pueda encontrar y recopilar.

	- De forma selectiva eliminar algunas de las entradas, adquirir el contenido del dispositivo, localizar y visualizar la información. - Esperar que los remanentes de la información eliminada puedan ser recuperados y reportados.
Llamadas Marcadas/ Recibidas en el teléfono	Determinar si la herramienta encuentra llamadas telefónicas marcadas, recibidas y perdidas, incluidas las llamadas que han sido eliminadas. Realizar y recibir llamadas desde y hacia varios números. - Esperar que todas las llamadas telefónicas marcadas, recibidas y perdidas se puedan organizar y reportar. - Selectivamente eliminar algunas entradas, adquirir el contenido del dispositivo, localizar y visualizar las llamadas marcadas y recibidas. - Esperar que las llamadas telefónicas eliminadas se puedan organizar y reportar.
Mensajes SMS/MMS	Determinar si la herramienta encuentra los SMS/MMS realizados, recibidos y borrados. - Colocar y recibir mensajes SMS/MMS. - Esperar que los mensajes SMS/MMS enviados, recibidos y borrados en el teléfono puedan ser organizados y recuperados - Eliminar de forma selectiva algunos mensajes, adquirir el contenido del dispositivo, localizar y mostrar todos los mensajes. - Esperar que los mensajes SMS/MMS borrados en el teléfono puedan ser organizados y recuperados.
Mensajes de Internet	Determinar si la herramienta puede recuperar correos electrónicos y mensajes instantáneos (IM) enviados y recibidos, incluyendo los mensajes borrados. - Enviar y recibir mensajes instantáneos y mensajes de correo electrónico. - Esperar que la mensajería instantánea y de correo electrónico que se haya enviado y recibido en el teléfono se la pueda reconocer y recopilar.

	- Eliminar de forma selectiva algunos mensajes. - Esperar que la mensajería instantánea y de correo electrónico que se haya eliminado en el teléfono se la pueda reconocer y recopilar.
Aplicaciones Web	Determinar si la herramienta puede encontrar sitios Web visitados y la información que fue intercambiada a través del Internet. - Utilizar el dispositivo para visitar sitios web específicos y realizar consultas - Esperar que la información sobre la actividad Web se pueda comprobar y recopilar. - Eliminar selectivamente algunos datos, adquirir el contenido del dispositivo localizar y mostrar el URL* de los sitios visitados y los datos adquiridos asociados (por ejemplo, imágenes, texto).
Formato de Archivos de Texto, Gráficos y Archivos Comprimidos	Determinar si la herramienta puede buscar y mostrar una recopilación de archivos de texto, gráficos y archivos comprimidos, que residen en el teléfono incluyendo los archivos eliminados. - Cargar el dispositivo con varios tipos de archivos (texto, gráficos y/o archivos comprimidos) de forma selectiva. - Esperar que todos los archivos con los formatos de archivo de texto, gráficos y/o archivos comprimidos puedan ser encontrados y reportados. - Eliminar algunos archivos, adquirir el contenido del dispositivo, encontrar y reportar la información. - Esperar que los archivos recopilados que se haya eliminado en el teléfono se la pueda reconocer y recopilar.
Tarjetas de Memoria Periféricas	Determinar que la herramienta pueda adquirir, identificar y evaluar archivos almacenados o eliminados de forma individual en una tarjeta de memoria insertada en el dispositivo. - Insertar una tarjeta de memoria antes formateada que contenga archivos de texto, gráficos y archivos comprimidos en una ranura apropiada en el dispositivo. - Esperar que los archivos en la tarjeta de memoria, puedan ser debidamente adquiridos, encontrados y reportados.

	- Eliminar algunos archivos, encontrar y adquirir el contenido del dispositivo. - Esperar que los archivos en la tarjeta de memoria eliminados, puedan ser debidamente adquiridos, encontrados y reportados.
Coherencia de Adquisición	Determinar si la herramienta proporciona valores *hash* consistente en los archivos residentes en el dispositivo para dos adquisiciones continuas, es decir una después de la otra (*back-to-back):* - Adquirir los contenidos del dispositivo y crear un *hash* sobre la memoria, para la adquisición física, y sobre los archivos individuales, por adquisiciones lógicas. - Esperar que los *hashes* en los archivos individuales sean compatibles entre las dos adquisiciones, pero incompatibles para el *hash* de la memoria.
Perdidas de Energía	Determinar si la herramienta puede adquirir cualquier información del dispositivo después de que éste ha perdido su energía. - Vaciar completamente el aparato de su energía por agotamiento de batería. - Adquirir contenidos del equipo, buscar y mostrar nombres de archivos disponibles. - Esperar que ningún archivo del usuario, excepto en los contenidos en un periférico de tarjeta de memoria, pueden ser recuperados.

Tabla 3.6: Escenarios de análisis para las herramientas forenses en el dispositivo móvil

Se considerará un conjunto de escenarios distinto para las herramientas forenses de SIM. Los escenarios SIM difieren de los escenarios de teléfono de varias maneras. La SIM es un dispositivo con interfaces estandarizadas, con comportamiento y contenido diferentes al equipo móvil.

Todas las herramientas para tarjetas permiten la adquisición de datos a través de un lector externo. Por lo tanto, el énfasis en estos escenarios es sobre la carga de la memoria de la tarjeta SIM con tipos específicos de información para su recuperación, en lugar de la memoria del teléfono. La tabla 3.7 ofrece una visión

general de los escenarios SIM, incluyendo su propósito, el método de ejecución, y los resultados esperados.

Estos escenarios genéricos han sido concebidos para reflejar situaciones que se presentan durante un examen forense de estos dispositivos y sus medios de comunicación. Los escenarios están estructurados para revelar cómo las herramientas seleccionadas reaccionan en diversas situaciones.

Escenarios	Descripción
Datos Básicos	Determinar si la herramienta puede recuperar del usuario: IMSI, ICCID, SPN, ADN, LND y mensajes SMS relacionados en la tarjeta SIM, incluidas las entradas de borrado, y si todos los datos tienen una decodificación correcta. - Colocar en la tarjeta SIM información conocida como llamadas, mensajes SMS que estén relacionados con la información que se puede verificar después de su adquisición, a continuación remover el SIM para su análisis. - Esperar que toda la información que reside en la tarjeta SIM pueda ser exitosamente adquirida y reportada, inclusive la información borrada.
Información de Localización	Determinar si la herramienta puede recuperar información como LOCI y LOCIGPRS en la tarjeta SIM, y si todos los datos son correctamente mostrados y decodificados. Esta información localizada puede indicar que el dispositivo fue utilizado por última vez, para un determinado servicio y en redes que se puedan encontrar. - Registros relacionados con la ubicación de los datos de mantenimiento de red de la SIM para realizar operaciones de datos en lugares conocidos, luego retire la tarjeta SIM para realizar la adquisición y el análisis. - Esperar que todo lo relacionado con la ubicación de la información pueda ser exitosamente adquirido y reportado, inclusive la información borrada.

Tabla 3.7: Escenarios de análisis para las herramientas forenses en la tarjeta SIM

Se utilizaron escenarios genéricos en el análisis de las herramientas forenses, ya que estos procedimientos no están destinados a servir como prueba formal de un producto o como una evaluación completa de éstas.

3.3 HERRAMIENTAS UTILIZADAS SEGÚN LOS NIVELES DE ANÁLISIS

Para el análisis de la extracción de información del teléfono celular, se debe considerar que este tipo de información se encuentra retenida o almacenada en las memorias internas del mismo, además se puede encontrar información valiosa en la tarjeta SIM. Para analizar esta información se consideran los niveles de extracción de la información.

Existe documentación sobre diversos temas que rodean al manejo de la integridad de evidencia en teléfonos móviles, sin embargo, pocos fabricantes son capaces de aportar soluciones completas. Este tipo de investigación tiende a conducir a nuevas vías que deben ser exploradas y verificadas.

Es por eso, que se ha considerado un análisis sistemático de ciertas herramientas que pueden obtener evidencia de los dispositivos móviles y tarjetas SIM, realizando un principal enfoque de ciertas herramientas que se detallarán a continuación, especificando a qué nivel de análisis corresponde cada una.

3.3.1 HERRAMIENTA DE EXTRACCIÓN MANUAL

Para la adquisición manual de evidencia (datos probatorios) en teléfonos celulares, han sido desarrolladas varias herramientas con la finalidad de satisfacer la necesidad de los examinadores al analizar un dispositivo electrónico (teléfono celular) que no es compatible con ninguna otra herramienta de análisis.

Esta limitación puede ser causada debido al tipo de manufactura, fabricante, versiones o actualizaciones del dispositivo a ser analizado.

Las características principales de las técnicas que utilizan estas herramientas se las detalló en la sección 2.2.2, por lo que se procederá a analizar la herramienta de interés.

3.3.1.1 ZRT 2

Figura 3.3: Componentes físicos de ZRT 2

El ZRT 2 ayuda al investigador a extraer información específica del dispositivo electrónico, por medio de sus herramientas de:

a. ***Hardware*:** Una cámara Canon EOS de alta resolución con sus respectivos aditamentos (lentes de precisión, cables de microUSB/USB, de audio/video, de energía, adaptador AC, entre otros), dongle[47], mantel y brazo flexible FERNICO para la cámara y sujetador en la mesa.

b. ***Software*:** Posee un *software* especial que interactúa con la cámara, generando con ello reportes personalizados con la ayuda de plantillas predeterminadas.

ZRT 2 genera grandes beneficios en cuanto al ahorro de tiempo a través de la captura de imágenes, para ir evidenciando paso a paso la información que se obtiene en el equipo móvil y proceder a la respectiva incorporación de la información obtenida en un reporte.

El reporte es una combinación de la información obtenida en el monitor (imágenes, video) con la experticia del investigador al saber utilizar el dispositivo móvil; este reporte puede ser generado en .pdf, .html, entre otros.

[47] D*ongle* es una pequeña pieza de *hardware* que se conecta a un ordenador portátil y se utiliza como protección para el acceso a un *software*.

3.3.1.1.1 ¿Cómo trabaja esta herramienta?

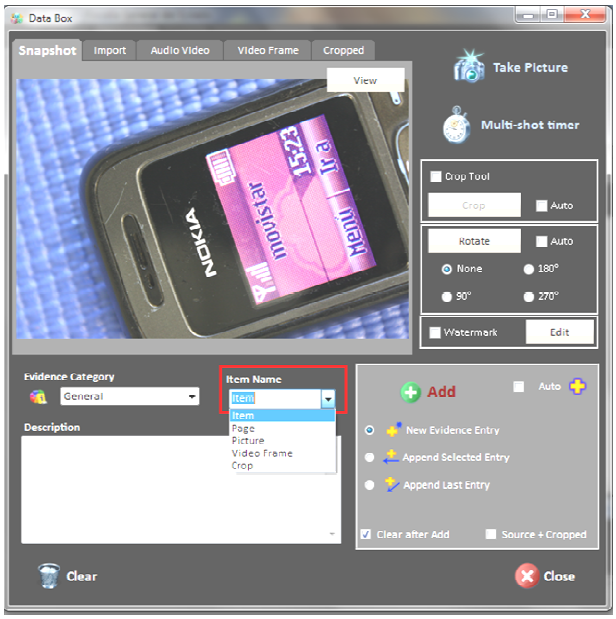


Figura 3.4: Adquisición de datos a través de imágenes

- Coloque el dispositivo celular a ser analizado en un área que pueda ser captada por el lente de la cámara, observe sus características físicas.
- Conecte la cámara y el computador con el cable *micro*USB/USB.
- Encienda la cámara con la opción de ajuste automático.
- Inicie el *software* ZRT 2.
- Elija la opción cámara y actualice la conexión de la misma escogiendo la cámara Canon EOS.
- Elija el generar un nuevo reporte.
- Llene los campos requeridos que se adapten al caso.
- Examinar la evidencia con ayuda de la captura de imágenes que considere de importancia; especifique la misma a través de campos especiales como por ejemplo, SMS recibido.
- Proceder a generar el respectivo reporte del caso.

3.3.1.1.2 Requerimientos del Sistema

- Windows XP, Vista, Windows 7 (64 or 32 bit).
- Puerto 2.0 USB.

3.3.1.1.3 Especificaciones

- Fuente de Energía: DC12V (±10%) con 120V AC 60hz de entrada.
- Imágenes por página 1, 2, 4, 6.
- Control automático de balances (enfoque).
- Calidad de imagen/video 720P/ 1080P.

3.3.1.1.4 Observaciones

- Para extraer información de forma manual, primero se debe revisar la documentación del teléfono celular y navegar previamente por los botones del móvil utilizando prenavegadores especiales o equipos con similares características.
- Debido a que es un dispositivo de captura física con interacción manual, no se va a poder obtener información de dispositivos que están bloqueados.
- Para obtener datos específicos como el IMEI se deberá utilizar comandos especiales tales como *#06#.
- A las imágenes capturadas por la herramienta se les asigna un código *hash* (MD5, SHA1, SHA256, entre otros) para evitar que sean vulneradas; esta información se puede verificar con el uso de herramientas especiales, como HELIX3[48] o EnCase.[49]

[48] *HELIX3* es una empresa desarrollada por expertos en informática forense. Recoge imágenes forenses de sistemas, incluyendo memoria RAM en múltiples plataformas, los procesos en ejecución, las variables de entorno y mucho más,

[49] *EnCase,* es un producto forense informático producido por Guidance Software, utilizado para analizar los medios de comunicación digitales.

- Si se cierra accidentalmente la herramienta de *software*, se guardará parte de la información como los datos capturados, pero no los campos llenados por el usuario.

3.3.2 HERRAMIENTAS DE EXTRACCIÓN LÓGICA[50]

En este nivel de análisis, se detallarán herramientas forenses como OPM II forense, *Device Seizure*, *SIM Seizure* y *Secure View*.

3.3.2.1 *Oxygen Phone Manager Forensic Suite* II

Figura 3.5: *Oxygen Forensic Suite* 2011

OPM II es una herramienta de *software* forense, que permite analizar dispositivos móviles y teléfonos inteligentes, que va más allá del análisis estándar lógico, por medio de protocolos propietarios, permitiendo extraer información como: agenda, llamadas (perdidas, marcadas y recibidas), SMS, *e-mail*, MMS; además recupera información de los dispositivos con un sistema de Geo-posición, entre otros datos.

3.3.2.1.1 *¿Cómo trabaja esta herramienta?*

- Para extraer información del dispositivo móvil, se debe elegir el medio de conexión (*Bluetooth*, IrDA, cable).

[50] Las imágenes que se presentan en esta sección, son capturas de pantalla obtenidas mientras eran utilizadas las herramientas.

Figura 3.6: Menú de Interfaces OPM II

- Se procede al reconocimiento del dispositivo móvil, y se muestra cierta información del dispositivo.

Figura 3.7: Reconocimiento exitoso del teléfono celular

- Se debe identificar el dispositivo (investigador, caso, algoritmo *hash*).

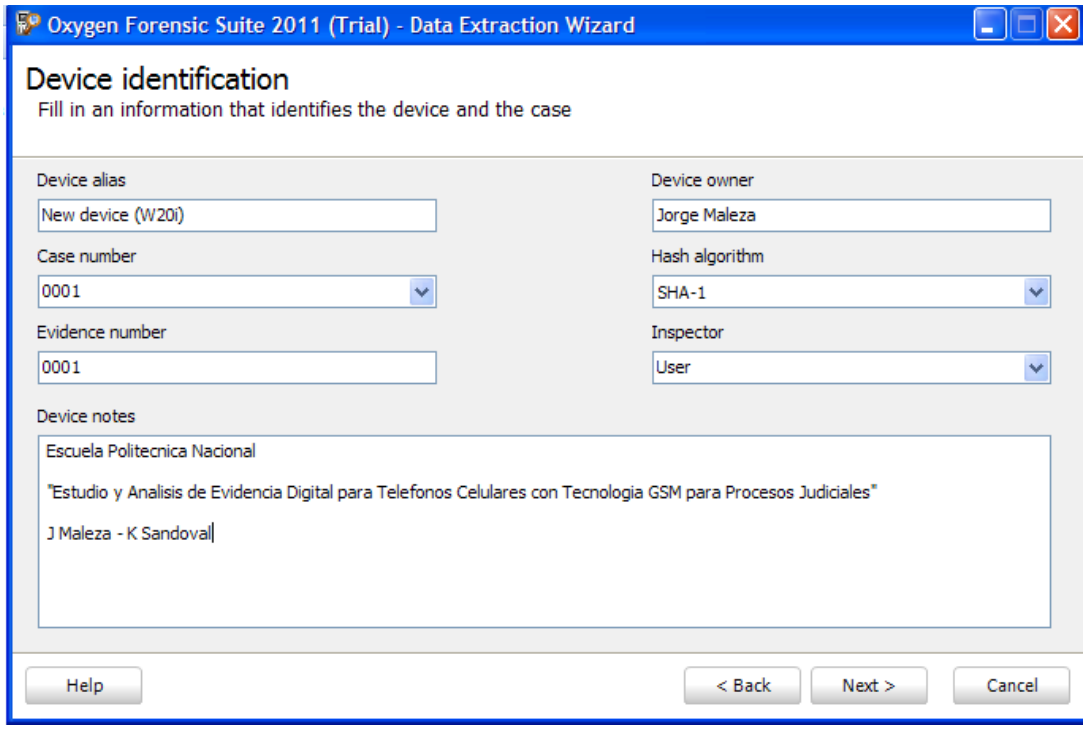


Figura 3.8: Identificador del dispositivo celular

- Seleccionar la información que se desea obtener.

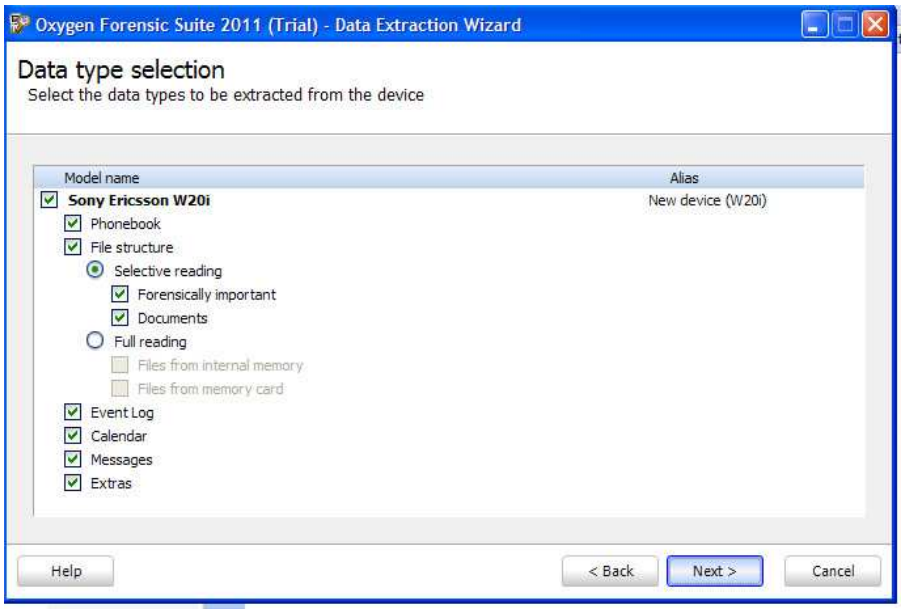


Figura 3.9: Selección de datos a extraer en el teléfono celular

- Analiza el dispositivo a tratar y muestra la información obtenida en el programa y en reporte.

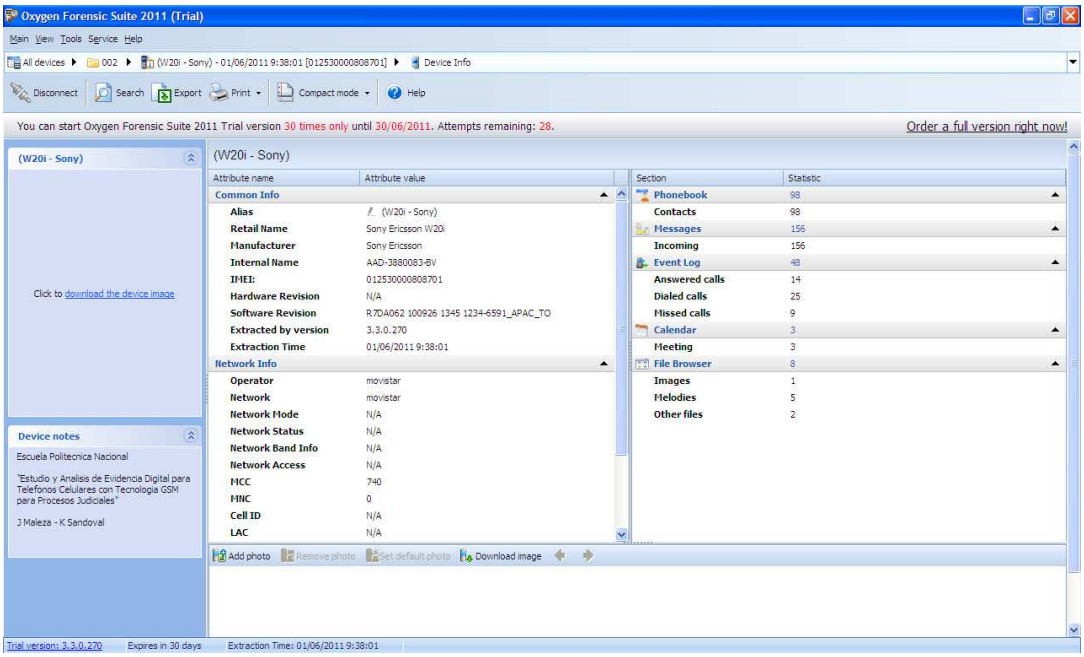


Figura 3.10: Información general recopilada del dispositivo analizado

3.3.2.1.2 Requerimientos del Sistema

- 128 MB RAM
- Celerón 2 GHz
- 256 MB de espacio en el Disco Duro
- SO: *Windows* 7, *Windows Vista*, *Windows* XP, *Windows* 2000 y *Windows Server* 2003.

3.3.2.1.3 Observaciones

- Para utilizar esta herramienta, se debe instalar previamente los *drivers* de los teléfonos celulares a ser analizados.
- OPM II puede recuperar SMS borrados si éstos no tienen un período mayor a 30 días.

- Obtiene información con detalle de GPS en teléfonos inteligente relacionados a imágenes, llamadas y mensajes.
- La herramienta no puede analizar un dispositivo si éste se encuentra bloqueado.
- Se puede elegir el tipo de código *hash* (MD5, SHA-1, SHA-2, entre otros) a utilizar en el análisis del dispositivo.
- Genera reportes en varios formatos como CSV[51], PDF, RTF[52], XML, TSV[53] y XLS.

3.3.2.2 *Device* y SIM *Card Seizure* (*Paraben*)

Estas herramientas forenses sirven para la adquisición de información de varios dispositivos incluidos los teléfonos, dispositivos GPS y tarjetas SIM. El paquete está diseñado para apoyar la adquisición completa de información, y el proceso de investigación, destacándose por la capacidad para realizar adquisición física de algunos teléfonos, lo cual permite recuperar datos eliminados.

Usando estas herramientas se pueden extraer los datos como (historial de mensajes de texto (recibidos, enviados, eliminados), agenda telefónica (almacenados en la memoria del dispositivo o en la tarjeta SIM), registro y datos de llamadas (recibidas, realizadas y perdidas), calendario, entre otros.

Estas herramientas de *Paraben* pueden almacenar la información de cada caso y de los investigadores relacionados con él; además cuando la adquisición es finalizada, se presenta al investigador una interfaz de usuario donde se muestran las propiedades de los datos adquiridos junto con un código *hash* de MD5 y/o SHA1.

---

[51] *CSV,* fichero generado con el programa *Microsoft Outlook Express*.

[52] *RTF,* formato de archivo de texto enriquecido que permite intercambiar texto entre distintos procesadores de texto y en distintos sistemas operativos.

[53] *TSV,* este tipo de archivo a menudo se asocia con *Microsoft Excel*, ya que es una de las formas estándar para transferir datos hacia y desde una hoja de cálculo.

Este *software* es bastante robusto y está dirigido a múltiples plataformas computacionales. La versión para dispositivos móviles se denomina "*Device Seizure*" y permite hacer análisis forense de un gran número de dispositivos y el "SIM *Card Seizure*" es para el análisis de tarjetas SIM.

3.3.2.2.1 ¿Cómo trabajan estas herramientas?

a. *Device Seizure*

- Al iniciar esta herramienta, se debe generar un nuevo caso, e introducir los datos del caso conocidos hasta el momento.

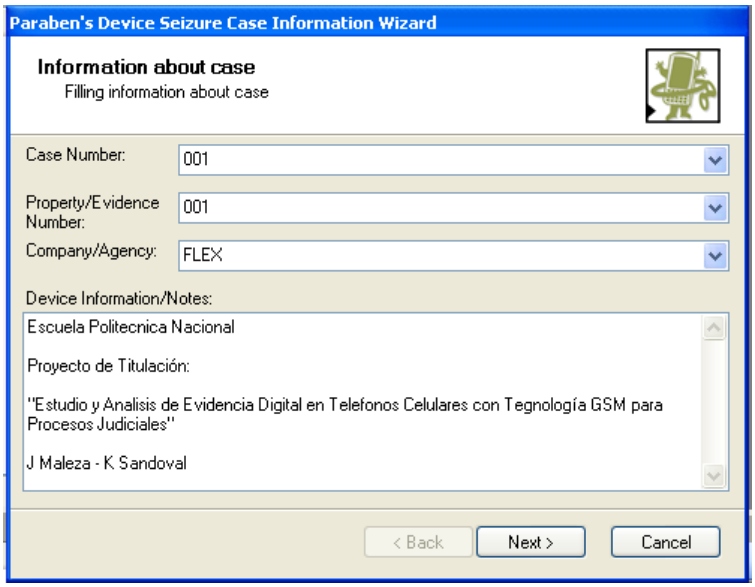


Figura 3.11: Información general del caso

- Introducir información relacionada al examinador, esto es, la persona que lleva a cabo el análisis.

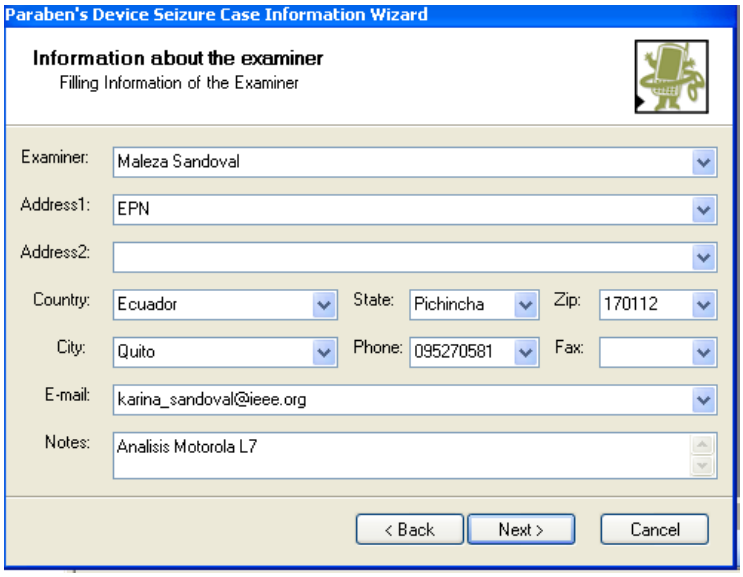


Figura 3.12: Información sobre el examinador

- Se elige al fabricante del dispositivo móvil a analizar, considerando si se desea realizar una adquisición física o lógica.

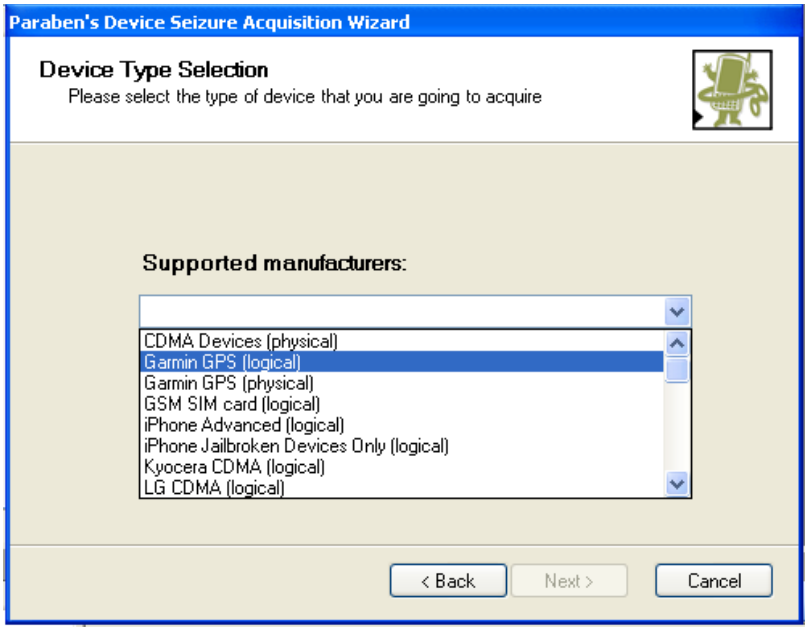


Figura 3.13: Seleccionar la interfaz que se analizará física o lógica

- Proceder a elegir el tipo de conexión que se realizará.

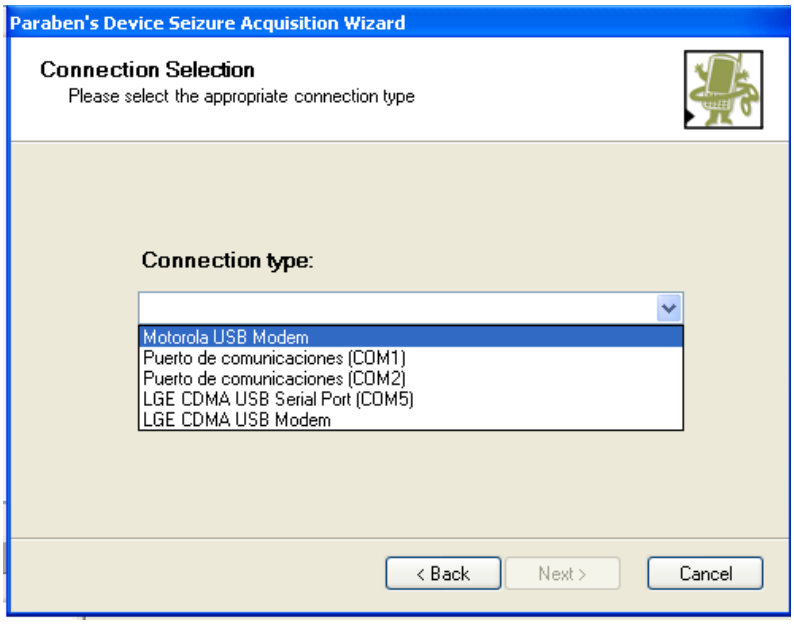


Figura 3.14 Seleccionar el tipo de conexión

- Además el investigador debe elegir la información que desea adquirir.
  - Adquisición lógica

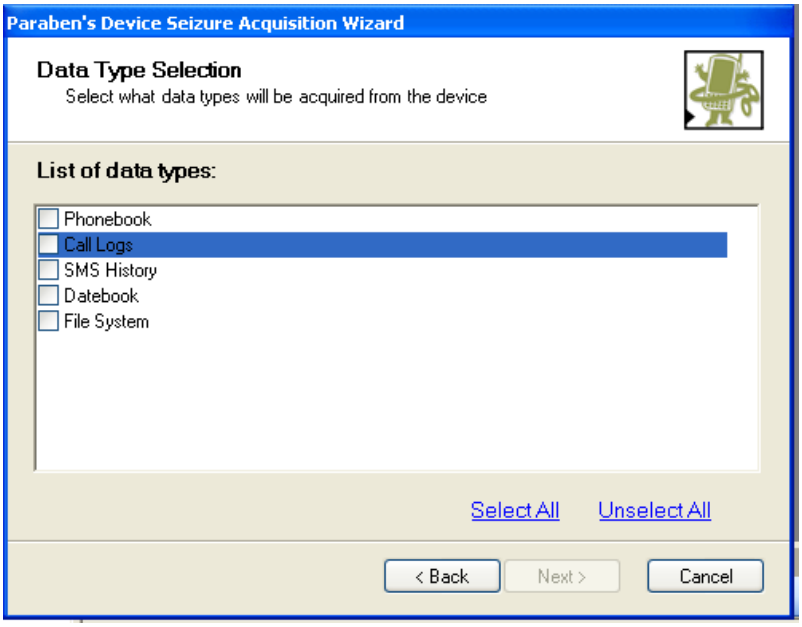


Figura 3.15: Selección de datos para un análisis de datos lógico

- Adquisición física

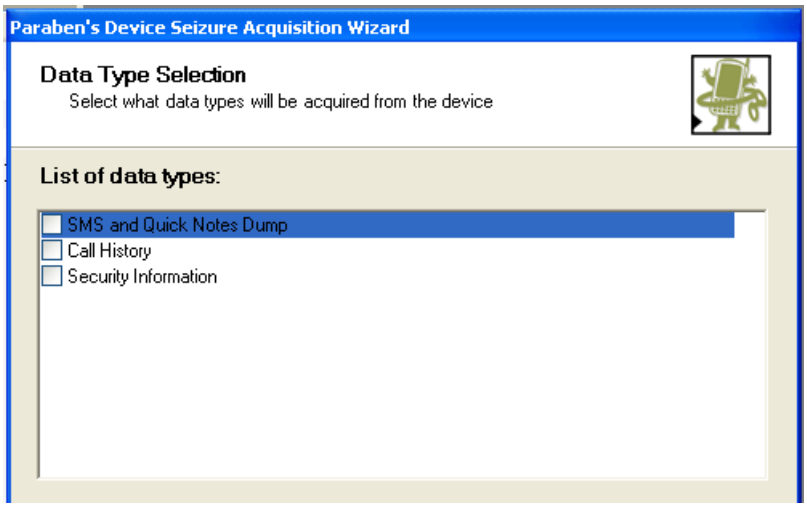


Figura 3.16: Selección de datos para un análisis de datos físico

- Analiza y recupera la información analizada en el dispositivo.
- Genera un reporte con la información obtenida.

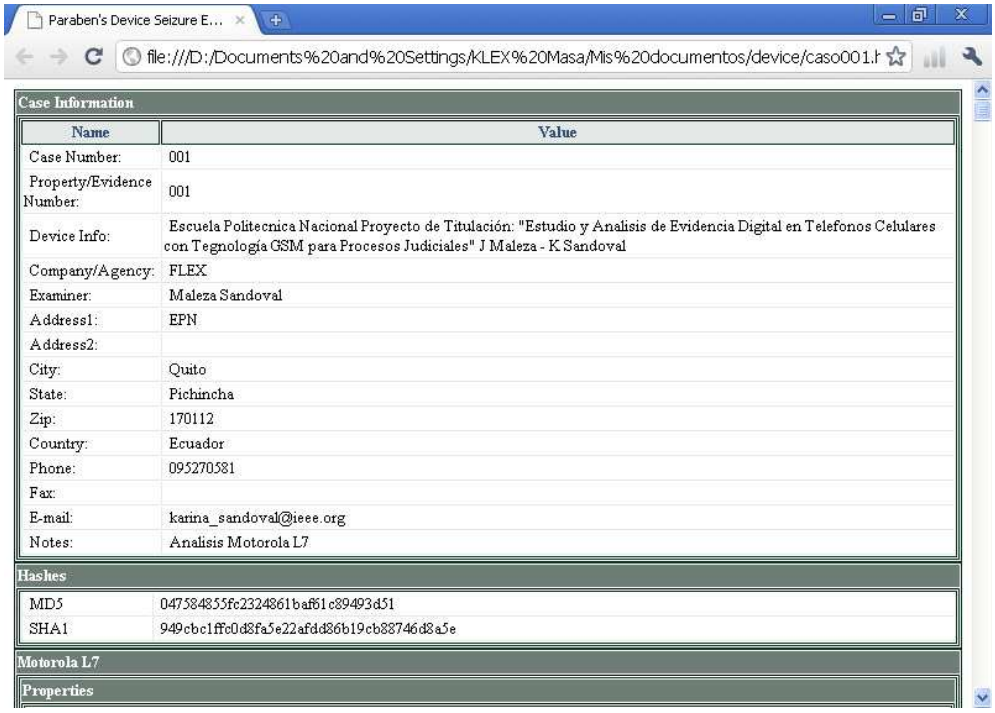


Figura 3.17: Reporte generado por *Device Seizure* en formato HTML

b. SIM *Card Seizure*

- Al iniciar esta herramienta, se debe generar un nuevo caso, e introducir los datos del caso conocidos hasta ese momento.

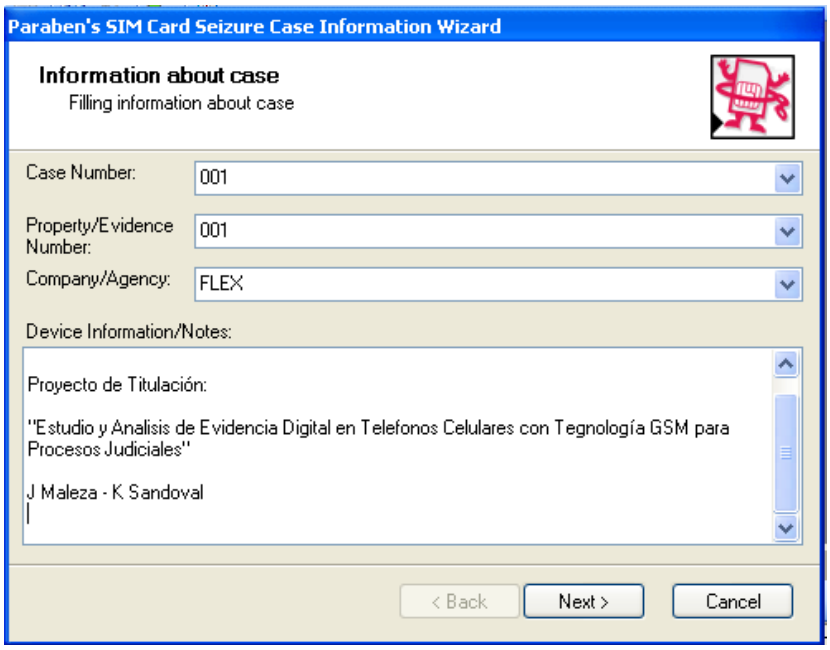


Figura 3.18: Información general del caso

- Introducir información relacionada al investigador, esto es la persona que lleva a cabo el análisis.

- Proceder a realizar el análisis de la Tarjeta SIM, para lo cual se utiliza un lector de tarjetas SIM como el *"Dekart SIM Manager"*[54].

[54] *Dekart SIM Manager* es una herramienta que permite administrar, leer, y editar el contenidola tarjeta SIM, además de crear y restaurar copias de seguridad del directorio telefónico, activar, cambiar o desbloquear el código PIN (PIN1/PIN2); gestionar otros sectores de la tarjeta SIM (archivo de SMS, números telefónicos, etc.)

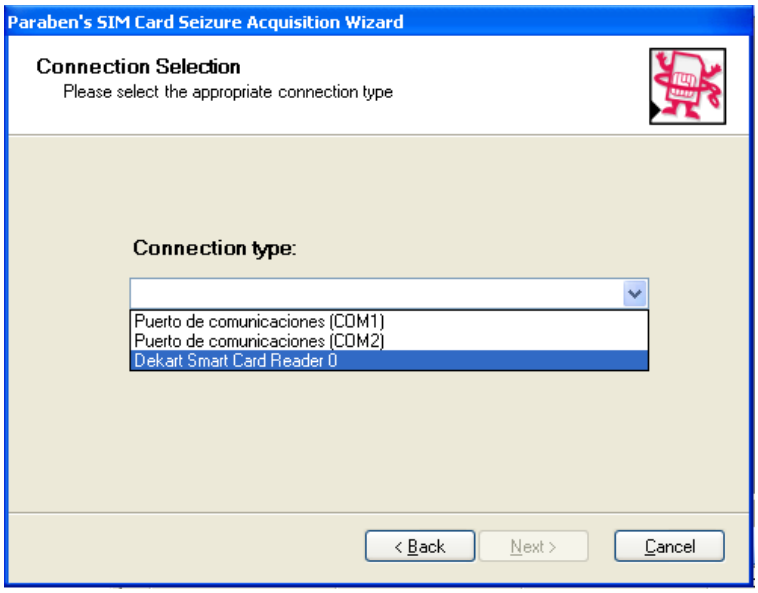


Figura 3.19: Seleccionar el tipo de conexión

- Elija la información que desea extraer de la tarjeta a analizar.

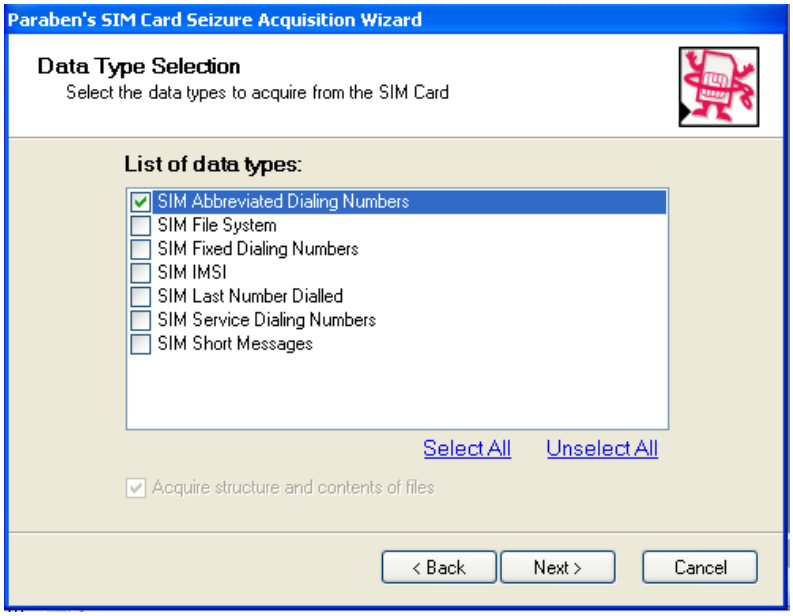


Figura 3.20: Seleccionar el tipo de información que se analizará en la tarjeta SIM

- La herramienta analiza la información obtenida de forma satisfactoria.

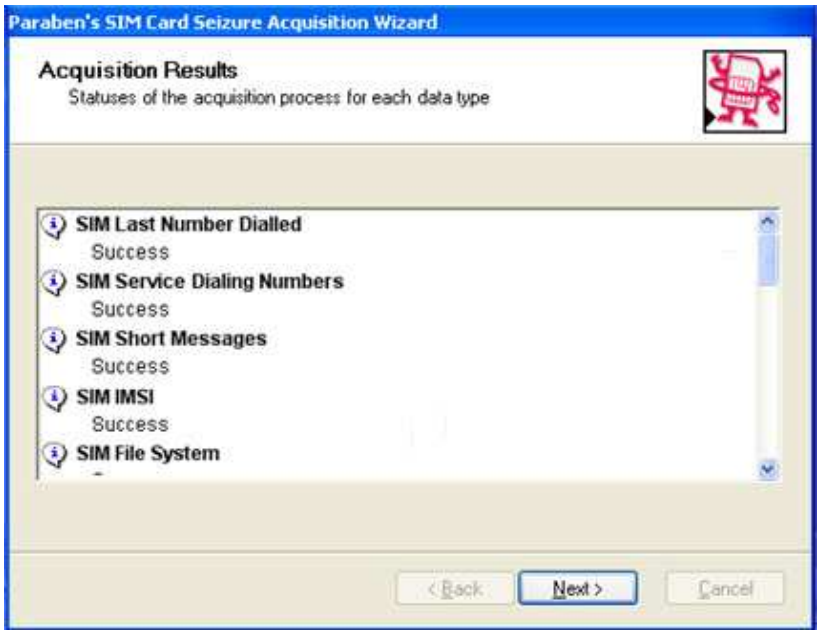


Figura 3.21: Información obtenida de manera exitosa de la Tarjeta SIM

- Presenta la información obtenida en la pantalla principal del programa SIM *Card Seizure*.

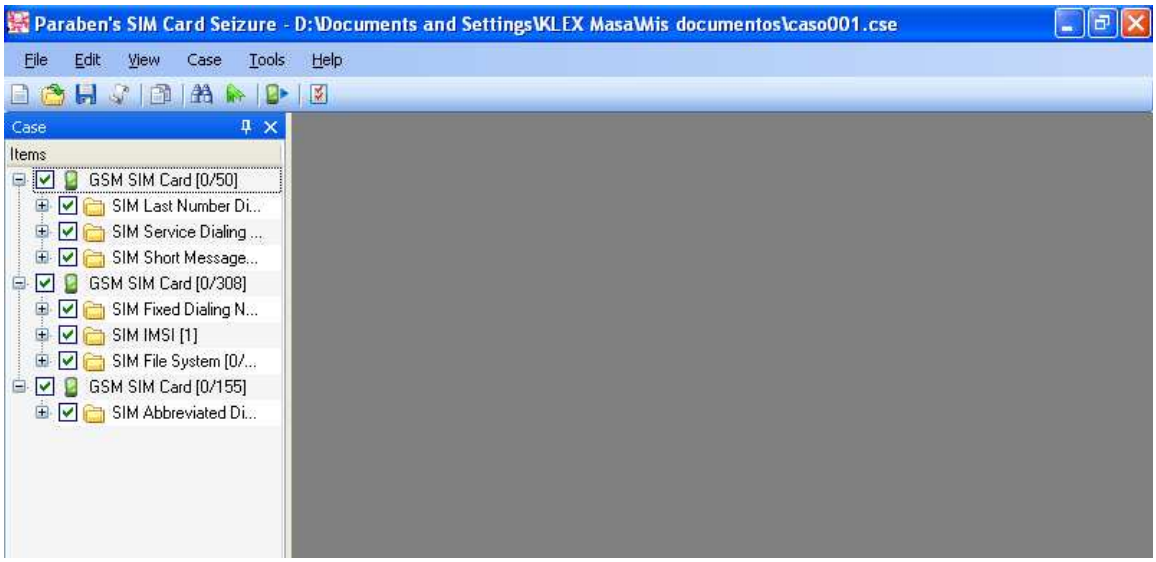


Figura 3.22: Interfaz con información obtenida en la Tarjeta SIM

- Para generar un reporte se puede elegir entre varios formatos.

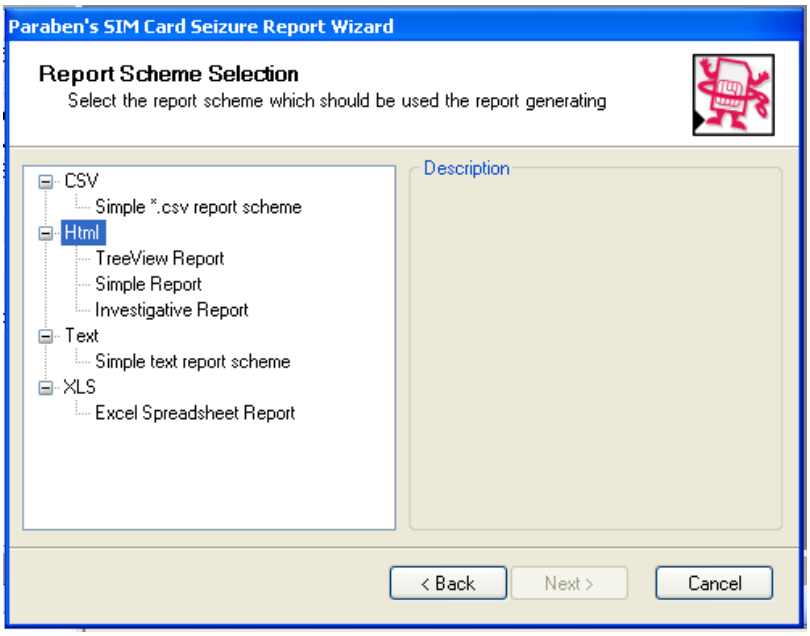


Figura 3.23: Selección del tipo de reporte a presentar

- Finalmente se obtiene el reporte.

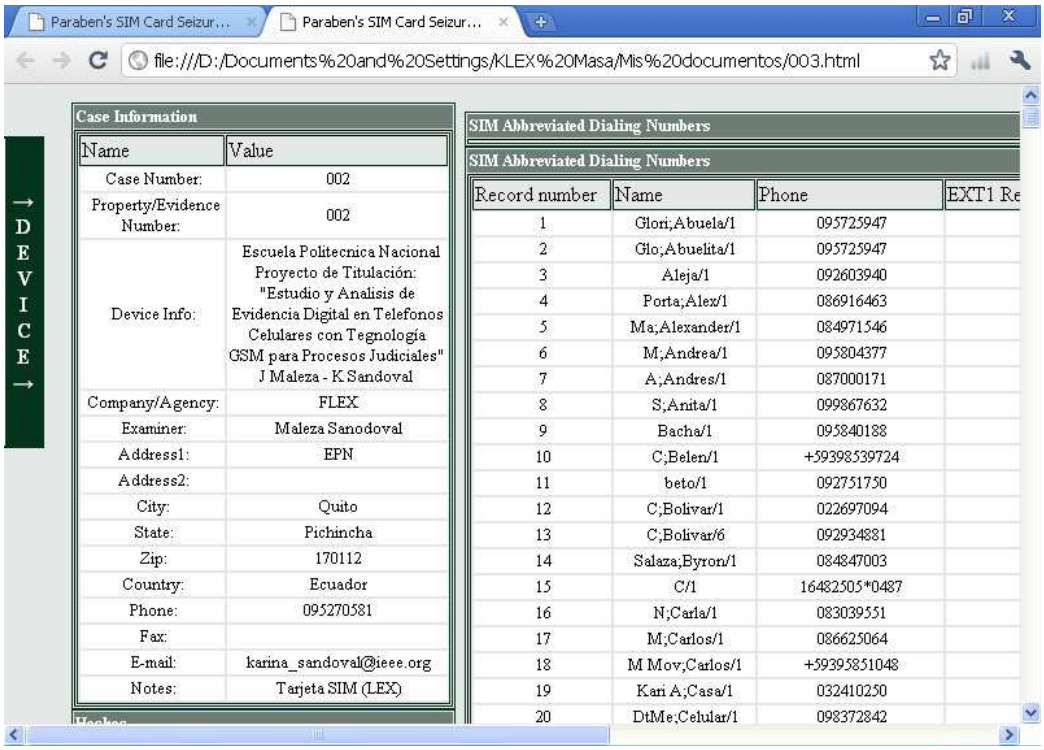


Figura 3.24: Reporte generado por SIM *Card Seizure* en formato HTML

3.3.2.2.2 Requerimientos del Sistema

a) Device Seizure

- Procesador de 1.4 GHz+
- RAM de 1 GB
- Espacio disponible en el disco de 200 MB
- SO: *Windows* 2000, XP, 2003, Vista, *Windows* 7 32 Bit y *Support* 64 Bit.
- *Windows* .NET *Framework* 2.0

b) SIM Card Seizure

- SO: *Microsoft Windows* 2000 or later 32 bit OS.
- RAM de 1 GB, (1.5 GB recomendada)
- *Windows Net Framework* version 2.1

3.3.2.2.3 Observaciones

- Para utilizar esta herramienta, se deben instalar previamente los *drivers* de los teléfonos celulares a ser analizados.
- Al trabajar con SIM *Card* y *Device Seizure*, se puede buscar información o datos específicos y observar dónde se encuentra localizada esta información, por ejemplo en SMS o llamadas.
- La información obtenida de la tarjeta SIM puede ser obtenida en formato binario, hexadecimal o texto normal.
- La información obtenida del dispositivo analizado (tarjeta SIM y teléfono celular) es almacenada en subcarpetas, manteniendo la codificación *hash* asignada, a fin de precautelar y no evidenciar cambio alguno en la información obtenida.

- *Device Seizure* ofrece diferentes opciones para seleccionar y analizar información deseada, según el dispositivo móvil a analizar.
- *Device Seizure* solo soporta interfaz de cable.

3.3.2.3 *Secure View* 2.0 (SV2)

Figura 3.25: Interfaz de la herramienta *Secure View*

SV2 es una herramienta forense de *software* que ayuda a analizar diferentes dispositivos como teléfonos móviles, tarjetas extraíbles y tarjetas SIM; soporta alrededor de 650 diferentes modelos de Norte América y Europa.

SV2 realiza un análisis externo a dispositivos móviles muy similar al tratamiento de análisis de las memorias externas. Además permite obtener información como: IMEI, agenda, contactos, llamadas recibidas, marcadas y perdidas. Esta información es guardada y reportada de manera automática en el computador, con un código *hash* MD5.

3.3.2.3.1 ¿Cómo trabaja esta herramienta?

Figura 3.26: Menú de Secure View

SV2 muestra un menú con varias opciones, las mismas que se explicarán brevemente a continuación:

a. Dispositivo Móvil

Figura 3.27: Menú de medio de comunicación para extracción de información

- Seleccionar el medio de comunicación, la interfaz (USB, cable serial, IrDA, *Bluetooth*).
- Seleccionar el país donde el teléfono funciona y su operadora.
- Extraer la información del dispositivo móvil (llamadas, mensajes, agenda).
- Muestra un reporte de la extracción realizada.

b. *Memory Card*

- Se selecciona el dispositivo de análisis (G:/, H:/)
- Se analiza la unidad y se extrae su información.
- Se despliega un reporte de la extracción.

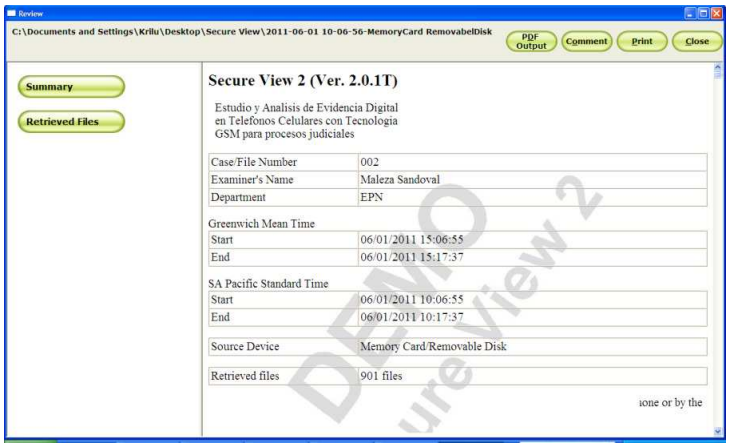


Figura 3.28: Reporte de Secure View de la *Memory Card*

c. SIM Card

- Para leer la tarjeta SIM se utiliza un lector de tarjetas SIM, en este caso se utilizó la herramienta "*Dekart SIM Manager*".
- SV2 procede a extraer la información de la tarjeta SIM.
- Muestra un reporte de la extracción.

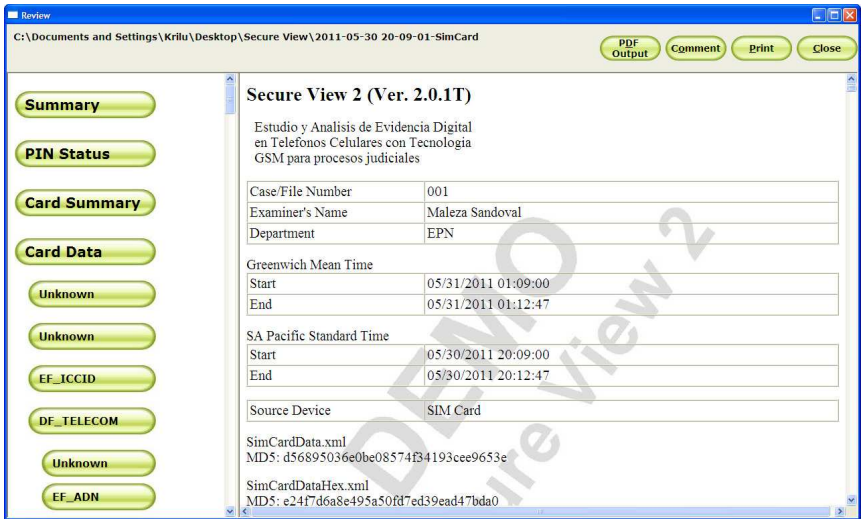


Figura 3.29: Reporte generado por análisis de Tarjeta SIM

d. svProbe

- Busca información específica (contactos, llamadas, SMS).

- Relaciona los datos y establece gráficas comparativas.

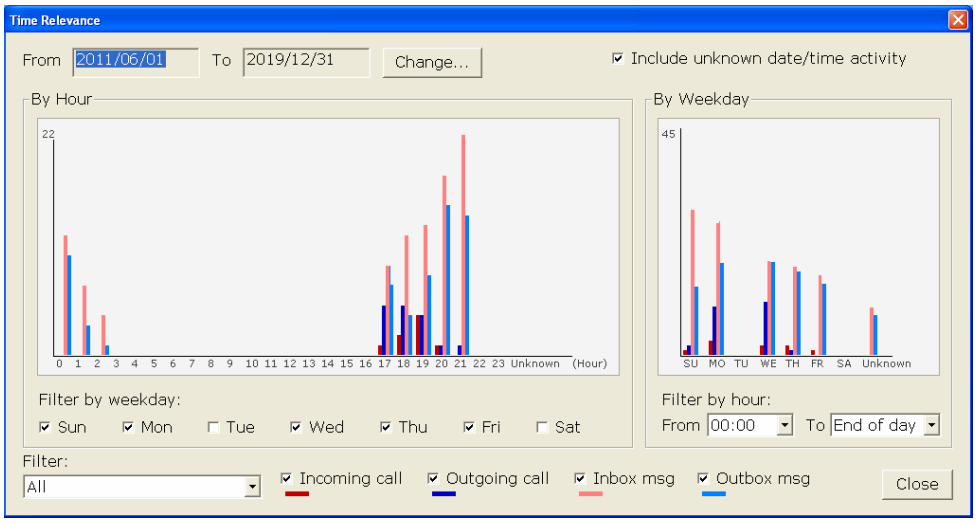


Figura 3.30: Filtración de Información obtenida del usuario

e. Reporte

- Muestra la información extraída del dispositivo electrónico en diferentes formatos.

3.3.2.3.2 Requerimientos del Sistema

- *Microsoft Windows* 2000 con SP3 or XP
- Procesador de 133 MHz
- 128 MB RAM
- Espacio disponible en el disco de 30 MB
- Resolución de 800 x 600, 8-*bit* (256 colores)
- Puerto USB

3.3.2.3.3 Observaciones

- Permite trabajar con un buscador (svProbe) que ayuda al investigador a encontrar, relacionar y graficar información perteneciente a un usuario o

dato específico, en cuanto a llamadas recibidas, marcadas y mensajes enviados y recibidos.

- Es compatible con los formatos de reportes de otras herramientas forenses como *Paraben* y *Cellebrite.*
- Recupera información de las memorias extraíbles analizadas, aunque éstas hayan sido formateadas.
- Para analizar dispositivos móviles, SV2 ofrece una variedad de dispositivos que se encuentran clasificados por operador y país, limitando sus funciones y por ende las herramientas del investigador.
- Al analizar las tarjetas SIM, la herramienta ofrece una gama de resultados, los mismos que muestran con una localidad de memoria específica para cada campo; también obtiene los datos bit a bit, realizando un breve volcado de memoria.

3.3.3 HERRAMIENTAS DE ANÁLISIS FÍSICO[55]

3.3.3.1 UFED (*CelleBrite*)

Figura 3.31: Herramienta UFED en funcionamiento

Cellebrite UFED es un dispositivo capaz de adquirir datos desde dispositivos móviles y almacenar la información en una unidad USB, tarjeta SD o en el

[55] Las fotografías que se presentan en esta sección, fueron obtenidas mientras era utilizada la herramienta.

computador. Además UFED incorpora un lector y generador de copias de tarjetas SIM.

Permite extraer información como: contactos, mensajes de textos (recibidos, enviados y eliminados), historial de llamadas, grabaciones de audio y video, fotos, entre otros. Cellebrite incluye UFED *Report Manager*, el cual provee una interfaz para realizar reportes sobre las investigaciones y exportar dichos reportes en diferentes formatos; realiza una codificación *hash* de MD5 y SHA-256.

3.3.3.1.1 ¿Cómo trabaja esta herramienta?

La adquisición forense en los dispositivos móviles se pueden realizar de dos formas, una es la estándar y la otra es mediante el volcado de memoria. Este proceso es rápido y simple con esta herramienta. Después de encender el dispositivo, se deben seguir los siguientes pasos:

a. Dispositivos Móviles

Figura 3.32: Menú principal de UFED

- Seleccionar “Extraer datos del teléfono”.
- Seleccionar el dispositivo móvil de interés.

Figura 3.33: Dispositivos móviles compatibles con la herramienta

- Seleccionar la unidad destino (PC, Tarjeta SD, USB).

Figura 3.34: Menú seleccionador de destino de la información que obtendrá UFED

- Seleccionar los tipos de contenido (registros de llamadas incluidas, agenda, SMS, fotos, videos, audio/música, entre otros).

Figura 3.35: Seleccionar la información que obtendrá UFED del dispositivo móvil

- Conectar el dispositivo con el puerto origen con el cable de conexión sugerido y la memoria USB en el puerto destino.
- Analiza y extrae la información del dispositivo.

Figura 3.36: Extrayendo información del dispositivo móvil

- Muestra en reporte de la información obtenida.

Phone Examination Report Properties

Selected Manufacturer:	LG GSM
Selected Model:	LG CU920 Vu
Detected Manufacturer:	LG ELECTRONICS
Detected Model:	CU920
Revision:	CU920-MSM4090201D-V10s-DEC-12-2008-ATT-US 1 [Nov 10 2008 23:00:00]
IMEI:	011847000055180
IMSI:	740000200899737
Extraction start date/time:	04/05/11 10:38:15
Extraction end date/time:	04/05/11 10:43:43
Phone Date/Time:	"80/01/30,18:32:12"
Connection Type:	USB Cable
UFED Version:	Software: 1.1.7.0 UFED , Full Image: 1.0.2.4 , Tiny Image: 1.0.2.1
UFED S/N:	5571002

Figura 3.37: Reporte generado por UFED

b. Tarjeta SIM

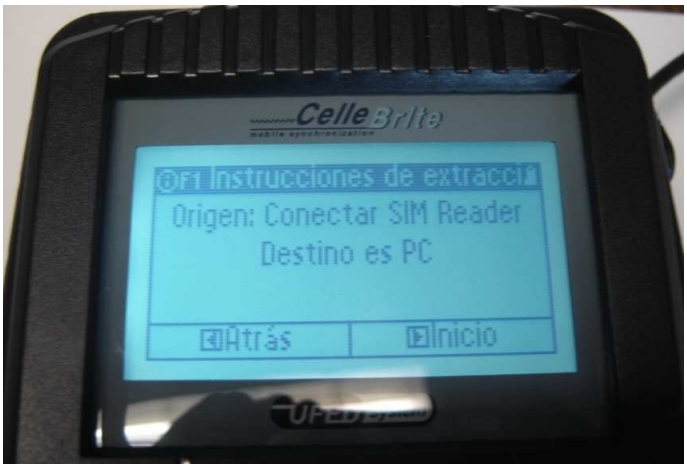


Figura 3.38: Insertar la tarjeta SIM antes de la extracción de información

- Se debe retirar la tarjeta SIM del dispositivo móvil e insertarla en la herramienta.

Figura 3.39: Tarjeta SIM insertada de forma adecuada

- Los contactos de la tarjeta SIM debe estar vista hacia abajo y la esquina recortada orientada hacia el examinador.
- Seleccionar la unidad de destino y el contenido que se desea analizar (registros de llamadas, SMS, entre otros).
- Analiza y extrae la información de la tarjeta SIM.
- Presenta la información obtenida en un reporte.

c. Extraer contraseñas

- Elegir el dispositivo móvil para realizar el análisis.
- Conectar el dispositivo móvil con el cable o interfaz sugerida por UFED.
- Proceder a realizar el análisis del dispositivo.

- Mostrar las diferentes contraseñas que posee el dispositivo analizado.

3.3.3.1.2 Especificaciones

- Fuente de alimentación: Entrada: CA 100–240 V, 50/60 Hz Salida: CC 12 V, 2 A

3.3.3.1.3 Requerimientos del Sistema

- SO: *Microsoft Windows* CE, *Windows* 2000, XP, 2003, Vista, *Windows* 7 32 *Bit* OS *Support* 64 *Bit*.
- Controlador de Eternet de (10/100 Mbps)

3.3.3.1.4 Observaciones

- Para utilizar la herramienta UFED se debe cerciorar que esté actualizada, para un mejor funcionamiento.
- UFED permite realizar dos métodos de adquisición de los datos del dispositivo móvil (análisis lógico y físico)
- UFED permite analizar información en teléfonos inteligentes (modo de cliente) a través de la instalación de un agente especial.
- La herramienta presenta inconvenientes para ciertos modelos de teléfonos celulares bloqueados.
- Al elegir la interfaz de USB o tarjeta SD para extraer información del dispositivo móvil, se muestra en la pantalla de la herramienta el IMEI del dispositivo.

3.4 ANÁLISIS COMPARATIVO DE LAS HERRAMIENTAS UTILIZADAS

El propósito de las herramientas forenses para teléfonos celulares es el de obtener datos del equipo móvil sin tener la necesidad de modificarlos o alterar los datos. Las herramientas deben proporcionar actualizaciones acorde a los cambios

que surgen en dispositivos móviles, ya sea a nivel de *software* y/o *hardware*. Las herramientas forenses actúan bajo diferentes circunstancias con diversas características, por lo que aunque sean herramientas del mismo nivel de análisis, presentan características e información diferente.

Al contar con diversas características, se analizó en un mismo entorno (escenarios) con la finalidad de encontrar circunstancias bajo las cuales actuarían de forma similar, dando apertura al criterio y experticia del examinador al momento de elegir la herramienta de trabajo.

En la Tabla 3.8, se muestra el comportamiento de las herramientas analizadas bajo diversos escenarios, cuando la información del dispositivo estaba almacenada, sin que exista modificación en dato alguno.

Para lo cual se utiliza la siguiente descripción, bajo los escenarios de análisis:

N/A El escenario propuesto, no tiene relación o aplicación alguna, bajo las características de las herramientas.

(*) El escenario propuesto, se cumplió a cabalidad por las herramientas, pero fue exitoso en pocos de los dispositivos analizados.

X El escenario propuesto, se cumplió a cabalidad por las herramientas en los dispositivos analizados.

(-) El escenario propuesto no se cumplió a cabalidad por las herramientas en los dispositivos analizados.

Escenario	**Herramientas Forenses Analizadas**					
	UFED	**Device Seizure**	**SIM Card Seizure**	**OPM**	**Secure View**	**ZTR 2**
Hex Dump/ Extracción Lógica	*	X	X	N/A	X	N/A
Conectividad y Recuperación	-	*	N/A	*	*	N/A
Aplicaciones PIM	X	X	-	*	-	X
Llamadas Marcadas/Recibidas	X	X	X	*	X	X
Mensajes SMS/MMS	X	X	X	*	X	X

Mensajes de Internet	-	-	N/A	*	N/A	X
Aplicaciones Web	-	-	N/A	-	N/A	X
Formato de Archivos de Texto, Gráficos y Archivos Comprimidos	X	X	N/A	*	N/A	X
Tarjetas de Memoria Periféricas	X	X	N/A	*	X	X
Coherencia de Adquisición	X	X	X	X	X	X
Pérdidas de Energía	-	*	N/A	-	N/A	N/A
Datos Básicos	X	N/A	X	X	X	N/A
Información Localizada	X	N/A	X	X	X	N/A

Tabla 3.8: Herramientas vs Escenarios (Información creada y recolectada)

Escenario	**Herramientas Analizadas**					
	UFED	**Device Seizure**	**SIM Card Seizure**	**OPM**	**Secure View**	**ZTR 2**
Hex Dump/ Extracción Lógica	X	X	X	N/A	X	N/A
Conectividad y Recuperación	-	*	N/A	*	N/A	N/A
Aplicaciones PIM	-	X	-	-	-	N/A
Llamadas Marcadas/Recibidas	X	X	X	*	X	N/A
Mensajes SMS/MMS	X	X	X	*	X	N/A
Mensajes de Internet	-	-	N/A	*	N/A	N/A
Aplicaciones Web	-	-	N/A	-	N/A	N/A
Formato de Archivos de Texto, Gráficos y Archivos Comprimidos	X	X	N/A	*	N/A	N/A
Tarjetas de Memoria Periféricas	X	X	N/A	*	X	N/A
Coherencia de Adquisición	X	X	X	X	X	N/A
Perdidas de Energía	-	-	N/A	-	N/A	N/A
Datos Básicos	X	N/A	X	X	X	N/A
Información Localizada	X	N/A	X	X	X	N/A

Tabla 3.9: Herramientas vs Escenarios (Información eliminada y recolectada)

La Tabla 3.9 muestra, cómo reaccionaron las herramientas utilizadas, al agregar y/o eliminar cierta información en el dispositivo a ser analizado, para comprobar la recuperación de la información establecida, en los escenarios sugeridos para este análisis.

Como se evidencia, existen diferencias entre las diversas herramientas y dispositivos móviles analizados, es papel fundamental del investigador el conocimiento de las funcionalidades de la herramienta a utilizar y las limitaciones que estas presentan bajo ciertos dispositivos móviles.

Al realizar el análisis de cada una de las herramientas forenses con los dispositivos meta seleccionados, se llega a evidenciar, como sí se puede extraer información de dispositivos móviles con la finalidad de utilizarla ante un juzgado, dando fe de su veracidad por medio de los diferentes valores de cifrado como los códigos *hash.*

CAPÍTULO IV

CAPÍTULO 4

4. PROCEDIMIENTOS Y PRINCIPIOS TÉCNICO-LEGALES APLICABLES AL ANÁLISIS FORENSE CELULAR EN EL ECUADOR

La inserción en el mundo de la tecnología ha hecho que ésta participe como objeto o medio en varias actividades humanas, sean éstas lícitas o ilícitas, haciendo que los conceptos tradicionales de investigación judicial, tengan que ampliarse para entender conceptos digitales y un mundo de bits.

Hay que reconocer que gran parte de la estructura legal Ecuatoriana está orientada a un mundo físico y/o material; sin embargo en Ecuador se está tratando de entender la regulación que se podría aplicar en un mundo digital.

En algunos países no se cree necesario contar con cuerpos normativos sobre materia tecnológica, por la falsa creencia que las normativas existentes pueden regular estas conductas delictivas que involucran tecnología.

Cuando el investigador se enfrenta con una "escena del hecho[56]" (escena del crimen o escena del delito) donde existen teléfonos celulares, debe suponer que esos dispositivos son sinónimo de un mundo virtual, dando lugar a una forma particular de investigación, la cual se ha denominado como "*Cellphone Forensics*" o Análisis Forense de Teléfonos Celulares.

Se debe tener en cuenta, que la evidencia digital presenta particularidades, no solo conceptuales sino relacionadas con el medio físico que lo soporta, que es electrónico; puede sufrir alteraciones o daños al ser apagado, trasladado, encendido o cualquier otra acción casual o intencional.

[56] *Hecho* es lo realmente sucedido, sin comentarios, opiniones ni previsión de consecuencias. La *escena del hecho*, es el lugar donde presuntamente se han cometido actos contrarios al ordenamiento normativo o Jurídico Penal.

Estas características definen a la evidencia digital como evidencia volátil y dinámica, ya que un conjunto de fenómenos físicos influyen directamente sobre la evidencia.

Los problemas que generan duda al manejar evidencia digital, se refieren a la forma cómo se recupera la información digital de dispositivos electrónicos, ya que se debe instrumentalizar un procedimiento o método adecuado para realizar esta tarea.

Hay que cumplir con la premisa de que estas prácticas deben ser aceptadas de forma universal, esto en relación a las capacidades que muestran los operadores de justicia, en el uso de la tecnología dentro de sus áreas de influencia.

Esto se debe al temor del uso de la tecnología que experimentan jueces, fiscales, defensores públicos e incluso la policía judicial, situación que hace que el uso de técnicas con el fin de extraer y preservar la evidencia digital sea considerado una práctica poco ortodoxa en el mundo analógico en el que todavía viven algunos operadores de justicia.

Se puede decir que en este campo aplica la frase “en casa de jabonero, el que no cae resbala” y más temprano que tarde, Ecuador verá emerger con más frecuencia la ocurrencia de actos ilícitos en los cuales se involucre tecnología tanto en su vida diaria como en su entorno.

Los delitos tecnológicos son cada día más frecuentes, la mayor parte del mundo los ha reconocido y discutido ampliamente, y Ecuador no puede permanecer aislado de esta corriente por la simple negativa al cambio.

Por esta razón el objetivo general de este Proyecto de Titulación, es proponer un sistema de análisis forense para teléfonos celulares con tecnología GSM, tecnología mayoritariamente utilizada en Ecuador.

El sistema se enfoca en colectar evidencia digital en la escena del hecho, y posteriormente analizarla, para contribuir en la investigación de un proceso judicial, aclarando que se estudia cómo debe tratarse el teléfono celular como

evidencia cuando éste es encontrado en una escena del crimen o en cualquier tipo de acción considerada delito luego de su perpetración.

En Ecuador no existen leyes claras en el tratamiento del teléfono celular como medio de prueba o evidencia, ya que las leyes existentes relacionadas a la tecnología, basan sus principios y sanciones en el cometimiento de infracciones exclusivamente informáticas. Es decir, cómo los equipos informáticos se usan para cometer fraudes, robo de información, intrusiones no autorizadas, distribución de pornografía, entre otros.

Precisamente este proyecto pretende ser una guía para el investigador de evidencia digital en teléfonos celulares, y está sujeta a cambios por cuanto la tecnología cambia día a día, por lo tanto debe haber cambios en la metodología a seguir, considerando este aspecto.

Ahora bien, el problema que se advierte por parte de las instituciones llamadas a realizar la investigación judicial, es la falta de preparación en ciencias forenses, esto debido a la falta de infraestructura y la formación necesaria, tanto de fiscales como policías e investigadores, dado que no existe en el país una unidad especializada.

Por parte de la Función Judicial falta preparación de Jueces en temas tecnológicos, ya que en algunas ocasiones, los llamados a impartir justicia se ven confundidos con la especial particularidad de este tipo de evidencias.

Es por tanto como manifiesta Phill Williams, Profesor de Estudios de Seguridad Nacional, Universidad de Pittsburgh, “Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los Estados para luchar contra la delincuencia, sino también, con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a la tecnología” [20].

Es necesario mencionar que son los operadores de justicia así como los profesionales en distintas áreas de ingeniería, los llamados a combatir los delitos tecnológicos, ya que los primeros saben cómo piensa el delincuente y su modo de

operación, mientras los otros conocen el funcionamiento de la tecnología. Unidos los dos conforman la llave para combatir efectivamente esta clase de infracciones.

El sistema inicialmente identifica y plantea las instancias o ciclos que normalmente lleva una investigación judicial y los actores posiblemente involucrados.

Para esto se identifican dos ciclos, el primer ciclo es el pre-procesal hace referencia a la indagación previa, lo constituye la colecta y análisis de la evidencia; el segundo ciclo es el procesal penal que lo conforma el juicio propiamente dicho. La Figura 4.1 muestra los ciclos y los posibles involucrados.

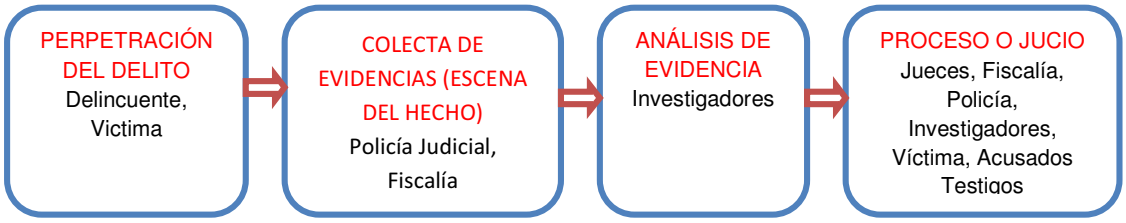


Figura 4.1: Secuencia y actores de las etapas generales en una investigación judicial

La finalidad del presente documento es brindar una mirada introductoria al Análisis Forense de Teléfonos Celulares, enfocándose en las etapas de colecta y análisis de evidencia digital. Con la finalidad de establecer bases en la investigación científica, se darán pautas a los futuros investigadores de cómo manejar una escena del delito, donde se vean involucrados teléfonos celulares y posteriormente realizar la recuperación de la llamada evidencia digital.

4.1 EVIDENCIA DIGITAL

Luego de analizar las definiciones antes citadas, se propone como evidencia digital “a la información de valor probatorio almacenada o transmitida en forma binaria en un medio electrónico”.

Las evidencias digitales, son hechos totalmente diferentes en su esencia con sus similares del mundo físico; pero son similares en sus posibles efectos y consecuencias a sus correlativas del mundo físico, es por ello que se presenta el Principio de Equidad Funcional, que se refiere a que todos los actos realizados

por medios electrónicos que cumplan con las disposiciones judiciales vigentes, poseen la misma validez y eficacia judicial que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales.

Para un adecuado manejo de este tipo de evidencia hay que recordar que forma parte de la llamada evidencia latente, como las huellas dactilares o el ADN, con características como:

- ✓ Son invisibles al ojo humano.
- ✓ Son sensibles al tiempo.
- ✓ Son de naturaleza frágil y puede ser fácilmente alteradas, dañadas o destruidas.
- ✓ Requiere de personal y herramientas especializadas para su colecta y análisis.
- ✓ Además una característica adicional para la evidencia digital, es que ésta puede trascender las fronteras con gran facilidad y rapidez.

Al mismo tiempo, para que la evidencia digital pueda ser usada en procesos judiciales se debe recordar cumplir con las siguientes características:

- ✓ Admisibilidad: Toda evidencia recolectada debe ajustarse a ciertas normas judiciales para presentarlas en una investigación.
- ✓ Autenticidad: La evidencia debe ser relevante al caso, dar una idea de lo sucedido en la escena del hecho, y permitir al investigador forense representar el origen y veracidad de la misma.
- ✓ Fiabilidad: Las técnicas usadas para obtener la evidencia deben gozar de credibilidad y de ser 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, qué proceso se siguió en la investigación y cómo la

integridad de la evidencia fue preservada, para que ésta sea comprensible y creíble en un proceso judicial.

4.1.1 EVIDENCIA DIGITAL EN LA LEGISLACIÓN ECUATORIANA

La legislación es el conjunto de leyes por las cuales se gobierna un Estado o una materia determinada. Estas leyes se encuentran jerárquicamente sometidas a la Constitución Política de la República, que es la norma principal que dicta los preceptos básicos bajo las cuales se rige un estado de derecho. Las demás leyes deben estar en perfecta armonía con la Constitución ya que de no estarlo serían nulas sus disposiciones.

Debe entenderse por leyes todas las normas rectoras del Estado y de las personas a quienes afectan, dictadas por la autoridad a quien esté atribuida esta facultad.

En términos generales la cadena legal y regulatoria en cualquier estado se basa en una jerarquía normalizada. Kelsen[57] propuso una estructura piramidal en cuyo vértice se encuentra la Constitución como norma fundamental.

De conformidad con la Constitución de 2008 de la República del Ecuador, el Art. 425 estipula "El orden jerárquico de aplicación de las normas será el siguiente: La Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos".

La pirámide de Kelsen aplicable al Ecuador se presenta en la Figura 4.2.

En la legislación ecuatoriana existe en vigencia leyes que pueden dar validez a la evidencia digital y cuyos artículos están relacionados con el sistema a proponer

[57] *Hanz Kelsen* nació en Praga, el 11 de octubre de 1881 y falleció en Berkeley, California, el 19 de abril de 1973, fue un jurista, político y filósofo del derecho austríaco de origen judío, el cual señalaba a la Constitución como la norma positiva de mayor jerarquía, la cual se encuentra en la cúspide de la pirámide jurídica y de la cual se deriva el fundamento de validez del resto de normas que se encuentran por debajo de ella.

en este Proyecto de Titulación, pues en este análisis el procedimiento propuesto no será aplicable sino se toma en cuenta el marco legal ecuatoriano.

Figura 4.2: Pirámide de Kelsen aplicable a Ecuador

Es por esta razón, que se revisa la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas[58], las reformas efectuadas al Código Penal por esta ley; el Código de Procedimiento Penal y Principios Técnicos reconocidos internacionalmente para un manejo adecuado de la Evidencia Digital.

4.1.2 VALIDACIÓN EN LA LEGISLACIÓN ECUATORIANA

Para dar validez a la evidencia digital la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas estipula en su Art.1, "Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas".

En base a esta ley se puede interpretar a la información digital como mensajes de datos, ya que los define como: "Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de

[58] Ley No. 67, publicada en el Registro Oficial Suplemento No. 577 de 17 de Abril del 2002.

datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos".

A la vez, esta información digital o mensajes de datos, constituyen evidencia digital cuando tal información tiene un valor probatorio, y por lo tanto son de interés para el proceso judicial.

De la igual manera esta ley tipifica los siguientes principios generales relativos a los mensajes de datos:

Art. 2, *Reconocimiento Jurídico de los Mensajes de Datos,* "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento".

Art. 4, *Propiedad Intelectual*, "Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual".

Por esta razón en la Ley de Propiedad intelectual Art. 26, se escribe, "También constituyen violación de los derechos establecidos en este libro cualquiera de los siguientes actos:

a) Remover o alterar, sin la autorización correspondiente, información electrónica sobre el régimen de derechos".

En este punto, cabe mencionar que para no incurrir en una violación a la ley, se debe contar con las autorizaciones judiciales respectivas.

Para utilizar mensajes de datos como evidencia en un proceso judicial, se debe considerar lo expuesto en el Art. 52 de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.

Art.52 *Medios de Prueba* "Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su

valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil".

Se puede observar en este artículo que la ley tiene un enfoque hacia el Comercio Electrónico, mas no hacia evidencias digitales; por lo tanto se recomienda que no solo se observe lo dispuesto en el Código de Procedimiento Civil, que trata de los deberes y derechos de los ciudadanos, sino también que se revise el Código de Procedimiento Penal, que es el encargado de tratar actos delictivos.

De esta manera se podría afirmar que la evidencia digital es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella; es cualquier mensaje de datos almacenado y transmitido por medios electrónicos que tengan relación con el cometimiento de una acto que comprometa a los presuntos responsables y que guie a los investigadores en el descubrimiento de posibles infractores.

4.1.3 VOLÁTIL Y DINÁMICA

Actualmente se puede pensar que en un teléfono celular existen evidencias digitales constantes y/o permanentes almacenadas en su memoria y que éstas se mantienen al momento de apagar el celular, pero no es así, tanto el celular como la tarjeta SIM tienen memorias volátiles.

Es decir que existe evidencia alojada temporalmente en las memorias del teléfono celular, que por su naturaleza inestable se pierden cuando el celular es apagado; este tipo de evidencias deben ser recuperadas casi de inmediato.

De lo dicho se desprende que cuando se encuentra un teléfono celular relacionado a un delito o contravención, la información directa o indirectamente que se relaciona con esta conducta, queda almacena en forma digital en el teléfono celular.

Puede convertirse en una dificultad, la obtención de esta clase de evidencia como prueba de la infracción cometida, debido a que el teléfono celular en donde se almacena la evidencia digital presenta características técnicas propias; por tal

razón la información ahí almacenada no puede ser colectada y analizada como medio de convicción sin utilizar métodos tecnológicos especiales..

La dinámica de la evidencia se refiere a la forma como se entienden y describen los diferentes factores (humanos de la naturaleza, de los equipos) que actúan sobre evidencias, a fin de determinar cambios que éstos producen sobre ellas.

Se puede afirmar indudablemente que existen muchos agentes que intervienen o actúan sobre la evidencia digital, cumpliendo con el Principio de Intercambio de Locard[59].

El investigador se ve en la necesidad de reconocer la forma como estos factores pueden alterar la evidencia, y asi tener la oportunidad de manejarla de manera apropiada, evitando generalmente contaminarla, dañarla y hasta perderla por completo.

Los principios criminalísticos[60], como el de Locard y el de mismidad[61] deben estar presentes en la mente del personal involucrado, en la investigación en cualquier escena del crimen.

4.1.4 ROLES Y FUNCIONES EN LA INVESTIGACIÓN

En el ámbito de una investigación judicial y de acuerdo a la Constitución de la Republica en su Art. 195 señala que: “La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre-procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal.

---

[59] *El Principio de Intercambio de Locard*, menciona que cuando dos objetos entran en contacto siempre existe una transferencia de material entre el uno y el otro. Es decir que cuando una persona está en una escena del crimen ésta deja algo de sí misma dentro de la escena, y a su vez cuando sale de ella ésta se lleva consigo.

[60] *Criminalística* es la disciplina que tiene por objeto el descubrimiento, explicación y prueba de los delitos, así como la detección de sus autores y víctimas

[61] *El principio de mismidad* permite establecer que determinado elemento material probatorio que se presenta en el juicio, es el mismo que se recolectó en la escena y que se encuentra en iguales condiciones a las de aquel momento.

Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá personal de investigación civil y policial; dirigirá el sistema de protección y asistencia a víctimas, testigos y participantes en el proceso penal; y, cumplirá con las demás atribuciones establecidas en la ley".

Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que afirma: "El ejercicio de la acción pública corresponde exclusivamente a la fiscal o el fiscal".

De lo dicho se puede concluir que el dueño de la acción penal y de la investigación tanto pre-procesal como procesal penal, de hechos considerados como delitos es el Fiscal, él es la voz dentro de la investigación. Como lo afirma el Art.195 de la Constitución "organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial". En tal virtud cualquier resultado de dichas investigaciones se incorporarán en su tiempo ya sea en la Instrucción Fiscal (investigación procesal) o a la Indagación Previa (investigación pre-procesal), utilizando como lo afirma el Art.195 "Ciencias Forenses".

La investigación científica de una escena del crimen es un proceso formal, donde el llamado investigador hace referencia a la participación de diferentes personas, que documentan y adquieren evidencias, usando su conocimiento, técnicas, herramientas y generando indicios suficientes para ayudar a resolver el caso.

Es por tanto necesario dejar en claro cuáles son los roles y la participación que tienen estas personas dentro de una escena del crimen o del hecho.

- ✓ **Personal de Primera Respuesta**, también llamados *First Responders,* son los primeros en llegar a la escena del hecho, son los encargados de colectar evidencias que ahí se encuentran.

  Tienen información básica en el manejo de evidencia y documentación, al igual que en la reconstrucción del delito y la localización de los elementos de convicción.

- ✓ **Examinadores de Evidencia Digital,** son los responsables de analizar y procesar toda evidencia digital obtenida por el Personal de Primera respuesta en las escenas del hecho. Para ello dichas personas requieren tener un alto grado de especialización en el área de interés dentro de la investigación.

- ✓ **Investigadores del Delito,** son los responsables de realizar la investigación y la reconstrucción de los hechos de manera general. Son personas con entrenamiento general en cuestiones tecnológicas de Análisis Forense; son Profesionales en Seguridad, Abogados, Policías y Examinadores forenses con conocimiento del marco regulatorio involucrado.

- ✓ **Peritos,** estos profesionales se hacen indispensables para la valoración de pruebas o elementos de convicción, por su conocimiento en materias especiales. Son personas que prestan su servicio especial al Fiscal y al Juez al momento de ilustrar sobre las materias, técnicas o artes que son de su conocimiento, con el fin de que dichos funcionarios, en función de las explicaciones puedan emitir su criterio en el momento adecuado (Dictamen Fiscal o Sentencia).

  La presencia de los peritos en una investigación judicial resulta a veces indispensable, pues el conocimiento del perito suple el del juez y el fiscal en cierta área de conocimiento de la cual éstos no son expertos; el perito entrega los elementos de convicción que permita al operador de justicia crear un razonamiento que desemboque en la resolución del caso propuesto, en fin elementos que tanto el Fiscal como el Juez valorarán al emitir su resolución.

  De acuerdo a lo que dispone el Art.94 del Código de Procedimiento Penal, “Son peritos los profesionales especializados en diferentes materias que hayan sido acreditados como tales, previo proceso de calificación”

Las condiciones que deben reunir las personas para ser peritos según el Dr Santiago Acurio son:

- Ser un profesional especializado y calificado por las Direcciones Regionales del Consejo de la Judicatura, considerando que el perito no solo es un profesional en determinada rama, sino que es una persona experta o especializada en un campo determinado.

- Mayores de edad, los peritos deben tener la mayoría de edad que en nuestro país se fija en 18 años, porque a esa edad la persona ha alcanzado la madurez psicológica necesaria para prestar esta clase de asesoramiento a la administración de justicia.

- Reconocida honradez, en cuanto a la calidad moral del perito, de proceder recto, íntegro y honrado en el obrar; el perito es un personaje esencialmente imparcial que cumple con su cometido y se desvincula del proceso.

- Conocimientos específicos en la materia sobre la que debe informar, es decir los conocimientos necesarios y específicos para cumplir su cometido.

La pericia es un medio de prueba específicamente mencionado por la Ley, “con el cual se intenta obtener para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba” [21].

Un informe pericial, sus conclusiones u observaciones no son definitivos ni concluyentes; la valoración jurídica del informe pericial queda a criterio del Fiscal, Juez o Tribunal Penal, quienes pueden aceptarlo o no con el debido sustento o motivación.

De lo expuesto, se desprende que un perito requiere la formación integral del tema específico del cual se hará cargo, y el conocimiento de disciplinas jurídicas, criminalísticas y forenses.

> En este sentido, el perfil que debe mostrar un perito del área de las TICs es el de un profesional hibrido que no le es indiferente su área de formación profesional y las ciencias jurídicas.

Es importante señalar que cada una de las personas tiene un rol definido dentro del proceso judicial, las cuales informarán al Fiscal y a la Policía Judicial, para que luego de la investigación, estén en la posibilidad de perseguir a los responsables del cometimiento de dicho incidente a través de la formulación de los cargos respectivos en una audiencia ante el Juez de Garantías, y posteriormente terminará ante el Tribunal Penal.

Esta serie de pasos y de instancias son parte del debido proceso, y por tanto tienen apego a las normas constitucionales y legales, creando una serie de pasos que se unen a otros creando una cadena irrompible.

En este punto siempre hay que recordar que todos los ciudadanos en nuestro país tienen derechos constitucionales y uno de ellos es el derecho a la intimidad y al secreto de las comunicaciones; los investigadores en todas los roles y etapas tienen que tomar en cuenta que los involucrados en un incidente gozan de las garantías antes mencionadas.

Por tanto todo acto de investigación que requerirá información relacionada a mensajes de datos, es necesario que cuente con la correspondiente orden judicial, caso contrario los investigadores tendrán responsabilidad sobre estas acciones, ya que serán responsables más allá de las órdenes emanadas por sus superiores, o por los consejos erróneos que ciertos consejeros legales proporcionan en estos casos.

En conclusión, el personal involucrado debe tener precaución al tratar con la intimidad y privacidad de los sospechosos; también hay que tener presente que todas las personas que intervienen podrán tener un grado de responsabilidad durante la realización de su trabajo, ya sean investigadores, Policía Judicial y hasta la Fiscalía. Por lo tanto es necesario definir el rol específico de cada uno de los participantes, a fin de que no existan malos entendidos y falta de comunicación.

4.1.5 MEDIO DE PRUEBA

La presunción de inocencia exige que a una persona acusada se le considere inocente hasta que el Fiscal, que tiene la carga de probar la culpabilidad del imputado, pruebe que esa persona cometió el delito “más allá de toda duda razonable”. Por consiguiente, el resultado de una causa penal dependerá de la calidad y peso de la evidencia, elementos considerados medios de prueba o elementos de convicción.

La prueba dentro del proceso es de vital importancia, ya que a partir de ella se confirma o desvirtúa una hipótesis o afirmación precedente y se llega a la posesión de la verdad material. De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables.

Los problemas al manejar investigaciones relacionadas con equipos electrónicos, es la forma cómo se recupera la información digital contenida en éstos, en otras palabras, el problema radica en cómo sistematizar un procedimiento o un método adecuado para realizar esta tarea, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal.

Estos elementos pueden ser considerados como medios de prueba de situaciones con implicancias jurídicas por ejemplo un mensaje de texto entre la víctima y un sospechoso de asesinato, en fin, nuevos elementos a ser incorporados a los procedimientos judiciales.

Es importante clarificar los conceptos y describir la terminología adecuada que señale el rol que tiene un equipo electrónico dentro del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener el caso.

Es así que, por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un secuestro; por lo tanto el rol que cumpla el teléfono celular determinará dónde debe ser ubicada y cómo debe ser usada la evidencia digital.

Para este propósito se han creado definiciones a fin de hacer una necesaria distinción entre el elemento material o *hardware* (evidencia electrónica), y la información contenida en éste (evidencia digital); esto es indispensable ya que el foco de la investigación será la evidencia digital aunque en algunos casos también será la evidencia electrónica como por ejemplo en la búsqueda de huellas dactilares.

Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia, y crear un paralelo entre una escena física del crimen y una digital.

En este contexto los elementos físicos hacen referencia al *hardware* (Equipo Móvil o Terminal Celular y Tarjeta SIM), mientras que los elementos digitales, se refieren a todos los datos almacenados y transmitidos usando el *hardware*.

El propósito de estas definiciones, es el de enfatizar el papel que juegan en la ayuda de una investigación judicial a fin de que el investigador tenga una trayectoria clara y precisa al buscar los elementos de convicción que aseguren el éxito del proceso judicial.

En estas condiciones para efectos probatorios son objeto de análisis, tanto el *hardware* como la información contenida en éste, para lo cual es necesario contar con el auxilio y conocimiento de las ciencias forenses.

Dada la ubicuidad de la evidencia electrónica y digital es raro el delito que no esté asociado a un mensaje de datos guardado o transmitido. Un investigador calificado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionadas con otras víctimas.

Se debe anotar que no solo los teléfonos celulares constituyen evidencia electrónica, en una escena del hecho se puede encontrar computadores portátiles y de escritorio, *hardware* de red, GPS, cámaras fotográficas y de video, memorias flash, copiadoras, impresoras, entre otras.

El investigador debe tener una idea clara de dónde buscar evidencia digital, éstos deben identificar otras fuentes de evidencia, situación que brindará al investigador el método más adecuado para su posterior identificación y preservación.

La evidencia es la materia que se usa para persuadir al tribunal o al juez de la verdad o falsedad de un hecho que está siendo controvertido en un juicio. Son entonces las normas procesales y las reglas del debido proceso las que informan al juez o al tribunal qué evidencias son relevantes y admisibles dentro de un proceso judicial y cuáles no lo son.

Es importante considerar estas normas y reglas desde el principio de la investigación, es decir, desde el descubrimiento de las mismas, a fin de evitar la exclusión de estas evidencias o elementos de convicción por atentar contra los principios constitucionales.

El investigador debe conocer y apegarse estrictamente a lo que dice la Constitución, las diferentes Leyes del Estado Ecuatoriano y principios técnicos propuestos por especialistas en la temática.

El incumplimiento o la transgresión de las leyes en las actividades de investigación así como las pruebas adquiridas de una manera no licita, tendrán un carácter de Ineficacia probatoria, como lo menciona el artículo 80 del Código de Procedimiento Penal, que textualmente dice:

Art. 80, *Ineficacia probatoria*, “Toda acción pre-procesal o procesal que vulnere Garantías constitucionales carecerá de eficiencia probatoria alguna. La ineficiencia se extenderá a todas aquellas pruebas que de acuerdo a las circunstancias del caso, no hubiesen podido ser obtenidas sin la violación de tales Garantías”.

Es por eso necesario proponer un sistema de análisis forense que no incumpla el marco regulatorio, el cual en este proyecto de titulación consta de dos ciclos: Colecta y Análisis, los cuales se dividen en varias etapas y a su vez éstas se dividen en varias fases a cumplirse.

Para colectar la evidencia en la escena del hecho, se realizará:

- ✓ Identificación
- ✓ Preservación

Para el posterior análisis de la evidencia digital en un teléfono celular, se efectuarán las siguientes fases:

- ✓ Evaluación
- ✓ Extracción
- ✓ Interpretación
- ✓ Presentación

Estos ciclos de Colecta y Análisis serán analizados en detalle, posteriormente, en el Sistema de Operaciones.

En estos casos el orden es fundamental, ya que el desorden es enemigo de la claridad, por tanto el seguir los pasos en el orden correcto garantizará que la evidencia digital obtenida no sea, dañada o alterada en el proceso investigativo; además también se garantizará la cadena de custodia[62] de los elementos físicos, a fin de que no haya duda de la procedencia de estos dispositivos en la escena del delito, y que éstos se mantengan íntegros.

Para la admisibilidad de la evidencia digital de un teléfono celular se debe tomar en cuenta dos situaciones:

1. El Estado a través del órgano judicial, la Fiscalía General del Estado, debe establecer que el equipo electrónico (teléfono celular) en donde se almacena la evidencia digital (mensajes de datos), es el equipo encontrado en la escena del hecho y relacionado con el imputado o sospechoso, más allá de toda duda razonable. Esto referido especialmente a la cadena de

[62] *Cadena de Custodia es* un procedimiento de seguridad, para garantizar que el examinador o perito reciba del investigador y/o fiscal, los elementos de prueba en el mismo estado en que fueron colectados en el lugar del hecho, igualmente que sean devueltos al investigador en la misma situación, que al ser presentados ante el tribunal se pueda comprobar su autenticidad y no existan dudas sobre los elementos de prueba.

custodia sobre los elementos físicos, “Elemento de Pertenencia de la Evidencia Digital”.

2. El Estado a través del órgano judicial, la Fiscalía General del Estado, debe establecer que el mensaje de datos (evidencia digital) que fue descubierto dentro del equipo electrónico (teléfono celular), fue guardado o almacenado originalmente en ese dispositivo, más allá de cualquier duda razonable de que alguna persona lo plantó ahí o fue creada por la herramienta utilizada por el examinador en el curso de su trabajo, “Elemento de Integridad de la Evidencia Digital.”

En base a estos dos enunciados se empieza a construir la admisibilidad de la evidencia dentro de un proceso judicial.

En el elemento de Integridad se debe cumplir con la utilización de funciones *Hash* cumpliendo con lo dispuesto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que establece en su Art. 7 *Información original* “Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación”.

Por esta razón los códigos de integridad tienen la misma funcionalidad que una firma electrónica y se presentan como valores numéricos de tamaño fijo, que se convierten en una verdadera huella digital del mensaje de datos, cumpliendo con el Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos:

Art. 6 *Integridad de un mensaje de datos*, “La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado

o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación".

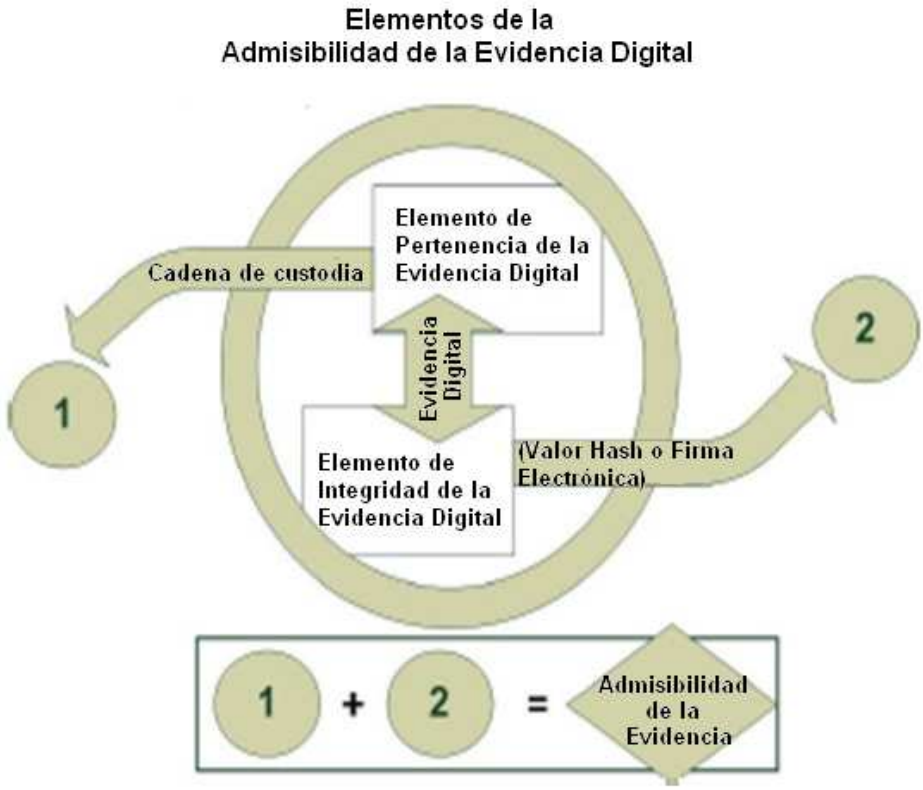


Figura 4.3: Admisibilidad de la evidencia [21]

Los valores recogidos a través de las funciones *Hash* son iguales a tomar una fotografía de un homicidio, es decir que le servirán al investigador al momento de rendir un testimonio, ya que el Fiscal podrá ofrecer este registro como evidencia dentro del juicio.

Por tanto para autenticar la evidencia obtenida en la escena del hecho, se debe comparar los valores *Hash* obtenidos de los mensajes de datos encontrados en el dispositivo, con los obtenidos dentro de la etapa procesal o juicio; por tanto si los valores *Hash* son idénticos, serán admisibles como prueba esos mensajes de datos, esto por cuanto estos códigos de integridad a través del uso de algoritmos de cifrado como el MD5 o el SHA-1 generan un valor único, el cual es difícil de alterar o modificar.

La admisibilidad de la evidencia digital está dada por la suma del elemento de Pertenencia y el elemento de Integridad. El primero de ellos es la vinculación del teléfono celular con la escena del hecho donde fue descubierto y relacionado con el sospechoso, vinculación física, y el segundo generado por la llamada función *Hash*, que es una vinculación de tipo digital al aplicar la firma electrónica y un sellado de tiempo al mensaje de datos que sirva como evidencia.

De otro lado es importante indicar que además de los elementos de Pertenencia e Integridad, hay que verificar que se cumplan los siguientes factores:

- ✓ Cumplimiento de los principios básicos, reconocidos internacionalmente en el manejo de evidencias digitales.
- ✓ Cumplir los principios constitucionales y legales.
- ✓ El establecimiento de un Sistema de Operaciones Estándar[63] que va a ser propuesto en este proyecto de titulación.
- ✓ Entender el trámite legal determinado principalmente en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Código de Procesamiento Penal.

En el sistema acusatorio la evidencia admisible, es la evidencia relevante. Es evidencia relevante aquella que tiene valor probatorio, esto es, si posee alguna tendencia a hacer más o menos probable algún hecho de importancia para la resolución sobre el caso [21].

[63] Conjunto de etapas o pasos que deben realizarse de forma ordenada al momento de colectar y analizar la evidencia digital, esto se realiza para garantizar la transparencia e integridad de la misma.

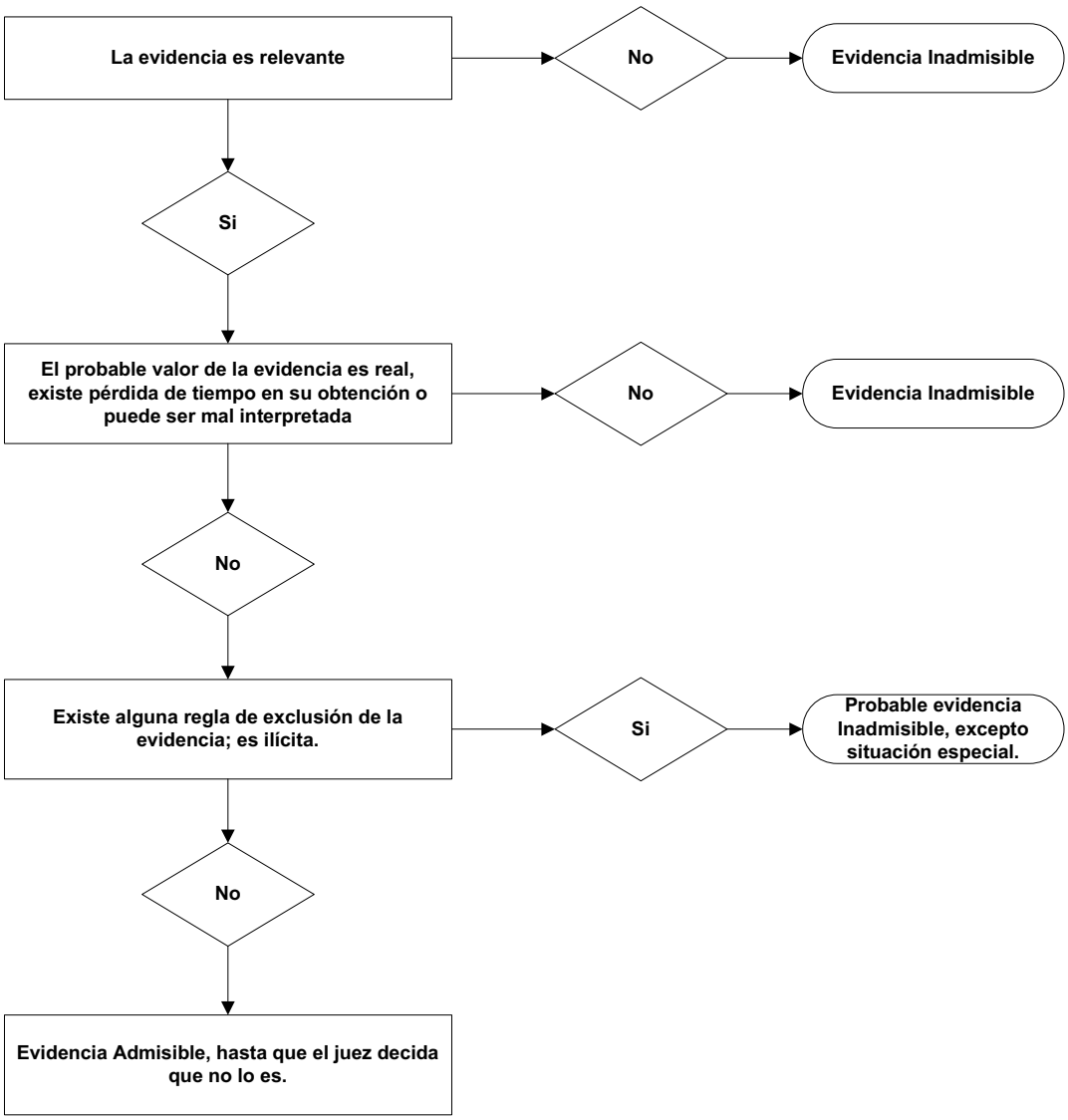


Figura 4.4: Diagrama de Flujo de Admisibilidad de la Evidencia [21]

A fin de evitar que la evidencia sea excluida o inadmisible en un proceso judicial, el investigador debe adoptar los procedimientos necesarios para que todos los mensajes de datos sean aceptados.

4.2 SISTEMA DE OPERACIONES

Cuando se va participar en una investigación judicial, es necesario tener en cuenta un sistema de operaciones, el mismo que es un conjunto de fases que

deben realizarse de forma ordenada al momento de Colectar y Analizar en este caso específico la evidencia digital en teléfonos celulares con tecnología GSM.

Esta serie de fases se utilizan para asegurar que toda la evidencia encontrada se la colecte y analice de una manera transparente e íntegra. La transparencia y la integridad metodológica (estabilidad en el tiempo de los métodos utilizados) se requieren para evitar errores, a fin de certificar, que se utilizan los mejores métodos, incrementando cada vez la posibilidad que dos examinadores forenses lleguen al mismo dictamen o conclusión cuando ellos analicen la misma evidencia por separado.

Antes del procedimiento técnico se debe tener claro los requisitos legales, expuestos en el Código de Procedimiento Penal.

- ✓ **Incautación:** En el Art. 93, *Incautación*, "Si el Fiscal supiere o presumiere que en algún lugar hay armas, efectos, papeles u otros objetos relacionados con la infracción o sus posibles autores, solicitará al juez competente autorización para incautarlos, así como la orden de allanamiento, si fuere del caso".

  El teléfono celular correspondería a "otros objetos relacionados con la infracción", por lo que si el investigador presume que existe algún tipo de evidencia digital en él, deberá pedir la correspondiente autorización judicial para incautar dichos elementos; de igual forma debe tener la autorización judicial para acceder al contenido almacenado y generado por dichos dispositivos.

  Antes de realizar la incautación de dispositivos electrónicos se debe tomar en cuenta lo siguiente:

  - ➢ No afectar los derechos fundamentales de las personas, como por ejemplo se podría lesionar la intimidad y la privacidad a través de los mensajes datos, basándose en la constitución ecuatoriana, en su Art. 66 "Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar".

Razón por la cual se debe contar con las respectivas autorizaciones judiciales.

- ✓ **Petición de Información:** En el Código de Procedimiento Penal Art.149, *Informes*, se afirma: "Los fiscales, jueces y tribunales pueden requerir informes sobre datos que consten en registros, archivos, incluyendo los informáticos. El incumplimiento de estos requerimientos, la falsedad del informe o el ocultamiento de datos, serán sancionados con una multa equivalente al cincuenta por ciento de un salario mínimo vital general, sin perjuicio de la responsabilidad penal, si el hecho constituye un delito. Los informes se solicitarán por escrito, indicando el proceso en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y la prevención de las sanciones previstas en el inciso anterior".

  Este artículo debe estar presente tanto para el Personal de Primera Respuesta como para los Examinadores e Investigadores involucrados en la investigación judicial.

- ✓ **Apertura de Correspondencia:** En el Código de Procedimiento Penal Art. 150, establece *Inviolabilidad*, "La correspondencia epistolar, telegráfica, telefónica, cablegráfica, por télex o por cualquier otro medio de comunicación, es inviolable. Sin embargo el juez podrá autorizar al Fiscal, a pedido de éste, para que por sí mismo o por medio de la Policía Judicial la pueda retener, abrir, interceptar y examinar, cuando haya suficiente evidencia para presumir que tal correspondencia tiene alguna relación con

el delito que se investiga o con la participación del sospechoso o del imputado".

Este artículo establece aunque no de manera clara a los mensajes de datos entendiendo éstos como correspondencia, por lo que permitiría a los Examinadores la extracción de la evidencia Digital en teléfonos celulares, cumpliendo con lo expuesto por este artículo.

- ✓ **Reconocimiento de la Evidencia:** En el Código de Procedimiento Penal Art. 156, afirma *Documentos Semejantes*, "El juez autorizará al Fiscal para el reconocimiento de las grabaciones, así como de películas, registros informáticos, fotografías, discos u otros documentos semejantes. Para este efecto, la intervención de dos peritos que jurarán guardar reserva, el Fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento. El Fiscal podrá ordenar la identificación de voces grabadas por personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos o con intervención pericial. Si los predichos documentos tuvieren alguna relación con el objeto y sujetos del proceso, el Fiscal ordenará redactar la diligencia haciendo constar en ella la parte pertinente al proceso. Si no la tuvieren, se limitará a dejar constancia, en el acta, de la celebración de la audiencia y ordenará la devolución de los documentos al interesado".

  En relación a este artículo se puede concluir que la evidencia digital en teléfonos celulares se la puede interpretar como registro informático o documentos semejantes; para lo cual existirá la intervención de peritos.

- ✓ **Utilización de los Medios Electrónicos** *Art. ..., (Agregado por el Art. 31 de la Ley s/n, R.O. 555-S, 24-III-2009),* "Los Fiscales podrán utilizar todos aquellos medios técnicos, electrónicos, informáticos y telemáticos que resulten útiles e indispensables para sustentar sus actuaciones y pronunciamientos, cumpliendo con los requisitos y obteniendo las autorizaciones que se exijan en la ley, respecto de la procedencia y eficacia

de los actos de investigación o de prueba que se formulen a través de dichos medios.

Las actuaciones que se realicen, y los documentos o información obtenidas a través de estos procedimientos, serán válidos y eficaces siempre que se garantice su integridad, autenticidad y reproducción, y no afecten en modo alguno los derechos y garantías fundamentales reconocidas en la Constitución y la ley"

Hay que notar que los artículos no son claros, por lo cual su interpretación es de gran importancia, al mismo tiempo se recomienda introducir a los Mensajes de Datos en el Código de Procedimiento Penal, en artículos que permitan la validez de la Colecta y posterior Análisis de Evidencia Digital.

4.2.1 BUENAS PRÁCTICAS DE INVESTIGACIÓN

Hay dos tipos de investigaciones forenses que en general se pueden estudiar. El primer tipo es donde ha ocurrido el incidente o escena del hecho, pero la identidad del delincuente no es conocida; el segundo tipo es cuando el delincuente y el incidente se conocen. Preparada la escena del incidente, el examinador forense puede proceder a:

- ✓ Recopilar información sobre la(s) persona(s) que está(n) involucrada(s) en el delito {Quién}.
- ✓ Determinar la naturaleza exacta de los hechos ocurridos {Qué}.
- ✓ Construir una línea de tiempo de los acontecimientos {Cuándo}.
- ✓ Descubrir la información que explique la motivación para cometer el delito {Por qué}.
- ✓ Descubrir las herramientas que utilizó {Cómo}.

La tabla 4.1 proporciona una referencia cruzada de las fuentes de pruebas que comúnmente se encuentran en los teléfonos celulares y su posible contribución para satisfacer los objetivos mencionados.

En muchos casos, los datos son periféricos a una investigación, y son útiles para fundamentar o refutar las afirmaciones de un individuo acerca de algún incidente.

Los archivos del usuario ubicados en el dispositivo para envío, y edición son también otra fuente de evidencia importante, archivos gráficos, contenido de grabaciones de audio y vídeo, hojas de cálculo, diapositivas y otros documentos electrónicos similares.

	Quién	**Qué**	**Dónde**	**Cuándo**	**Porqué**	**Cómo**
Identificadores Subscriptor/Terminal	X					
Registro de Llamadas	X			X		
Directorio Telefónico	X					
Calendario	X	X	X	X	X	X
Mensajes	X	X	X	X	X	X
Localización			X	X		
Web URL /Contenido	X	X	X	X	X	X
Imágenes/Video	X	X	X	X		X
Otro Contenido	X	X	X	X	X	X

Tabla 4.1: Referencia Cruzada de Fuentes de Información y Objetivos

Muchos datos son una amenaza para la validez del análisis forense en teléfonos celulares; debido a que hay dificultades en la adquisición de ciertos tipos de datos que se derivan de la naturaleza propia de los teléfonos celulares.

Además, características tales como *Bluetooth* y la capacidad de ejecutar aplicaciones propietarias pueden crear problemas adicionales. Como resultado, las herramientas para análisis forense en celulares constantemente están luchando para adquirir de forma fiable los datos de una amplia gama de teléfonos. Como la cantidad de pruebas y los diferentes tipos de teléfonos celulares aumentan al mismo tiempo, las herramientas también deben avanzar en funcionalidad para adaptarse a estos cambios.

El tema de que los teléfonos celulares estén presentes en la escena del crimen o escena del hecho se ha incrementado, principalmente por la facilidad con la que se puede adquirir un teléfono celular, por lo que se hace necesario identificar la información que puede ser utilizada como evidencia digital, y estudiar los elementos de las estaciones móviles o teléfonos celulares involucrados que fundamentalmente son el equipo móvil y la tarjeta SIM con sus características de *hardware* y *software*.

Aprender las habilidades necesarias para convertirse en un buen investigador lleva tiempo y, en algunos casos, educación avanzada, especializaciones, certificaciones técnicas, entre otros.

El funcionario investigador deberá cultivar determinadas cualidades personales tales como: sentido de pertenencia, cohesión, responsabilidad individual, compañerismo, confianza en sí mismo y en los demás, equilibrio, honestidad, liderazgo, inteligencia emocional, autocrítica, humildad, entre los más importantes

Estas cualidades son importantes y no pueden permanecer solo en cada persona, sino que deben trascender al grupo con el cual trabaja, de tal manera que un grupo identificado por estas cualidades, por la responsabilidad solidaria y el esfuerzo conjunto orientado a un fin común, se convierta en un verdadero equipo de trabajo.

Toda investigación penal requiere de un investigador, un tema de investigación y un propósito, orientados a identificar a las partes involucradas, establecer el mecanismo infractor o delictivo y obtener los suficientes elementos de convicción para que se conviertan en medios probatorios útiles.

La investigación penal se distingue porque ninguna se repite, en cada oportunidad que se debe llevar a efecto una investigación se debe considerar que es única, tienen sus propias características, complicaciones, bondades, efectos, es propietaria de un espíritu singular.

Para que una investigación judicial sea efectiva y sus resultados fidedignos, debe estar caracterizada por 4 atributos, debe ser: objetiva, completa, relevante, y exacta.

Los investigadores deben adherirse a las leyes que supervisan la investigación como la búsqueda, apoyo en la incautación y detención de un sospechoso; estas leyes varían de estado a estado y de país a país.

Los pasos generales para la investigación penal, se deberán basar en la observación, la descripción y la explicación del presunto hecho punible.

4.2.2 PRINCIPIOS APLICABLES A LA EVIDENCIA DIGITAL

Según la Asociación de Jefes y Oficiales Policiales de Reino Unido (*ACPO, Association of Chief Police Officers*[64]), en su Guía de buenas prácticas de manejo de evidencia digital [22] plantean cuatro principios.

Principio 1:

Ninguna acción tomada por las agencias gubernamentales de la función judicial y sus agentes debe cambiar los datos almacenados en dispositivos electrónicos, los cuales subsecuentemente pueden ser de importancia en la investigación judicial.

Principio 2:

En circunstancias donde un investigador necesariamente tiene que acceder a los datos originales almacenados en un computador o un medio de almacenamiento, el investigador debe ser competente para hacerlo y estar en la capacidad de dar una declaración explicando la importancia y las implicaciones de sus acciones.

Principio 3:

Un mecanismo de auditoría u otro registro de todo el proceso aplicado a la evidencia deber ser creado y preservado. Un tercero independiente debe poder examinar estos procesos y alcanzar el mismo resultado.

Principio 4:

[64] *ACPO (Association of Chief Police Officers),* es un cuerpo estratégico independiente y profesionalmente constituido. Centrados en el interés público y en la igualdad de la sociedad activa con el Gobierno y la Asociación de Autoridades Policiales, ACPO lidera y coordina la dirección y desarrollo del servicio policial en Inglaterra, Wales e Irlanda del Norte.

La persona a cargo de la investigación (el oficial del caso) tiene la total responsabilidad de asegurarse que la ley y estos principios estén relacionados.

Según la Organización Internacional de Evidencia Computarizada (IOCE, *International Organization on Computer Evidence*[65]) cuando se necesita recuperar evidencia digital, en su publicación "La guía para la mejor práctica en la examinación forense de tecnología Digital" considera los siguientes principios:

- Las reglas generales de evidencia deben ser aplicados para toda la evidencia digital.
- Al capturar la evidencia digital, las acciones tomadas no deben cambiar la evidencia.
- Cuando es necesario que una persona acceda a la evidencia digital original esta persona debe ser preparada adecuadamente para este propósito.
- Todas las actividades relacionadas con la incautación, acceso, almacenamiento o transferencia de evidencia digital deben ser documentadas, preservadas y estar disponibles para su revisión.
- El agente encargado será responsable de que todas las acciones tomadas con respecto a la evidencia digital, mientras esta evidencia está en su posesión.

Como se aprecia tanto los principios propuestos por los Jefes y Oficiales Policiales de Reino Unido y la Organización Internacional de Evidencia Computarizada tienen una estrecha relación, por tal razón en posteriores instancias cuando se cite Principios Aplicables a la Evidencia Digital se hará referencia a los principios propuestos por Jefes y Oficiales Policiales de Reino Unido.

[65] *IOCE (International Organization on Computer Evidence)* El propósito de esta organización será proporcionar un foro internacional para las agencias de aplicación de la ley de intercambio de información sobre investigación de equipos digitales y forenses.

Se debe notar que estos principios no se pueden aplicar en su totalidad a los teléfonos celulares, porque sus datos se encuentran cambiando continua y automáticamente sin interferencia de ninguna persona.

La adquisición de datos de los teléfonos celulares debe afectar lo menos posible al contenido, y en lo posible respetar los principios. El examinador debe ser competente para entender tanto el *hardware* como el *software* de teléfonos celulares específicos que estén involucrados en los casos delictivos.

Se deben reconocer las herramientas a ser utilizadas para adquirir evidencia digital del teléfono celular, ya que más de una herramienta es recomendada mientras que otras pueden ser erróneas para ser usadas en una tarea particular.

Los principios anteriormente citados, no pueden ser aplicados en toda la evidencia digital, y no necesariamente la evidencia recolectada puede ser considerada como evidencia relevante para un caso judicial, según las leyes y reglamentos de cada país se debe adoptar un procedimiento adecuado para su extracción y validación.

Estos principios generan recomendaciones, que el personal involucrado en la Colecta los llamados "*First Responders*", y el personal a cargo del Análisis los llamados Examinadores de Evidencia Digital deben tener conocimiento, tales recomendaciones estarán expuestas en las Etapas de Colecta y Análisis.

4.2.3 COLECTA DE EVIDENCIA DIGITAL EN LA ESCENA DEL HECHO

La etapa de colecta de evidencias tiene por objeto recabar todos los elementos de juicio necesarios para poder establecer alguna relación inequívoca dentro del proceso de investigación judicial e impedir la contaminación de la escena del hecho, para lo cual se siguen las etapas y fases mostradas en la Figura 4.5.

Se debe considerar que la contaminación puede ocurrir mediante inserción de evidencia digital o si el teléfono celular se encuentra encendido después del hecho, ya que al no ser aislado de señales de radiofrecuencia provenientes de la red celular, si alguna información es receptada puede alterar la evidencia digital del teléfono celular.

Figura 4.5: Etapas y Fases dentro del Ciclo de Colecta de Evidencia

Antes de comenzar con la etapa de colecta se deben tener los elementos necesarios, tanto legales antes nombrados, como los elementos técnicos expuestos a continuación. Considerar que no siempre se trabaja en ambientes pulcros e higiénicos.

Se recomienda no utilizar como material de empaque documentos o material de la misma escena, procure llegar con su propio material; se recomienda tener lo siguiente.

- ✓ Bolsas de Faraday
- ✓ Bolsas antiestáticas
- ✓ Sobres antihumedad
- ✓ Cajas de cartón
- ✓ Considerar que el entorno puede no contar con ninguna facilidad, de ser posible llevar diferentes fuentes de energía.
- ✓ Utilizar guantes de látex o pulseras antiestáticas para evitar daños debido a la estática
- ✓ Utilizar sobres de embalaje diferente para cada evidencia
- ✓ Utilizar algún medio para identificar los sobres

Si bien las guías internacionales recomiendan contar con dispositivos confiables y a su vez costosos, se podría dotar de elementos basados en el principio físico de la evidencia digital, que no tengan mucha dependencia con la marca o calidad.

Los indicios y/o evidencias que se colecten de la escena del hecho, se deben transportar hasta los ambientes predefinidos, que puede ser la oficina de auditoría interna, laboratorios de Investigación Forense, ambientes de la Fiscalía u otros.

En este punto se debe considerar que al no existir las garantías de traslado, la evidencia digital quedara inválida en el proceso judicial. Tomar en cuenta el riesgo de traslado, sobre todo con evidencias con componentes radioeléctricos que puedan sincronizarse como en el caso de teléfonos celulares. Hay que ser escéptico y si alguna vez se ha oído sobre la ley de Murphy “Si algo puede salir mal, saldrá mal”, tomarla en cuenta.

4.2.3.1 Identificación

El objeto de esta fase es realizar la identificación física de la escena del crimen y documentar todos los elementos encontrados, y decidir cuáles se utilizarán para llevar a cabo la investigación, trabajo realizado en su mayoría por el Personal de Primera Respuesta.

La escena del delito es el punto de partida de una investigación forense, aquí se aplican los principios criminalísticos como el de Locard y el de mismidad, explicados anteriormente; aquí se da inicio al procedimiento pertinente de acuerdo a la infracción cometida.

Se debe considerar la valoración de "bien mayor' o "mal menor" en el sentido de identificar qué acción es más oportuna; además se debe considerar que se pueden encontrar otros dispositivos electrónicos relacionados a teléfonos celulares tales como, computadores personales o de escritorio, agendas electrónicas, una o varias memorias flash, CDs o DVDs.

Esta etapa inicia con el aviso al Fiscal de que se ha llevado a cabo un delito, por cualquiera de los medios posibles, ya sea de oficio, por un informe de policía ante

una situación de flagrancia, por una denuncia penal o por una comunicación de otra autoridad o entidad del estado u órgano de control.

El Fiscal procede a analizar tal información, para determinar la existencia de un hecho penalmente relevante que amerite investigación, y así realizar o no la investigación.

Tener siempre presente que en realidad las investigaciones no son tan simples como lo muestran los libros o las películas. El Personal de Primera Respuesta debe tener a mano una metodología que les permita manejar escenas de variada complejidad.

Las siguientes fases se piden cumplir en esta etapa:

1. **Roles y funciones:** El Fiscal y el Investigador, al abordar la investigación de un caso conformarán el equipo de trabajo y procederán al análisis, depuración y valoración de la información con la cual cuentan hasta ese momento, independiente del medio por el cual haya llegado hasta ellos la noticia de la ocurrencia del delito.

   El trabajo en equipo, permitirá que se ahorre tiempo en la medida en que se desecha lo que no sea útil a la investigación; se produce un mayor rendimiento ya que cada cual desarrolla su rol, respetando el rol del otro, despareciendo la duplicidad de funciones o de tareas. Esto debe ser registrado para lo cual se debe llenar el correspondiente formulario. (Ver Anexo A) y tener presente lo siguiente:

   a. La persona a cargo de la investigación debe asegurarse que el personal encargado de la colecta esté apropiadamente entrenado y preparado para trabajar con dispositivos móviles y que estén equipados con los materiales de embalaje adecuado.

   El personal debe estar consciente que los dispositivos móviles, se pueden sincronizar con la red o que cualquier interacción manual con el dispositivo puede modificar o borrar evidencia.

b. Se establecerán las premisas que servirán de base para la ejecución de las labores de investigación o trabajo de campo; se realizarán las siguientes actividades:

- Obtener un conocimiento general del tema a ser investigado.
- Conocer, tanto como sea necesario, la información inicial para comprender el tema en investigación.
- Establecer, motivadamente, si amerita o no la investigación, es decir, si existen suficientes indicios como para considerar procedente todo el proceso investigativo.
- Elaborar las hipótesis preliminares para la investigación, estableciendo los posibles indicios.
- Definir las estrategias de la investigación que se aplicarán en la siguiente fase de "ejecución del trabajo" que corresponde a la investigación propiamente a ser ejecutada.

2. **Detección de Evidencia:** en esta etapa se debe, identificar el lugar dónde se presentó el incidente y diligenciar el formulario de actuación del Personal de Primera Respuesta (Ver Anexo B).

   Para la identificación del lugar, se requiere realizar una Narración o Fijación de la escena del hecho; se debe procurar que el medio a utilizar sea en un formato estándar (por ejemplo MP3).

   Si en una escena física se procede con el acordonamiento del lugar, en casos de escenas que comprendan teléfonos celulares, se debe tener en cuenta que éstos están conectados a la red celular, por ello se deberá aislar de manera eficiente.

   Tener presentes las siguientes recomendaciones:

   a. Recordar que antes de arribar a la escena del delito es necesario que el Personal de Primera Respuesta posea la orden judicial previamente

obtenida para el efecto. (Orden de Incautación, Orden de Interceptación, Orden de Apertura y Examen Pericial)

b. Se recomienda al Personal de Primera Respuesta nunca acudir solos al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos personas. Una segunda persona, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos.

c. Cuando en una escena del hecho se tiene que trabajar en condiciones adversas, como en incendios, inundaciones, derrames de gasolina o químicos peligrosos, es indispensable que el Personal de Primera Respuesta en la escena del hecho tome las medidas de seguridad necesarias para asegurar en primer lugar su integridad física, posteriormente implementar algún procedimiento que posiblemente recupere las evidencias de la manera más completa.

d. En muchos de los casos, el investigador forense no es el primero en llegar a la escena del delito, a veces llega después de un tiempo de cometido éste, como un experto secundario, pero aún así debe estar consciente de su entorno de trabajo, igual como si hubiera sido el primero en llegar.

e. Tener presente que otros agentes diferentes al Personal de Primera Respuesta, en algunas ocasiones por accidente cambia, reubica, o altera la evidencia o el sospechoso o imputado trata de cubrir sus rastros, deliberadamente borrando o alterando los mensajes de datos.

f. Asegurar físicamente la escena, este paso es crucial durante una investigación. Se debe retirar de la escena del hecho a todas las personas extrañas a la misma; el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.

g. La escena del hecho en la que hay dispositivos electrónicos es idéntica a una escena del hecho cualquiera, respecto a los cuidados requeridos;

no se debe utilizar el dispositivo, prender o apagar los dispositivos, sin ningún criterio justificable ya que se estaría contaminando las evidencias, introduciendo elementos foráneos al hecho, cambiando fechas, modificando archivos, borrando huellas.

h. Hacer un uso adecuado de fotografías y/o videos para registrar el estado de la colecta en la escena del hecho.

Debe considerarse la posibilidad de fotografiar la escena en la cual el dispositivo fue encontrado. El estado de la colecta debe ser registrada. Toda la información en pantalla debe ser anotada y/o fotografiada.

- Fotografía o videograbación de la disposición de los dispositivos y medios; por ejemplo la grabación podría decir jueves 25, horas 09:45, escritorio de Juan Pérez, se encuentra un teléfono celular marca Nokia conectado a una máquina portátil marca Compac, que se encontraba apagada, etc.

- Utilizar algún método de señas numeradas que permita reconstruir con exactitud la ubicación física de cada evidencia colectada en la escena del hecho.

i. La identificación debe tomar en consideración cualquier requerimiento para preservar otro tipo de evidencia (ADN, huellas digitales, narcóticos, armas de fuego).

La secuencia de análisis es crítica, puesto que técnicas de recuperación de huellas digitales pueden dar como resultado que el teléfono celular quede inservible. Igualmente el análisis de teléfonos celulares, sin tomar las apropiadas precauciones, puede destruir evidencia, como huellas digitales o ADN.

j. Estado del Dispositivo *(On - Off*)

Si el dispositivo móvil ha sido encontrado en una escena del hecho, tener en cuenta si está encendido o apagado. Es importante dejar el

teléfono celular en el estado de encendido o apagado en el que fue encontrado; tener presente:

- Si el dispositivo está encendido, anotar su fecha y hora y compararla con la fecha y hora del Personal de Primera Respuesta.

- El tiempo en un dispositivo se puede fijar dependiente o independiente de la Operadora de Telefonía Celular y puede verse afectada por el aislamiento de señales de radiofrecuencia.

- Si el dispositivo móvil está apagado, las actualizaciones de fecha y hora pueden darse una vez que el dispositivo sea encendido. Encender el dispositivo puede afectar sus registros de posición respecto a la ubicación actual. Si el registro de ubicación o posición última es fundamental para la investigación, estos datos se deben preservar antes del análisis del dispositivo. Si es posible a través de la colaboración de la Operadora.

k. Aislar el dispositivo de señales de radiofrecuencia, crea una "zona muerta" temporal para todo el tráfico de teléfono celular considerado evidencia, lo cual se logra:

- *Apagando el dispositivo en la incautación***:** si se realiza esta acción códigos de autenticación, como los códigos PIN y PUK de la tarjeta SIM, códigos de seguridad o de bloqueo, pueden ser requeridos para el acceso al dispositivo y a los datos, si éstos están habilitados, lo cual probablemente puede hacer al dispositivo y/o a la tarjeta SIM inaccesible para el análisis.

  Esto puede retrasar el análisis, en circunstancias en donde un retraso es inaceptable, como cuando una vida está en riesgo, el consejo de un especialista debe ser pedido; en el caso de algunos proveedores de servicio extranjeros los códigos PUK no están disponibles.

- *Colocando el dispositivo en una bolsa/contenedor protector de señales de radiofrecuencia, c*ausa que el dispositivo incremente la potencia para encontrar señal, la duración de la batería se reducirá debido al incremento de veces que el teléfono celular trata de conectarse con la red lo que puede causar que la batería se descargue rápidamente y eventualmente el teléfono celular se apague y producirse los efectos antes mencionados.

  Se puede causar pérdida de datos sobre dispositivos que tengan una memoria volátil, la cual es dependiente de la batería. Entonces el dispositivo necesita ser cargado mientras está dentro del ambiente protector o la entrega inmediata para el análisis al personal responsable es necesaria.

- *Utilizando Airplane mode,* requiere usar el teclado del teléfono, interactuando manualmente, esto desconecta al celular de la red y no siempre se encuentra en el mismo lugar para todos los dispositivos.

- *Petición a la Operadora de Telefonía Celular:* que puede deshabilitar al dispositivo de la red. Esto depende de la colaboración de la Operadora y no puede ser práctico para todos los casos. El aislamiento de señales de radiofrecuencia puede prevenir el bloqueo o borrado remoto, esto también previene que el dispositivo reciba nuevos datos de la Operadora y la posible evidencia puede ser sobrescrita.

La detección propiamente dicha consiste en tomar conocimiento del hecho ocurrido; los investigadores, deben realizar la observación de la escena y decidir acerca de la presencia de los peritos o especialistas que deben participar en la investigación.

- Concluida la identificación que impedía tocar la escena, se puede alterar la escena del hecho en busca de evidencias o algún rastro; se puede mover todo tipo de objetos en busca de huellas digítales o

de indicios de otro tipo, y en ese caso se debe volver a fotografiar los nuevos descubrimientos.

- La detección debe absorber toda la información inicial y asociativa al hecho sucedido.

- Recordar el Principio de *e-Locard*, este principio obligará a no descartar ningún dispositivo que tenga capacidad de almacenamiento. Dado que a simple vista no se puede concluir al respecto, se deben considerar, todos los dispositivos electrónicos como fuente posible de evidencia digital.

- Específicamente se buscan dispositivos con capacidad de procesar, transmitir y/o almacenar, además de otro tipo de dispositivos y documentación relacionadas con el teléfono celular.

- Cuando se identifique un nuevo dispositivo se deberá caracterizarlo técnicamente según su tipo, marco, modelo y estado (apagado o encendido).

La detección de evidencias fácilmente da una idea del perfil del sospechoso en cuanto a su conocimiento de la tecnología. Existen dispositivos que por sus características no las utiliza cualquier individuo. Algo tan simple como identificar el uso de *software* propietario o *software* libre puede decir sobre las características del sospechoso.

3. **Documentación relacionada con el dispositivo**: para realizar esta actividad es necesario tener en cuenta los siguientes pasos y diligenciar el formulario de identificación del dispositivo (Ver Anexo C).

   a. El personal de Primera Respuesta deberá, como objetivo considerar cualquier otro material y equipamiento relacionado con el dispositivo.

   Cables, cargadores, cajas en las que viene empacado el equipo, tarjetas de memoria, manuales, facturas telefónicas etc., material que

puede ayudar a la investigación y reducir al mínimo las demoras en cualquier análisis.

Materiales de empaquetamiento y papeles asociados pueden ser una buena fuente de códigos PIN y PUK.

Identificación de una conexión mediante un cable del teléfono celular a un computador o mediante conexiones inalámbricas ya sea mediante la interfaz *Bluetooth*, infrarrojo o *WiFi*; esta última puede ser una conexión a Internet dependiendo de las capacidades del teléfono celular. En este punto se recomienda validar mediante la observación las conexiones existentes y registrarlo en actas. Se debe asumir que como no se ve la presencia de conexiones inalámbricas, entonces no se puede afirmar su existencia o ausencia.

- Si el dispositivo se encuentra conectado a algún cargador o computador personal o de escritorio; determinar si hubo o no sincronización, pues al desconectarlo, se pueden ejecutar en él, comandos de eliminación de archivos.

- Si un dispositivo se encuentra conectado a un computador, se recomienda desconectar el dispositivo del computador para evitar la sincronización de datos y sobreescritura de información.

- En caso de estar conectado a un computador, verificar si el dispositivo se encuentra “montado”, de ser así, se debe desmontar antes de desconectarlo, pues el celular puede fallar o presentar daños.

- Etiquetar los cables según el dispositivo al que pertenecen.

Por último, tener en cuenta que algunos teléfonos pueden tener funciones de limpieza automática, las cuales borran los datos después de varios días. Por ejemplo, algunos teléfonos que tienen *Symbian* como sistema operativo comienzan a eliminar llamadas y registros de

sucesos después de 30 días, o cualquier otro período definido por el usuario.

b. Identificar y documentar los siguientes ítems sobre el dispositivo, sin afectar su estado.

- Estado (encendido/apagado)
- Estado de protección PIN (activado/desactivado).
- Estado de protección código de seguridad (activado/desactivado)
- Marca, Modelo (número/generación)
- Número de Serie
- Número ICCID
- IMEI
- Operador de telefonía celular
- Dimensiones
- Tarjeta de memoria externa (tarjeta *miniSD* o *TransFlash*)
- Cámara digital (ubicación - delantera o trasera del dispositivo)

4. **Documentación de los elementos incautados:** es necesario realizar la identificación y documentación (Ver Anexo D) de todos los componentes electrónicos o no, que se encuentren en la escena del crimen, relacionados al teléfono celular. Esto debido a que en el momento de realizar la detección de evidencia, en algunos casos no todos los elementos pueden ser incautados.

4.2.3.2 Preservación

Su objeto es preservar la evidencia electrónica encontrada en la escena del hecho con el fin de posteriormente realizar el análisis de la evidencia digital.

Todo proceso de investigación requiere de un registro confiable del o de los hechos producidos, plasmados de una manera adecuada en un acta, con todas las formalidades de rigor; de forma tal, que permita el estudio posterior, la reconstrucción en una época alejada de la ocurrencia o utilizarla en un proceso judicial.

1. **Creación del registro de cadena de custodia:** la cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso (Ver Anexo E).

   El objetivo de esta actividad es iniciar la documentación de la cadena de custodia, la cual debe ser diligenciada durante toda la investigación de manera estricta. La cadena de Custodia es un mecanismo que garantiza la autenticidad de los elementos probatorios colectados y examinados.

   Esto significa, que las pruebas correspondan al caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna. Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y preservación de dichos elementos.

   La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente:

   a. Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega.

   b. Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta.

   c. Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.

d. Etiquetas que tienen la misma información que los rótulos, pero pueden ir atadas a bolsas de papel Kraft, frascos, cajas de cartón o a sacos de Fibra.

e. Libros de registro (de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.

2. **Aseguramiento de la evidencia electrónica:** los dispositivos electrónicos en los cuales se almacena la evidencia digital, son frágiles y sensitivos a altas temperaturas, humedad, golpes, electricidad estática, y campos magnéticos.

   El Personal de Primera Respuesta debe tomar las precauciones necesarias con la documentación, fotografías, embalaje, transporte y almacenamiento de la evidencia digital para evitar la alteración, daño, o destrucción.

   Se recomienda seguir estos pasos:

   a. Embalaje: al momento de embalar la evidencia digital para su posterior transportación, se recomienda que el personal de primera respuesta en la escena del hecho realice lo siguiente:

   - Asegurarse que toda la evidencia colectada está apropiadamente documentada, etiquetada, marcada, fotografiada, videograbada o esbozada, e inventariada antes del embalaje. Todas las conexiones y los dispositivos conectados deben ser etiquetados para una posterior fácil reconfiguración del sistema.

   - Recordar que la evidencia digital puede contener evidencia latente, rastros de evidencia, o evidencia biológica y tomar los pasos apropiados para que esta evidencia sea preservada. La extracción de la evidencia digital debe ser realizada antes de llevar a cabo procesos de recuperación de otro tipo de evidencia.

   - Asegurarse que el teléfono celular esté empaquetado en un material que bloquee las señales de radiofrecuencia tales como bolsas de

aislamiento Faraday, o papel aluminio para evitar que información, como mensajes de datos puedan ser enviados o recibidos por los dispositivos. El Personal de Primera Respuesta debe estar consciente de que si inadecuadamente se embala, o se remueve del elemento protector, el dispositivo puede ser capaz de enviar y recibir información.

- Asegurarse de empaquetar todas las evidencias electrónicas y material relacionado como cargadores y cables en embalaje antiestático. Se debe utilizar bolsas de papel, sobres, cajas de cartón, y envases antiestáticos para este tipo de evidencia. Los materiales plásticos no deben utilizarse porque el plástico puede producir o transmitir electricidad estática y permitir la humedad, lo cual puede dañar o destruir la evidencia.

- Asegúrese de que todas las pruebas digitales sean empaquetadas correctamente para evitar que se doblen, rayen o deformen.

- Etiquetar todos los contenedores usados para embalar evidencia de manera clara y correcta.

- Asegurarse que ha sido creado el registro de cadena de custodia.

b. Transporte: cuando se transporte evidencia electrónica, se recomienda realizar por parte del Personal de Primera Respuesta en la escena del hecho lo siguiente:

- Mantener la evidencia electrónica fuera de campos magnéticos, como los producidos por los transmisores de radio, los imanes del altavoz. Otros peligros potenciales que el Personal de Primera Respuesta debe tener en cuenta; se relacionan a cualquier dispositivo o material que puede producir la electricidad estática.

- Evitar guardar las evidencias electrónicas en un vehículo durante períodos prolongados de tiempo. El calor, el frío y la humedad pueden dañar o destruir este tipo de evidencia.

- Asegurarse que los dispositivos electrónicos se empaqueten y aseguren durante el transporte para evitar daños por golpes y vibraciones.

- Mantener la cadena de custodia de todas las pruebas transportadas.

c. **Almacenamiento:** cuando el Personal de Primera Respuesta almacene evidencia electrónica se recomienda lo siguiente:

   - Asegurarse que esta evidencia electrónica está en un inventario de conformidad con las políticas de la agencia gubernamental.

   - Asegurarse que la evidencia electrónica se almacena en un entorno seguro, con temperatura controlada o en un lugar que no está sometido a temperaturas extremas o humedad.

   - Asegurarse de que la evidencia digital no está expuesto a campos magnéticos, humedad, polvo, vibración, o cualesquiera otros elementos que puedan dañar o destruirlo.

     - NOTA: Hasta la mínima Evidencia Digital puede ser muy valiosa, aunque éstas sean las fechas, horas, y ajustes de configuración del sistema. Las mismas se pueden perder por un almacenamiento prolongado del teléfono móvil, sin que se ayude a conservar esta información. Es de vital importancia el informar al custodio de pruebas y al examinador forense, qué dispositivos electrónicos requieren baterías para preservar los datos almacenados en ellos.

4.2.4 ANÁLISIS DE EVIDENCIA DIGITAL

La etapa de análisis de evidencias tiene por objeto encontrar los elementos de juicio necesarios para la resolución de la investigación judicial, para lo cual se recomienda seguir las etapas y fases mostradas en la Figura 4.6.

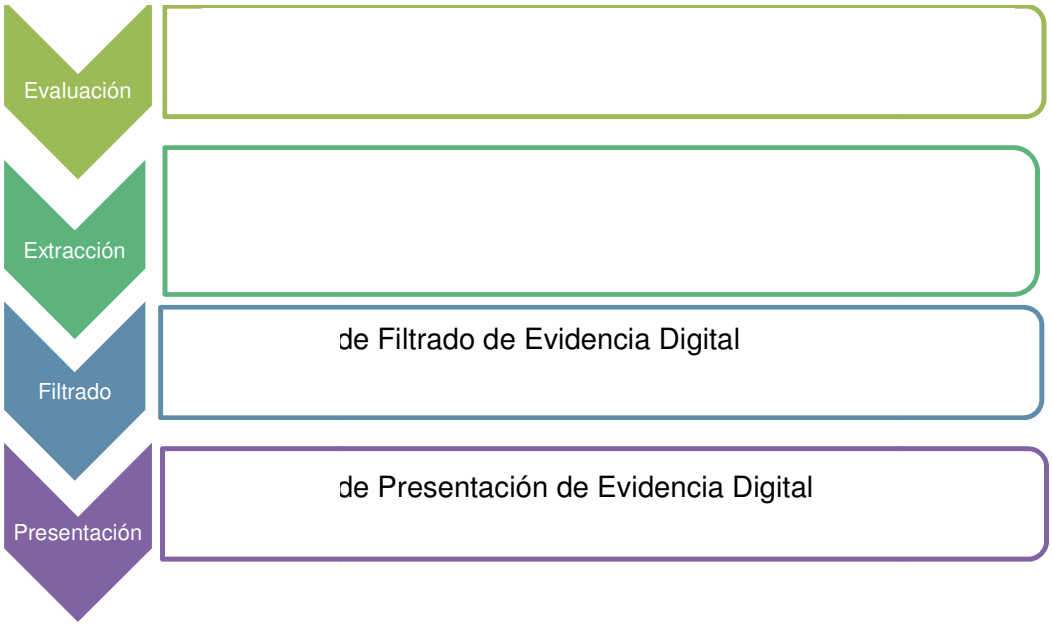


Figura 4.6: Etapas y Fases dentro del Ciclo de Análisis de Evidencia

4.2.4.1 Evaluación

En esta etapa se recepta la evidencia electrónica proveniente de la colecta en la escena del hecho. Esta evidencia llegará a un laboratorio, en este punto el investigador debe saber qué clase de delito se está investigando, con el propósito de discernir cuáles son las evidencias necesarias y relevantes para solucionar el caso; es así que en la escena deberá discriminar los medios digitales que más probablemente tengan valor en la investigación. Como se dijo anteriormente el objetivo del investigador es la evidencia admisible, pero antes de llegar a ella se debe encontrar la evidencia relevante.

1. **Documentación e Identificación del Dispositivo**: el objeto es conocer la escena del hecho, identificar las características del teléfono celular involucrado en la escena del crimen y verificar se cumpla la cadena de custodia.

   Se debe tener conocimiento cómo la evidencia fue transferida hasta llegar a manos del examinador o investigador forense, con ese fin se puede consultar los formularios: de elementos incautados y el de cadena de custodia.

Anotar cualquier característica física relacionada al estado del dispositivo (si falla al prenderse, está dañado, *display* roto, error de inicio etc.)

Fotografiar todos los aspectos externos visibles del dispositivo. En caso de no disponer de la etapa de colecta de manuales, cargadores, baterías asociadas al dispositivo, buscar estos materiales.

Al momento de identificar el dispositivo tomar en cuenta las siguientes recomendaciones.

a. Intentar documentar lo siguiente sobre el dispositivo sin afectar a su estado:

- Marca, Modelo
- Logo Operador
- Estilo del Teléfono Celular (*flip, clam,o slide*)
- Tarjeta de memoria externa (tarjeta miniSD, TransFlash etc.)
- Cámara digital (ubicación - delantera o trasera del dispositivo)
- Identificadores (ESN o IMEI) y SIM (ICCID).
    - ✓ Este tipo de información sólo se debe extraer si el dispositivo está apagado. En algunos dispositivos, como teléfonos inteligentes, no se le puede quitar la tapa posterior y la información estará en la parte delantera del dispositivo.

b. Descargar el manual del usuario del dispositivo para entender las características del mismo; si el dispositivo no es reconocido o similar a uno que nunca ha sido analizado, es vital obtener una copia electrónica del manual del usuario para familiarizarse con las características y la navegación del teléfono celular.

- El examinador debe ingresar a foros web forenses para ver si otro examinador ya ha analizado el dispositivo. Hay varios recursos

basados en la web que mantienen una base de datos de dispositivos y de los mecanismos que han funcionado con éxito.

2. **Aislamiento de señales de radiofrecuencia:** con el fin de proteger y preservar la evidencia digital. Para ello el Personal de Primera Respuesta debió haberlo realizado en el momento de la Colecta caso contrario el Examinador debe registrarlo, aislar el teléfono celular de señales de radiofrecuencia y realizar el análisis respectivo, considerando:

   a. **Aislar al dispositivo de la red para el análisis en el laboratorio forense,** esto se puede lograr a través de:

      - *Un inhibidor de señales portable*, no recomendado, el uso de estos dispositivos ya que puede interferir con la cobertura de la red fuera del área de análisis.

      - *Un cuarto inhibidor de señales*, recomendado, para tener un cuarto fijo, el costo es relativamente alto y los exámenes están vinculados a una localización específica, reduce la movilidad.

        Bolsas de Faraday son una solución económica y portable, pero probablemente son menos seguras que un cuarto fijo (los cables de alimentación de voltaje no pueden ser usados en la bolsa porque pueden funcionar como antenas).

        La duración de la batería se reduce por el incremento de la potencia consumida debido a las veces que el teléfono celular trata de conectarse a la red, el dispositivo debe ser cargado totalmente antes del examen.

      - *Usar una caja/recipiente protector,* esto permite que las examinaciones puedan conducirse seguramente en diferentes áreas geográficas.

        La duración de la batería se reduce debido a que la potencia consumida se incrementa, porque el equipo móvil trata de conectarse a la red.

Como tal, el dispositivo se debe cargar totalmente antes del examen o conectar a una fuente de energía portable dentro de la caja.

Los cables dentro de la caja deben estar completamente protegidos para prevenir la intrusión de señales de la red.

4.2.4.2 Extracción

Esta etapa tiene por objeto planificar el proceso de extracción de la evidencia digital, documentar el mismo con el fin de evitar la pérdida de datos importantes para el caso, y utilizar las Funciones *Hash* para garantizar la integridad de la evidencia digital.

1. **Elección de la Herramienta(s) Forense(s) de Extracción:** El objetivo de esta fase es realizar la elección de la(s) herramienta(s) forense(s) que va(n) a ser utilizada(s) durante la investigación, dichas herramientas serán seleccionadas dependiendo del nivel de análisis que se quiera tener en la investigación o el contexto en el cual haya sido encontrado el dispositivo.

   En el nivel básico, las herramientas forenses estándar deben recuperar datos del equipo móvil o terminal celular y la tarjeta SIM, es decir podrían analizar lo que el usuario observa, además de recuperar los mensajes de texto borrados de la tarjeta SIM, utilizando un lector de tarjetas.

   En el nivel intermedio, el uso de herramientas que cumplan con la técnica de *Hex Dump* (volcado de memoria flash o *"flash dump*") del terminal celular deben ser capaces de recuperar datos borrados y otros datos útiles del Equipo Móvil y la Tarjeta SIM, pero se requiere de *hardware* especializado y experiencia.

   En el nivel avanzado, remover los chips físicos de memoria es posible, pero requiere *hardware* muy específico y experiencia. Utilizando la técnica *Chip Off* se podría estar en la capacidad de recuperar datos borrados (más allá que los *flashes dump*s).

La(s) elección(es) de la(s) Herramienta(s) se puede llevar a cabo teniendo en cuenta las herramientas nombradas en el Capítulo 3 de este proyecto de titulación.

Se recomienda en esta fase:

a. Utilizar el *software* que está diseñado para propósitos de análisis forense, siempre que sea posible. Muchas herramientas adquieren los datos vía petición al sistema operativo, por lo tanto es inevitable la existencia de dos vías para la transferencia de datos.

b. El dispositivo muchas de las veces no es soportado por la herramienta forense, y solamente puede ser reconocido por el administrador de teléfonos del modelo en particular.

c. Si se utilizan herramientas no forenses, éstas deben ser probadas en ambientes seguros, con la misma marca y el modelo del dispositivo que va a ser examinado de manera formal y así entender el funcionamiento y efectos que se pueden dar. Estas herramientas deben ser utilizadas como última opción en el proceso de extracción.

d. Asegurarse que la batería del dispositivo contenga aproximadamente al menos el 50% de carga antes del análisis.

Es muy probable la necesidad de tener múltiples herramientas ya que existe un conjunto de herramientas con las que actualmente se puede extraer todo tipo de información de un teléfono celular. Recuerde que debe recopilar un conjunto de herramientas y otros recursos específicos para el dispositivo a analizar pues cada dispositivo es diferente entre marcas y modelos.

e. Los examinadores deben aceptar que el proceso de extracción de algunos tipos de datos puede afectar su estado. Por ejemplo, la recuperación de mensajes SMS no leídos a través del equipo móvil o terminal celular da como resultado que éstos cambien su estado a ‘’leídos”. Esto puede ser

inevitable, pero debe ser registrado, porque extracciones posteriores pueden producir resultados diferentes.

2. **Proceso de Extracción:** el objeto de esta etapa, es llevar a cabo la adquisición y el análisis de la evidencia digital, registrando todo lo encontrado en el formulario (Ver Anexo F).

   Se debe tener especial cuidado en la preservación de la integridad y admisibilidad de la evidencia digital.

   a. Realizar la documentación pertinente al caso en investigación, consiste en la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar a cabo un historial de todas las actividades que se llevan a cabo durante el proceso de adquisición de evidencia. Esta información es útil en la fase de presentación de la evidencia.

   b. Adquisición y búsqueda de evidencia digital, el objeto es realizar la adquisición y la búsqueda en profundidad de evidencia digital. La(s) herramienta(s) escogida(s) para ello, revelarán datos escondidos, eliminados, modificados o corruptos. Para realizar esta actividad es necesario seguir las siguientes recomendaciones:

      - *Dispositivo apagado*: Se procederá con el examen externo y/o documentación del dispositivo. Si el dispositivo contiene tarjeta SIM o tarjeta de memoria, analizar esto primero. Lo ideal sería no colocar la tarjeta SIM nuevamente en el equipo móvil o terminal, ya que los datos se pueden sobrescribir cuando se encienda el teléfono celular, por lo cual se recomienda:

        - Analizar la tarjeta SIM para preservar la posición de la última información de uso, y permitir la extracción de los mensajes de texto borrados de la tarjeta SIM. Los mensajes de texto borrados en una tarjeta SIM no se puede extraer a través del dispositivo (mientras que la tarjeta SIM está dentro del dispositivo), se debe utilizar un lector de tarjetas SIM.

- Para preservar la SIM original, el Examinador debería idealmente clonar la tarjeta SIM y usar esta tarjeta clonada en el interior del dispositivo durante el análisis de la memoria del dispositivo. Una tarjeta SIM clonada imitará la identidad de la tarjeta SIM original y puede no permitir acceso de red.

  Estas tarjetas necesitan ser configurados con la identificación exacta del suscriptor para "engañar" al terminal o equipo móvil y que "piense" que la SIM original está presente, Aunque los datos del usuario se mantienen, hay la posibilidad que otros datos en el terminal se puedan perder o cambiar como resultado de que esta tarjeta sea insertada.

- Pedir a la Operadora de Telefonía Celular que deshabilite la cuenta del suscriptor, es una opción que requiere la intervención del proveedor, que puede estar o no dispuesto a cooperar.

  Este enfoque no ha sido probado a fondo y los efectos en el terminal y la tarjeta SIM no se conocen al momento de la extracción. Por lo tanto, esto no es un enfoque recomendado en este momento, sin embargo, si la cuenta del suscriptor está deshabilitada, cualquier mensaje de voz dentro del sistema para esa cuenta se pueden perder.

- Si se encuentra una tarjeta de memoria externa en el teléfono celular, tomar las medidas adecuadas para proteger contra escritura a la tarjeta durante el proceso de análisis, obtener la imagen y utilizar herramientas tradicionales de informática forense como EnCase, FTK, WinHex, ProDiscover, iLook.

  Hay adaptadores USB para tarjetas de memoria, que se pueden conectar a un puerto bloqueado en escritura USB y hacer una imagen forense de la tarjeta de memoria.

- Análisis de la memoria interna del teléfono celular apagado debe ocurrir después, asegurándose de que el dispositivo está aislado de señales radiofrecuencia durante el análisis.

- *Dispositivo encendido:* Proceder a la extracción de datos o a la captura de pantallas del teléfono celular. Como se mencionó anteriormente, el ciclo de carga del dispositivo, puede causar que el dispositivo inicie mecanismos de autenticación. Una vez que la extracción de datos desde el terminal se complete, se debe realizar el análisis de la tarjeta SIM y/o tarjetas de memoria.

  - La descarga de la batería conduce a la pérdida de datos: Si el dispositivo es de un tipo donde la descarga de la batería puede causar pérdida de datos, entonces extraer los datos inmediatamente o mantener la batería en carga hasta que el dispositivo se puede analizar, en un entorno aislado de señales de radiofrecuencia.

    La mayoría de los dispositivos GSM contienen tres interfaces para la conexión del teléfono celular con otros dispositivos electrónicos que son: cable, infrarrojo y *bluetooth*, pero se recomienda utilizar una interfaz de conexión confiable, que minimice el intercambio de datos.

  - Cable: la conexión mediante cable es segura, generalmente confiable y tiene un menor impacto en el teléfono celular, con menor cantidad de efectos negativos, respecto al intercambio de datos con Infrarrojos y *Bluetooth*.

  - Infrarrojos (IrDA): menos seguro y menos fiable que el cable, es necesario que el examinador interactué manualmente con el teléfono celular, para activar o activar el IrDA.

  - *Bluetooth*: la interfaz menos segura de las antes mencionadas, requiere la interacción manual con el teléfono celular, y se

escriben datos en el teléfono durante el proceso de autenticación.

Herramientas de *software* para análisis forense de teléfonos celulares no puede tomar ventaja de las tres opciones de conexión para la extracción de datos y, a menudo el fabricante recomienda un método de conexión.

Captura de Pantallas (último recurso): es posible que las herramientas no puedan extraer los datos, por lo que un examinador debe tomar fotografías de la pantalla, mostrando la información de interés. Un examinador puede hacer esto utilizando una cámara profesional de alta calidad con un *software* especializado.

- *Dispositivos GSM sin tarjeta SIM:* Al encender un dispositivo GSM que no contiene una tarjeta SIM, en la pantalla generalmente se muestra el mensaje "Insertar SIM". Sin la tarjeta SIM utilizada por última vez del dispositivo específico, el Examinador no será capaz de llevar a buen término la adquisición de evidencia del dispositivo. Sin embargo, no todos los dispositivos GSM requieren una tarjeta SIM para poder realizar el análisis. En este caso, hay opciones que el examinador pueda explorar:

  - Es recomendable hacer una copia forense de la tarjeta SIM que se utilizó por última vez en el dispositivo. Esto puede ser determinado teniendo el IMEI del dispositivo GSM, y realizar la petición al proveedor de servicios de red de los últimos ICCID conocidos y el IMSI que se utilizó para ese dispositivo, siempre que sea presentada la documentación oportuna a la Operadora. El ICCID y el identificador IMEI se utilizan para hacer un clon forense de una tarjeta SIM, utilizando la herramienta adecuada.

- Con la tarjeta SIM clonada e insertada en el dispositivo, el teléfono GSM puede ser entonces encendido con éxito sin causar pérdida de datos en el dispositivo.

- A falta de una herramienta que pueda crear un clonado forense de la tarjeta SIM, un examinador puede tratar, utilizando un tarjeta SIM en blanco es decir que nunca ha sido activada, para iniciar correctamente el dispositivo. Esto se debe utilizar sólo como un último recurso.

- El insertar una tarjeta SIM diferente a la que estaba en el dispositivo GSM causará la pérdida de los datos del teléfono, ya que el dispositivo GSM buscará el ICCID pasado conocido y el identificador IMSI.

3. **Preservar la integridad de la evidencia digital:** el objeto de esta fase es mantener la integridad de toda la evidencia digital recolectada, mediante la utilización de funciones *Hash* tales como MD5 y SHA-1, comprobar que las herramientas obtengan valores *Hash* coherentes, es decir que se obtenga el mismo valor *hash* luego de dos o más adquisiciones.

   Para asegurar la integridad de cada elemento extraído, se recomienda generar varias copias de la extracción realizada, asegurarlas en un lugar restringido y trabajar siempre con una copia de respaldo exactamente igual a la original para prevenir alteraciones sobre su contenido durante la fase de filtrado de la evidencia digital.

4.2.4.3 Filtrado

Se la conoce también como la fase de análisis en la investigación forense, consiste en la búsqueda sistemática y profunda de evidencia digital relacionada con la investigación judicial, en donde el investigador busca filtrar todos los elementos de evidencia digital preservados de la escena del delito a fin de separar los elementos que no tienen valor como evidencia de los que sí.

1. **Fase de Filtrado de Evidencia Digital:** el objeto de esta fase es realizar el filtrado de los datos obtenidos en la Extracción de evidencia digital, para construir una línea de tiempo, de forma tal que los eventos se puedan correlacionar y a partir de esto reconstruir la escena y obtener la mayor cantidad de detalles del incidente. Para ello, se deben realizar las siguientes acciones:

   a. Identificar propiedades generales de la adquisición

   b. Estructura de la adquisición

   c. Identificación de las particiones actuales y anteriores (las que sea posible recuperar)

   d. Identificación del sistema de archivos

   e. Identificación de archivos existentes y protegidos

   f. Determinación del sistema operativo

   g. Recuperación de archivos eliminados

   h. Identificación de información oculta y de aplicaciones instaladas

   i. Consolidación de archivos potencialmente analizables

   j. Análisis de datos:

      - Identificadores del dispositivo y del proveedor de servicio
      - Fecha/hora
      - Lenguaje
      - Información de la lista de contactos
      - Información del calendario
      - Mensajes de texto

- Registro de llamadas (recibidas, perdidas, marcadas)
- Correo electrónico
- Fotos /Videos / Audio
- Mensajes multimedia
- Mensajería instantánea y navegación web
- Documentos electrónicos
- Revisión de los registros del sistema
- Identificación de rastros de conexiones (*Bluetooth*, Infrarrojo, cable)
- Consolidación de archivos sospechosos
- Análisis de los archivos sospechosos
- Determinación de los archivos comprometidos con el caso
- Obtención de la línea de tiempo definitiva

4.2.4.4 Presentación

El objeto de esta etapa es presentar la documentación de todas las acciones, eventos y hallazgos obtenidos durante el proceso de investigación. Todo el personal está involucrado en esta etapa y es vital asegurar la integridad de la cadena de custodia de la evidencia. Los reportes de resultados generalmente, son generados por la herramienta que se utiliza para efectuar el análisis.

Involucra la presentación de la evidencia digital encontrada, y los resultados del análisis de la misma al equipo de investigación, ésta es la etapa final de la investigación, es cuando se presentan los resultados, los hallazgos del investigador.

1. **Fase de Presentación de Evidencia Digital:** La presentación debe ser entendible y convincente, es decir aquí se debe reseñar los procedimientos

y las técnicas utilizadas para identificar, preservar, evaluar, extraer y filtrar la evidencia de manera que exista certidumbre en los métodos usados, aumentado así la credibilidad del investigador en un contra examen de los mismos.

Para el desarrollo del proceso judicial, la totalidad de reportes que fueron creados durante los ciclos de colecta y análisis deben ser presentados.

a. Formulario de identificación de personal
b. Formulario de identificación y detección de la escena del hecho.
c. Formulario de Identificación del Dispositivo.
d. Formulario de Elementos Incautados.
e. Cadena de Custodia.
f. Formulario de Análisis del dispositivo
g. Conclusiones de la investigación (Dentro del Formulario de Análisis del Dispositivo)

Además se debe tener presente que en este tipo de investigaciones, si bien es cierto requieren de conocimientos adicionales y de una buena preparación, el testificar dentro de un proceso penal para los investigadores en esta área, es igual que testificar en un caso de robo o en un homicidio, para lo cual debe estar preparado.

Recordar que la misión del Fiscal es el presentar la evidencia colectada por el investigador dentro del juicio, esto se lo debe efectuar de manera comprensible, a fin de que la evidencia presentada persuada al Juez o Tribunal de la existencia de un delito y de la culpabilidad o inocencia del acusado.

Por tanto el Fiscal debe conocer y entender la evidencia lo suficiente para explicar a cualquiera su efectividad, no dejando vacios para que el abogado defensor los explote, haciendo que la evidencia presentada sea confiable y digna de credibilidad más allá de cualquier duda razonable.

CAPÍTULO V

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

- ✓ Las nuevas tecnologías, crean nuevas vulnerabilidades, y en los teléfonos móviles no es la excepción, de hecho, se tiene una arquitectura y software totalmente diferente que varía según el fabricante de teléfonos móviles (Nokia, Motorola, Sony Ericsson, *BlackBerry*, Hp, Samsung, Lg, Apple, entre otros) ya que emplean sistemas operativos y estructuras de almacenamiento heterogéneos.

- ✓ Debido a los cambios rápidos en la tecnología los teléfonos celulares presentan un problema especial para la aplicación de la ley. Hay más de tres mil modelos de teléfonos celulares en uso hoy en día. Muchos de estos dispositivos utilizan conexiones y sistemas operativos propietarios, lo que hace extremadamente difícil para la extracción de las pruebas forenses.

- ✓ El análisis forense se puede definir al conjunto de disciplinas cuyo objeto común es el de la materialización de la prueba a efectos judiciales mediante una metodología o un procedimiento científico. Cualquier análisis se convierte en forense en el momento que sirve al procedimiento judicial.

- ✓ Se recomienda que el análisis forense de teléfonos celulares sea un procedimiento estándar, aceptado por la comunidad judicial en una investigación enfocada en evidencia digital, con la ayuda de herramientas tecnológicas para extracción y análisis de evidencia digital, con el fin de validar dicha evidencia.

- ✓ El número y la variedad de modelos de teléfonos que salen al mercado mundial son significativos cada año, creando cierta dificultad para los fabricantes de herramientas forenses para mantener sus productos al día.

- ✓ El análisis físico de evidencia digital consiste en llevar a cabo el volcado de memoria del teléfono celular y/o la Tarjeta SIM, es decir, tomar la imagen

binaria bit a bit de la memoria del dispositivo comprometido, con sus respectivos valores *hash*.

- ✓ El análisis lógico de la evidencia digital consiste en llevar a cabo la obtención de información almacenada en el teléfono celular, manteniendo el sistema de archivos, pudiendo obtener información como: lista de contactos, historial de llamadas, historial de mensajes, imágenes y videos, correo electrónico, eventos de calendario, información entre el dispositivo y el computador relacionado; la información obtenida con este método es de fácil interpretación respecto a la obtenida con el análisis físico.

- ✓ Las herramientas forenses de análisis lógico realizan la recuperación de datos, a través de protocolos soportados por el dispositivo de análisis, sean éstos de facto o de jure. Por el contrario las herramientas de análisis físico realizan un análisis a través de señales eléctricas y leen directamente la información en la memoria del teléfono celular.

- ✓ Se recomienda utilizar herramientas forenses, ya que éstas ayudan a recopilar la información de una manera exacta, asisten en la recuperación de evidencia digital sin borrarla o alterarla, pueden obtener un valor *hash* para verificar la integridad de la evidencia, agilitan el proceso para analizar toda la información encontrada.

- ✓ La herramienta ZRT2 redimensiona las imágenes o audio obtenido automáticamente en una plantilla de informe, creando una presentación personalizada para el tribunal, ayudando a visualizar claramente los motivos del acusado o de las acciones que se recuperaron directamente desde su teléfono celular.

- ✓ Para simplificar el proceso de recuperación de datos, debería existir un método forense que permita utilizar una interfaz común y un protocolo estándar para todos los modelos y marcas teléfonos celulares, que permita la recuperación de datos; con este fin existe una norma propuesta por

Open Mobile Terminal Platform[66] (OMTP) que especifica el uso de micro USB, como una interfaz universal, en la que el cable del fabricante serviría para proporcionar una conexión para la energía y permitir las comunicaciones. Su capacidad de sincronización de datos con el tiempo, generarían una oportunidad para tener una forma más consistente de recuperación de datos, siempre y cuando, sea adoptada por los fabricantes.

- ✓ El sistema propuesto describe una transformación de los elementos obtenidos en un contexto físico (evidencia electrónica) mediante la colecta de evidencia en la escena del hecho, pasando luego a un contexto virtual (evidencia digital) mediante el análisis de evidencia y terminando en el contexto legal, proporcionando bases legales para que esta evidencia sea admitida.

- ✓ En la actualidad se encuentran disponibles varias herramientas para recuperar evidencia digital, por lo que se recomienda antes de utilizar cualquier tipo de herramienta forense en los dispositivos móviles a analizar, tener conocimiento previo de las funcionalidades, y limitaciones que posee dicha herramienta, evitando con ello tergiversar de forma accidental la información del teléfono celular.

- ✓ Se recomienda seguir estos cuatro los principios para tener éxito en el análisis forense a realizarse, éstos son: Minimizar la pérdida de los datos, almacenar y guardar todo, analizar todos los datos recolectados y reportar los hallazgos.

- ✓ De las herramientas analizadas para dispositivos móviles, no todas pueden realizar un análisis con las diversas interfaces (cable de datos, *bluetooth*, IrDA)

[66] *Open Mobile Terminal Platform (OMTP)* fundada en junio del 2004 por un grupo de ocho operadores de telefonía móvil. Para julio del 2010 cuenta con nueve operadoras AT&T, Deutsche Telekom AG, KT, Orange, Smart Communications, Telecom Italia, Telefónica, Telenor y Vodafone además, es auspiciado por dos fabricantes de teléfonos celulares Ericsson y Nokia. Se creó con el objetivo de simplificar la experiencia del cliente de servicios móviles de datos y mejorar la seguridad de dispositivos móviles.

- ✓ Al realizar el análisis de información de los teléfonos celulares a través de interfaces inalámbricas, aumenta el riesgo de intercambio de información y aumenta el tiempo de extracción y transferencia de datos con las herramientas utilizadas, con lo cual no se garantiza la integridad de la evidencia digital.

- ✓ Se recomienda para la extracción de evidencia digital utilizar un cable de datos, ya que produce resultados superiores a la extracción utilizando interfaces inalámbricas. Sin embargo, a pesar de que una interfaz inalámbrica sea una alternativa, cuando el cable de datos no está disponible, debe utilizarse como un último recurso debido a la posibilidad de modificar la información del dispositivo.

- ✓ Cuando se analizan dispositivo móviles a través de la interfaz de *bluetooth*, se realiza una comunicación previa con la herramienta forense, por medio de un emparejamiento de la comunicación (sincronización), sin que esto afecte los datos originales del dispositivo móvil.

- ✓ Gran parte de las herramientas forenses utilizadas obtienen la codificación *hash* MD5, sin embargo, esta codificación puede ser vulnerada, por lo que se recomienda utilizar otro tipo de codificación.

- ✓ OPM II y *Device Seizure* permiten obtener información (mensajes, imágenes, videos) encontrada en el dispositivo móvil con un detalle de localización, de donde fue realizada tal acción.

- ✓ Cuando el dispositivo móvil se encuentra bloqueado, gran parte de las herramientas de software no pueden acceder a ningún tipo de información del dispositivo en cuestión.

- ✓ Para recuperar exitosamente información borrada, este proceso debe realizarse lo más pronto posible, evitando que otro tipo de información sea sobrescrita en esa localidad de memoria.

- ✓ En dispositivos móviles inteligentes las herramientas de extracción física permiten instalar o no un *bootloader*, es recomendable no instalarlo y así

evitar que se pueda cambiar cierta información y con ello afectar la evidencia contenida en el dispositivo.

- ✓ El poder buscar información específica en varias de las herramientas utilizadas, muestra la importancia del análisis, no solo relacionado al hecho en cuestión, sino a relacionar información y por ende conocer el círculo social del implicado.

- ✓ La adquisición de datos mediante un enfoque de bajo nivel utilizando JTAG, es el mejor método para recopilar datos en una memoria *flash*, independientemente del tipo de teléfono celular. Si una herramienta forense usa el interfaz JTAG, se pueden recuperar los datos eliminados como SMS, fotos, y llamadas realizadas.

- ✓ La adquisición de datos de la memoria *flash* completa, se puede hacer utilizando el método físico por método de bajo nivel. El método de nivel de acceso físico puede mejorar la tasa de recuperación de datos borrados que cuando se utiliza el método de nivel de acceso lógico.

- ✓ El desarrollo de métodos fiables de recuperación de datos es crítico para cualquier investigación forense. Hay diferentes herramientas forenses de *software* y *hardware* disponibles en la actualidad que intentan recuperar datos de teléfonos móviles, sin embargo la mayoría de ellos trabajan de forma selectiva debido a la falta de normas en el mercado de la telefonía móvil.

- ✓ El aumento de almacenamiento de memoria y cámaras digitales de alta calidad es común entre los teléfonos móviles inteligentes, lo que los hace capaces de almacenar grandes cantidades de imágenes. Estas imágenes pueden contener metadatos, o información adicional incorporada, que describe los detalles críticos sobre la imagen (hora y fecha de la imagen).

- ✓ Los dispositivos móviles poseen una dinámica de datos, es decir que no tienen un método no invasivo para acceder a los datos almacenados. En concreto, los datos de los teléfonos celulares están cambiando

constantemente, independientemente de los métodos convencionales de bloqueo de escritura.

- ✓ Se recomienda bloquear las señales de entrada y salida de un dispositivo inalámbrico, para evitar la pérdida o sobre escritura de información en el dispositivo, para lo cual se puede utilizar bolsas y cajas de Faraday.

- ✓ Al analizar un dispositivo móvil, no se debe abrir correos electrónicos ni mensajes de texto, que no hayan sido leídos por el propietario del dispositivo; además no se puede contestar llamadas telefónicas entrantes del dispositivos incautado, porque se presentarían dificultades legales, al no tener el consentimiento del propietario, sobre todo si el examen no se lleva a cabo de manera oportuna.

- ✓ La idea principal del análisis forense de teléfonos celulares, es realizar un estudio total de todo tipo de evidencia digital que se encuentre en un teléfono celular e involucrada en un crimen, con el fin de hacer que esta evidencia cobre un valor legal, y que así mismo, sea admisible a la hora de entablar proceso judiciales en los cuales esta evidencia tenga un carácter determinante en el mismo.

- ✓ Cuatro diferentes pasos son identificados como precedente para lograr la admisión de cualquier evidencia: autenticidad, fiabilidad, entendimiento y credibilidad, pero al aplicar estos pasos en evidencia digital, surge una serie de problemas relacionados a la probatoria de que la evidencia existe en la realidad físicamente, es por esto la necesidad de un procedimiento estándar aceptado por la comunidad judicial ecuatoriana.

- ✓ La evidencia digital es muy poderosa, es la perfecta memoria de lo que ha sucedido en una escena del delito o del hecho, no existe razón para que ésta mienta, y no pueda eliminarse o cambiarse como una bala o una arma de fuego.

- ✓ El talón de Aquiles de la evidencia digital está en su comprensión por parte de Abogados, Jueces y Fiscales, esto en la medida del conocimiento de la función que tiene la tecnología ya sea en la descubrimiento de esta clase

de evidencia, en su recolección, en su análisis y después en su presentación. Por tanto la mala interpretación y desconocimiento de la tecnología y de sus detalles puede ser la causa para que los participantes dentro de un proceso penal no aprecien la importancia y relevancia que tiene la evidencia digital en los procesos judiciales y de investigación.

- ✓ Es necesario realizar una fluida traducción entre la tecnología y los términos legales, esto con la finalidad de usar un lenguaje claro y así evitar errores de interpretación y equívocos en esta clase de procesos que tienen como eje principal la evidencia digital.

- ✓ En el Ecuador existe la Ley de Comercio Electrónico y Mensajes de Datos, que se enfoca en las infracciones informáticas, como ya se demostró diferente al análisis de teléfonos celulares, creando dificultad para sancionar al infractor, sin contar que gran parte de los ecuatorianos desconocen las leyes que están vigentes en nuestro país.

- ✓ Existe una gran dificultad al realizar un análisis forense en dispositivos móviles, dadas las diferencias que existen entre los dispositivos de diferentes fabricantes así como, las numerosas diferencias entre modelos y versiones del mismo fabricante.

- ✓ El análisis forense en dispositivos móviles aparece como una necesidad latente y necesaria a nivel de las investigaciones actuales en cualquier país del mundo, por esta razón, se recomienda no descuidar los avances tecnológicos en este tema; para esto se deben generar convenios a nivel de investigación que involucren a los técnicos y a los entes de policía judicial.

- ✓ La Legislación del Ecuador puede ser mejorada en el ámbito de Delitos relacionados con evidencia digital, al aclarar especificaciones técnicas con respecto a las sanciones de los involucrados en estos delitos.

El desarrollo de este proyecto de titulación brinda una perspectiva diferente en cuanto, a como la tecnología puede ayudar a resolver actos delictivos; para ejemplificar esto, en el Anexo G, se muestra el seguimiento que debería tener la

evidencia digital a través de los formularios propuestos y la utilización de herramientas forenses analizada anteriormente.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS

- ALZAROUNI, Marwan, Mobile Handset Forensic Evidence: A Challenge For Law Enforcement, School of Computer and Information Science, Edith Cowan University.
- DANKER Shira; AYERS Rick; MISLAN Richard P., Hashing Techniques for Mobile Device Forensics, Small Scale Digital Device Forensics Journal, vol. 3, no. 1, ISSN 1941-6164, June 2009
- WOLLESCHENSKY, Lars, Cell Phone Forensics, Seminararbeit, Ruhr-Universität Bochum, August 2007.
- JANSEN Wayne A.; DELAITRE Aurelien; Reference Material For Assessing Forensic Sim Tools, Paper No. ICCST 2007-74, 2007
- JANSEN Wayne A.; DELAITRE Aurelien; Mobile Forensic Reference Materials: A Methodology and Reification, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg-MD 20899-8930, Publication NISTIR 7617, October 2009
- ROSSI, M.: Internal Forensic Acquisition for Mobile Equipments. Dipartimento di Informatica, Sistemi e Produzione, Università di Roma "Tor Vergata". (2008).
- BROTHERS, Sam, Cell Phone and GPS Forensic Tool Classification System, 2009.
- SOBIERAJ, Sean, Mobile Device Forensics Case File Integrity Verification, A Thesis Submitted to the Faculty of Purdue University, West Lafayette, Indiana, may 2008.
- KIPPER, Gregory; "Wireless Crime and Forensic Investigation"; Auerbach Publications; 2007.

- ARIZA, Andrea; RUIZ, Juan; CANO Jeimy, iPhone 3G: Un Nuevo Reto para la Informática Forense, Departamento de Ingeniería de Sistemas, Pontificia Universidad Javeriana, Carrera 7 No. 40 – 62, Bogotá, Colombia, 2008
- REITH, M; CLINT, C; GUNSCH, G; An Examination of Digital Forensic Models. International Journal of Digital Evidence, Air Force Institute of Technology, Volume 1 Issue 3, 2002.
- CARRIO, Alejandro, Justicia Criminal, Citado por JAUCHEN, Eduardo, Tratado de la prueba material, Rubinzal - Culzoni Editores, p. 614, 2000.

CITAS BIBLIOGRÁFICAS

[2] BECERRIL SIERRA, Israel, El Análisis Forense en Dispositivos Móviles y sus Futuros Riesgos, Revista Digital Universitaria, 10 de abril 2008, Volumen 9, Número 4, ISSN: 1067-6079

[4] CASEY, Eoghan, Digital Evidence and Computer Crimen, Página 9, 2da Edición, Edit Elsevier Ltda, 2004

[5] Miguel López Delgado, Análisis Forense Digital, Página 5, 2da Edición, 2007

[6] SWGDE Scientific Working Group on Digital Evidence.

[8] ZDZIARSKI, J., iPhone Forensics, Recovering Evidence, Personal Data & Corporate Assets. O Reilly Media, Inc. (2008)

[13] MARTIN Andrew, Mobile Device Forensics, GCFA Gold Certification, August 29, 2008.

[14] MEZA AYALA, María José, Fraude en Telecomunicaciones, Dirección General de Investigación en Telecomunicaciones, Supertel

[18] SAUTER Martin, Communication Systems for Mobile Information Society, Editorial Wiley, 2006

[19] JANSEN, Wayne; AYERS Rick, Guidelines on Cell Phone Forensics, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg-MD 20899-8930, Special Publication 800-101, May 2007.

[20] WILLIAM, Phil.: Crimen Organizado y Cibernético, sinergias, tendencias y respuestas, Centro de Enseñanza en Seguridad, Universidad Carnegie Mellon.

[21] ACURIO DEL PINO, Santiago; PAEZ, Juan.: Derecho y Nuevas Tecnologías, Corporación de Estudios y Publicaciones (CEP), Junio 2010, Primera Edición.

[22] ASSOCIATION OF CHIEF POLICE OFFICERS.: Good Practice Guide for Computer-Based Electronic Evidence, version 4.0, págs: 45 a 51.

REFERENCIAS ELECTRÓNICAS

- http://www.supertel.gov.ec/pdf/estadisticas/sma.pdf, última visita Agosto 2010.
- http://www.gsmworld.com/newsroom/press-releases/2010/5265.htm, última visita Agosto 2010.
- BREZINSKI, D; KILLALEA, T.: Guidelines for Evidence Collection and Archiving. IETF RFC 3227. (2002). http://www.ietf.org/rfc/rfc3227.txt, última visita Agosto 2010.
- DELGADO, M., Análisis Forense Digital. Hackers y Seguridad, 2nd ed. (2007) http://www.criptored.upm.es/guiateoria/gt_m335a.htm última visita Agosto 2010.
- BEM, D; HUEBNER, E; Computer Forensic Analysis in a Virtual Environment. International Journal of Digital Evidence. Volume 6, Issue 2. (2007). http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf, última visita Agosto 2010.

- CASTILLO, C; ROMERO, A; Cano, J.: Análisis Forense Orientado a Incidente en Teléfonos Celulares GSM: Una Guía Metodológica. Conf. XXXIV Conferencia Latinoamericana de Informática, Centro Latinoamericano de Estudios en Informática (CLEI). (2008). http://www.clei2008.org.ar/, última visita Agosto 2010.

- WILLASSEN, S.: Forensic analysis of mobile phone internal memory. Norwegian University of Science and Technology.

  http://digitalcorpora.org/corpora/bibliography_files/Mobile%20Memory%20Forensics.pdf, última visita Agosto 2010.

CITAS ELECTRÓNICAS

[1] MELLAR, B, Forensic examination of mobile phones, United Kingdom, 2004, http://faculty.colostatepueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf, última consulta Febrero de 2010.

[3] http://www.revistalideres.ec/2010-10-04/Informe.aspx, última visita Febrero 2010

[7] CANO M, Jeimy J, Introducción a la Informática Forense, Revista Sistemas N° 96, Publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS), http://www.acis.org.co/, última visita Marzo 2010.

[9] BURNETT Robert; SEGERSTAD Ylva Hård af, The SMS Murder Mystery: the dark side of technology, Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities

http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/robert_burnett.pdf, última visita Marzo 2010.

http://en.wikipedia.org/wiki/Knutby_murder, última visita Marzo 2010.

[10] SUMMERS Chris, Mobile phones the new fingerprints, BBC News Online http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk/3303637.stm, última visita Marzo 2010.

[11] SHACHTMAN Noah, Fighting Crime with Cellphones Clues, NY Times, http://www.mobileforensicstraining.com/inthenews_main.html última visita Marzo 2010.

[12] Mobile Phone Analysis – video retrieval, Case Study, http://www.ccl-forensics.com/Case_Studies-27.html?linkto=38. última visita Marzo 2010.

[15] BECERRA RAVASCHIO, Luis; "La experiencia de ANTEL en la problemática del fraude"; http://www.citel.oas.org, última visita Marzo 2010.

[16] PINTO SALOMON, Marcos Vinicius; "Fraude nas Redes de Telefonia Celular"; TELECO; http://www.teleco.com.br, última visita Marzo 2010.

[17] http://www.fcc.gov/cgb/consumerfacts/spanish/CellPhoneFraud.html, última visita Marzo 2010.

ANEXOS

Anexo A	**Formulario de Identificación de Personal**
Anexo B	**Formulario de Identificación y Detección**
Anexo C	**Formulario de Identificación del Dispositivo**
Anexo D	**Formulario de Elementos Incautados**
Anexo E	**Formulario de Cadena de Custodia**
Anexo F	**Formulario de Análisis del Dispositivo**
Anexo G	**Documentación de un Caso**
Anexo H	**Informe de la Herramienta UFED (Universal Forensic Extraction Device)**
Anexo I	**Informe de la Herramienta *Paraben SIM Card Seizure***

ANEXO A

FORMULARIO DE IDENTIFICACIÓN DE PERSONAL

FORMULARIO DE IDENTIFICACIÓN DE PERSONAL		
ROL	**NOMBRE**	**IDENTIFICACIÓN**
Personal de Primera Respuesta		
Investigador		
Examinador Forense		
Custodio de la Evidencia		
Datos y firma del Responsable, quien llenó el formulario		
_____ Firma Responsable:_____ CI: :_____		

ANEXO B

FORMULARIO DE IDENTIFICACIÓN Y DETECCIÓN

FORMULARIO DE IDENTIFICACIÓN Y DETECCIÓN												
Día			**Mes**			**Año**					**Hora**	
Ciudad						**Barrio**						
Dirección						**Teléfono**						
Observación del lugar de los hechos:												
Personas encontradas en el lugar de los Hechos												
Nombres y Apellidos						**Identificación**						
Personal de Primera Respuesta												
Nombres						**Apellidos**						
N° de Identificación												
Entidad												
Cargo												
Firma												

ANEXO C

FORMULARIO DE IDENTIFICACIÓN DEL DISPOSITIVO

FORMULARIO DE IDENTIFICACIÓN DEL DISPOSITIVO													
Caso número:						**Código de Evidencia:**							
Día			**Mes**			**Año**					**Hora:**		
Estado de Conexión													
Estado de conexión	Conectado			Desconectado									
	Observaciones:												
Estado	Encendido			Apagado									
Estado de protección PIN	Activado			Desactivado									
	Observaciones:												
Estado de protección código de seguridad	Activado			Desactivado									
	Observaciones:												
Información General													
Propietario													
Dispositivo aislado	Bolsa/ Contenedor Faraday												
	Bolsa /Contenedor Antiestático												
	Observaciones												
Material Asociado al Teléfono Celular	Cargador												
	Manual												
	Observaciones												
Tarjeta SIM	SI				NO								
Tarjeta de Memoria Extraíble	SI				NO								
Modelo													
Cámara	SI		NO										
Número de serie													
Número ICCID													
Dimensiones													

IMEI	
Número de teléfono (si es conocido)	
Operador de telefónico (si es conocido)	
Observaciones:	
Datos y firma del Responsable, quien llenó el formulario	
_____ Firma Responsable:_____ CI: :_____	

ANEXO D

FORMULARIO DE ELEMENTOS INCAUTADOS

FORMULARIO DE ELEMENTOS INCAUTADOS												
Caso Número :												
Día			**Mes**			**Año**					**Hora**	
Elementos no Incautados												
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**	**Estado**	**Propietario**	**Código de Evidencia**					
Elementos Incautados												
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**	**Estado**	**Propietario**	**Código de Evidencia**					
Productos de la Escena del Hecho												
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**	**Estado**	**Propietario**	**Código de Evidencia**					
Observaciones:												
Datos y firma del Responsable, quien llenó el formulario												
_____ Firma Responsable:_____ CI: :_____												

ANEXO E

FORMULARIO DE CADENA DE CUSTODIA

FORMULARIO DE CADENA DE CUSTODIA														
Caso Número						**Código de Evidencia**								
Día			**Mes**			**Año**					**Hora**			
Fecha (dd/mm/aa)		**Hora**		**Nombre e Identificación de quién recibe la evidencia**		**Propósito del traspaso o Traslado**								**Firma**
Observaciones:														
Observaciones:														
Observaciones:														
Observaciones:														
Observaciones:														

ANEXO F

FORMULARIO DE ANÁLISIS DEL DISPOSITIVO

FORMULARIO DE ANÁLISIS DEL DISPOSITIVO												
Caso Número:					Código de Evidencia:							
Investigador:												
Examinador:												
Descripción del Caso:												
Recepción para el análisis:												
Día			Mes			Año					Hora:	
Análisis:												
Día			Mes			Año					Hora:	
Detalles del Teléfono Celular												
Propietario (si es conocido)												
Condición												
Fabricante												
Modelo												
Serial												
IMEI												
Número de Teléfono												
Operadora												
PIN												
Número de Tarjeta SIM												
IMSI												
Interfaz de Conexión												
Fecha/Hora Dispositivo												
Fecha/Hora Examinador												

Características del Teléfono Celular

☐ *Ringtones* Personalizados	☐ Notas/Memos	☐ SMS	☐ Cap. de Almacenamiento
☐ *Ringtones*	☐ FDN	☐ MMS	☐ Múltiples Lenguajes
☐ Cámara	☐ Agenda Telefónica	☐ EMS	☐ Notas de Voz
☐ Capacidad de Imagenes ID	☐ Registros de llamadas	☐ USB	☐ Bluetooth
☐ Capacidad de Video	☐ LND	☐ Disco Duro	☐ Reenvío de Datos
☐ Voz recoder	☐ Gráficos personalizados	☐ Comandos de Voz	☐ Soporta varios numeros por contacto
☐ Calendario	☐ Tarjeta Externa	☐ GPS	

Particularidades

Teléfono Bloqueado	Soporta Modo de Vuelo	Saludo Inicial	Telefono Encendido	PUK Obtenido
☐ Si	☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No	☐ No
	Esta habilitado?	_____		_____
	Si No	_____		_____
	☐ _____	☐ _____		☐ _____
	_____	_____		_____
	_____	_____		_____
	_____			_____
	_____			

Clave del Dispositivo: _____ Cargador:_____

Cable: _____ Programa: _____

Detalles de la Batería

Fabricante de la Batería: _____

Capacidad de Voltaje de la Batería:_____

Número de Serie Batería:_____

Resultados Voltímetro de la Batería: _____

Batería Removida	Dispositivo Cargado
☐ Si	☐ Si
☐ No	☐ No

Notas:

Características de la Tarjeta SIM		
Información de la Tarjeta SIM:		
Número ICCID en la Tarjeta SIM:	SIM Card Dañada	Si __
Proveedor: Movistar		No: _
Describa el daño: _____ _____		
Errores durante la adquisición: _____ _____		
Datos Básicos:		

IMSI	ICCID	MSISDN	SPN
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

SDN	EXT3	ADN	LDN
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

EXT1	FDN	EXT2	SMS
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

Información de Localización		
LOCI	LOCIGPRS	FPLMN
☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A

Observaciones y Conclusiones:

ANEXO G

DOCUMENTACIÓN DE UN CASO

COLECTA Y ANÁLISIS DE EVIDENCIA DIGITAL

ÍNDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

COLECTA Y ANÁLISIS DE EVIDENCIA DIGITAL

A. DEFINICIÓN DEL CASO

El escenario de prueba con el cual será ejemplificado el procedimiento de operaciones propuesto en el capítulo 4, se basa en la experiencia de los Investigadores y documentos que se tuvo acceso del Departamento de Investigación y Análisis Forense de la Fiscalía con los cuales tuvimos el placer de compartir 6 meses.

El análisis empieza con asumir que ya se cumplió con el aviso al Fiscal de que se ha llevado a cabo un delito de Acoso, por cualquiera de los medios posibles, ya sea de oficio, por un informe de policía ante una situación de flagrancia, por una denuncia penal o por una comunicación de otra autoridad o entidad del estado u órgano de control.

Además, se asume que ya se ha cumplido con todos los requisitos legales (órdenes de incautación, orden de allanamiento) emitidas por los jueces pertinentes, los documentos antes mencionados no pueden ser publicados en este anexo ya que son elementos confidenciales dentro de una investigación.

A continuación se presenta la explicación de las Etapas propuestas conjuntamente con los formularios.

B. COLECTA

I. Identificación

1. Roles y funciones

Para el desarrollo de la presente investigación se realizará la asignación de roles según lo mencionado en la sección 4.2.3.1 y llenando el correspondiente Formulario que se muestra a continuación; sin embargo al no poder publicar los nombres de los investigadores forenses, la totalidad de los roles serán asignados a nombres ficticios.

FORMULARIO DE IDENTIFICACIÓN DE PERSONAL		
ROL	**NOMBRE**	**IDENTIFICACIÓN**
Personal de Primera Respuesta	Alexander Maleza	1718971456
Investigador	Karina Sandoval	1720932563
Examinador Forense	Jorge Peñaherrera	1760517456
Custodio de la Evidencia	Augusto Becerra	1720841458
Datos y firma del Responsable, quien llenó el formulario		
_____ Firma Responsable:_____ CI: :_____		

Tabla G.1: Formulario de Identificación de Personal

2. Detección de Evidencia

A continuación se muestra la documentación del lugar de los hechos según y el estado general de la escena del crimen, según lo propuesto en la sección 4.2.3.1, llenando el Formulario de Identificación y detección; los datos llenados corresponden a un lugar ficticio puesto que no se pueden colocar las direcciones verdaderas del caso en investigación.

FORMULARIO DE IDENTIFICACIÓN Y DETECCIÓN												
Día	1	6	Mes	0	5	**Año**	2	0	1	1	Hora	21:30
Ciudad	Quito					**Barrio**	La Vicentina					
Dirección	Oleas E13-174 e Hidalgo					**Teléfono**	095971581					

Observación del lugar de los hechos: Lugar de aproximadamente de 120m^2, presenta un cuarto principal, un baño, sala, comedor y cocina. Se encontraron dispositivos electrónicos de interés como una *Laptop HP Pavilon* dv-4000 (encendida), un teléfono celular *Nokia Xpress Music* (en aparente funcionamiento) de la operadora Movistar. Se adjunta bosquejo tomado en la escena del hecho en donde se identifica el lugar en el cual fueron encontrados los dispositivos electrónicos.

Personas encontradas en el lugar de los Hechos	
Nombres y Apellidos	**Identificación**
Daniel Peñaherrera	1801258963

Personal de Primera Respuesta			
Nombres	Alexander	**Apellidos**	Maleza
N° de Identificación	1718971456		
Entidad	Fiscalía		
Cargo	Investigador del Departamento de Investigación y Análisis Forense		
Firma			

Tabla G.2: Formulario de Identificación y Detección

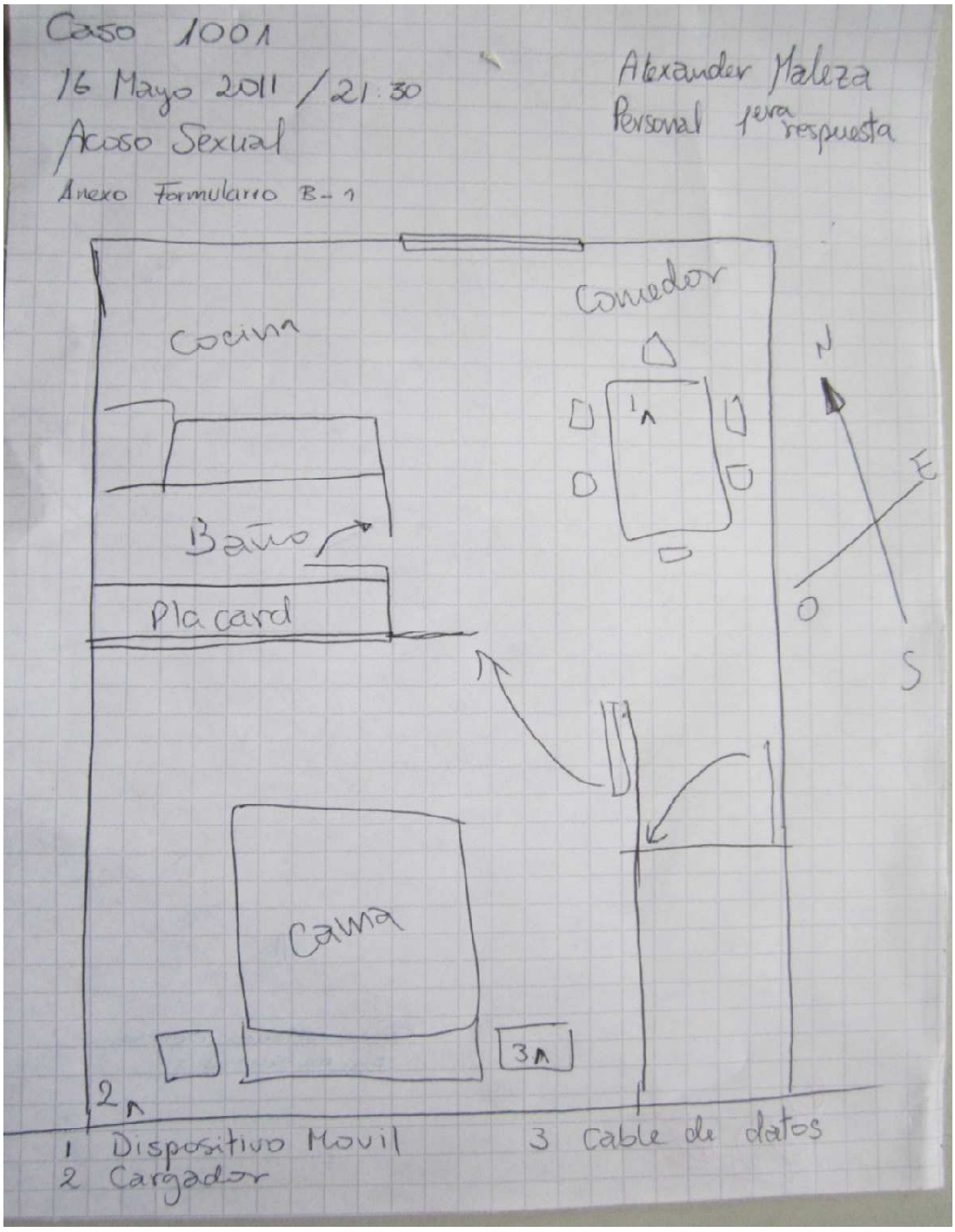


Figura G.1: Bosquejo de la Escena del Hecho (del Personal de Primera Respuesta)

3. Documentación relacionada con el dispositivo

En la escena del hecho se encontró un teléfono celular y cumpliendo con la sección 4.2.3.1 se procede a llenar el Formulario de Identificación del Dispositivo.

FORMULARIO DE IDENTIFICACIÓN DEL DISPOSITIVO, PRIMERA PARTE												
Caso número:			1001			**Código de Evidencia:**					1001-1	
Día	1	6	**Mes**	0	5	**Año**	2	0	1	1	**Hora:**	21:50
Estado de Conexión												
Estado de conexión						Conectado		-			Desconectado	X
						Descripción: Teléfono celular Nokia 5130c *Xpress Music* desconectado, en propiedad del sospechoso Daniel Peñaherrera.						
Estado						Encendido		X			Apagado	-
Estado de protección PIN						Activado		-			Desactivado	X
						Observaciones:						
Estado de protección código de seguridad						Activado		-			Desactivado	X
						Observaciones:						
Información General												
Propietario						Daniel Peñaherrera						
Dispositivo aislado						Bolsa/ Contenedor Faraday		-				
						Bolsa /Contenedor Antiestático		-				
						Observaciones		Debido a la premura del operativo, se procedió a incautar el dispositivo y aislarlo en una bolsa de Faraday casera hecha con papel aluminio.				
Material Asociado al Teléfono Celular						Cargador		X				
						Manual		-				

FORMULARIO DE IDENTIFICACIÓN DEL DISPOSITIVO, SEGUNDA PARTE						
	Observaciones			-		
Tarjeta SIM	SI			X	NO	-
Tarjeta de Memoria Extraíble	SI			X	NO	-
Modelo	Nokia *Xpress Music*					
Cámara	SI	X	NO	-	Descripción: Teléfono de colores rojo y negro, cámara de 2 MP.	
Número de serie	N/A, estaba encendido el dispositivo.					
Número ICCID	N/A, estaba encendido el dispositivo.					
Dimensiones	10 x 4 cm					
IMEI	352717049930525					
Número de teléfono (si es conocido)	N/A					
Operador de telefónico (si es conocido)	Movistar, por logo visible.					
Observaciones:						
El dispositivo se encuentra con la carga de la batería a la mitad, aparentemente en buenas condiciones, posee un bloqueo automático sin seguridad.						
Datos y firma del Responsable, quien llenó el formulario						
_____ Firma Responsable:_____ CI: :_____						

Tabla G.3: Formulario de Identificación del Dispositivo

4. Documentación de los elementos incautados

A continuación se muestra la información correspondiente a los dispositivos incautados en la escena del hecho, cumpliendo con lo dispuesto en la sección 4.3.2.1 numeral 4, y llenando el Formulario de Elementos Incautados como se muestra a continuación.

FORMULARIO DE ELEMENTOS INCAUTADOS, PRIMERA PARTE												
Caso Número : 1001												
Día	1	6	Mes	0	5	Año	2	0	1	1	Hora	22:30
Elementos no Incautados												
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**		**Estado**		**Propietario**				**Código de Evidencia**
N/A												
Elementos Incautados												
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**		**Estado**		**Propietario**				**Código de Evidencia**
Teléfono Celular	Nokia	Xpress Music	N/A	Celular encendido, aparente buen estado, con la batería del dispositivo a la mitad. Color rojo y negro.		Encendido		Daniel Peñaherrera				1001-1
FORMULARIO DE ELEMENTOS INCAUTADOS, SEGUNDA PARTE												
Cable De Datos	Nokia	N/A	0730368946	Aparente buen estado		N/A		Daniel Peñaherrera				1001-2

Cargador	Nokia	N/A		Aparente buen estado	N/A	Daniel Peñaherre-ra	1001-3
Productos de la Escena del Hecho							
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**	**Estado**	**Propietario**	**Código de Eviden-cia**
DVD-R	Maxell	N/A	N/A	DVD-R que almacena videos e imágenes de la escena del hecho.	N/A	Fiscalía	1001-4
Observaciones: N/A							
Datos y firma del Responsable, quien llenó el formulario							
_____ Firma Responsable:_____ CI: :_____							

Tabla G.4: Formulario de Elementos Incautados

II. Preservación

1. Creación del registro de cadena de custodia

A continuación se muestra el registro de cadena cumpliendo con lo propuesto en la sección 4.2.3.2

CADENA DE CUSTODIA, PRIMERA PARTE												
Caso Número			1001			**Código de Evidencia**					1001-1, 1001-2, 1001-3, 1001-4	
Día	1	6	**Mes**	0	5	**Año**	2	0	1	1	**Hora:** 23:00	
Fecha (dd/mm/aa)		**Hora**		**Nombre e Identificación de quién recibe la evidencia**		**Propósito del traspaso o Traslado**						**Firma**
16/05/2011		23:00		Karina Sandoval 1720932563		Transporte de la evidencia a las instalaciones de la Fiscalía.						
Observaciones: He recibido del señor Alexander Maleza, personal de primera respuesta, un teléfono celular envuelto en una bolsa de papel aluminio, un cable de datos, un cargador y un CD con información obtenida de la escena del hecho.												
16/05/2011		23:15		Augusto Becerra 1748567890		Guardar la evidencia incautada en el Departamento de Investigación y Análisis Forense de la Fiscalía.						
Observaciones: He recibido de la señorita Karina Sandoval, investigador, un teléfono celular envuelto en una bolsa de papel aluminio, un cable de datos, un cargador y un CD con información obtenida de la escena del hecho. Se procederá a cargar el dispositivo móvil en un lugar aislado de señales de radiofrecuencia.												
17/05/2011		08:15		Karina Sandoval 1720932563		Recoger la evidencia, para entregárselo al examinador forense a cargo.						
Observaciones: He recibido del señor Augusto Becerra, custodio, un teléfono celular cargado completamente y dentro de una bolsa que evita las señales de radiofrecuencia, además un cable de datos, un cargador y un CD con información obtenida de la escena del hecho												

CADENA DE CUSTODIA, SEGUNDA PARTE				
17/05/2011	10:00	Jorge Peñaherrera 1760517456	Procederá a analizar la evidencia, con la petición respectiva del investigador del caso Karina Sandoval	
Observaciones: He recibido de la señorita Karina Sandoval, investigador del caso, un teléfono				

celular cargado completamente y dentro de una bolsa que evita las señales de radiofrecuencia, además un cable de datos, un cargador y un CD con información obtenida de la escena del hecho. Se analizará la información contenida en el teléfono celular por medio de herramientas forenses.				
17/05/2011	17:00	Karina Sandoval 1720932563	Entrega de la evidencia con resultado del análisis	
Observaciones: He recibido del señor Jorge Peñaherrera, un teléfono celular cargado completamente y dentro de una bolsa que evita las señales de radiofrecuencia, además un cable de datos, un cargador y un CD con información obtenida de la escena del hecho y el formulario de análisis del dispositivo..				

Tabla G.5: Cadena de Custodia de los elementos electrónicos incautados

CADENA DE CUSTODIA, PRIMERA PARTE												
Caso Número			1001			**Código de Evidencia**					A-1, B-1, C-1, D-1,E-1 E-2	
Día	1	6	**Mes**	0	5	**Año**	2	0	1	1	**Hora:** 23:00	
Fecha (dd/mm/aa)		**Hora**		**Nombre e Identificación de quién recibe la evidencia**		**Propósito del traspaso o Traslado**						**Firma**
16/05/2011		23:00		Karina Sandoval 1720932563		Transporte de los formularios a las instalaciones de la fiscalía.						
Observaciones: He recibido los formularios respectivos de la investigación del señor Alexander Maleza, personal de primera respuesta, junto con un bosquejo de la escena del hecho.												

CADENA DE CUSTODIA, SEGUNDA PARTE				
16/05/2011	23:15	Augusto Becerra 1748567890	Guardar los formularios en el Departamento de Investigación y Análisis Forense de la Fiscalía.	
Observaciones: He recibido los formularios respectivos de la señorita Karina Sandoval, Investigador.				

17/05/2011	08:15	Karina Sandoval 1720932563	Recoger los formularios para entregárselos al examinador forense a cargo.	
Observaciones: He recibido los formularios respectivos de la investigación del señor Augusto Becerra, custodio.				
17/05/2011	10:00	Jorge Peñaherrera 1760517456	Proceder analizar el dispositivo móvil, con la petición respectiva del investigador del caso Karina Sandoval	
Observaciones: He recibido los formularios respectivos de la señorita Karina Sandoval, investigador.				
17/05/2011	17:00	Karina Sandoval 1720932563	Entrega de formularios de la investigación realizada.	
Observaciones: He recibido los formularios respectivos de la investigación del señor Jorge Peñaherrera, examinador forense del caso.				

Tabla G.6: Cadena de Custodia de los formularios producidos de la escena del hecho

2. Aseguramiento de la evidencia electrónica

Aislamiento del dispositivo:

El dispositivo vulnerado fue aislado de la red GSM introduciéndolo en una bolsa de papel aluminio, la cual fue anteriormente probada con varios modelos de teléfonos celulares, lo cual se muestra en la Figura G.2.

Figura G.2: Aislamiento del dispositivo de señales de Radiofrecuencia

Aseguramiento de la evidencia física

La totalidad de la evidencia incautada fue etiquetada y almacenada en bolsas transparentes, las cuales solo los investigadores pueden tener acceso luego de realizar el debido trámite de registro de cadena de custodia, como muestra en la Figura G.3.

Figura G.3: Etiquetas y Almacenamiento de la Evidencia

C. ANÁLISIS

I. Evaluación

1. Documentación e Identificación del Dispositivo

Cumpliendo con la sección 4.2.4.1 se recepta los elementos incautados y formularios, con el fin de obtener un conocimiento general de la escena del hecho.

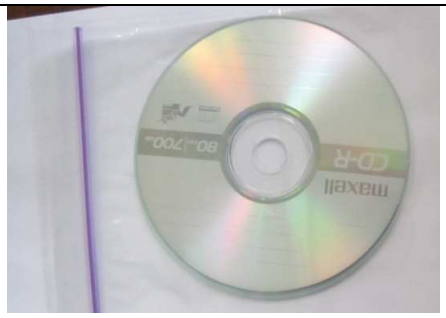
Fotografías	Descripción
	Dispositivo Móvil, encontrado en el comedor de la casa (escena del hecho)
	Cable de Datos, ubicado en una cómoda, alado de la cama del cuarto principal de la casa (escena del hecho)
	Cargador del dispositivo móvil, encontrado en un toma corriente de una pared del cuarto principal (escena del hecho)
	DVD-R, dispositivo que almacena las fotografías y videos obtenidos en la escena del hecho.

Tabla G.7: Elementos Incautados de la Escena del Hecho

Figura G.4: Elementos Incautados de la Escena del Hecho etiquetados como evidencia

2. Aislamiento de señales de radiofrecuencia

El dispositivo es recibido dentro de una bolsa de papel aluminio, con la carga del celular completa como se muestra en la Figura G.5.

Figura G.5: Teléfono celular aislado de señales de radiofrecuencia

II. Extracción

1. Elección de herramienta(s) forense(s)

Para la investigación judicial en curso, fue necesario realizar un *Toolkit* Forense compuesto por varias herramientas de hardware y software provenientes de distintos fabricantes, cumpliendo con la sección 4.2.4.2, en base a pruebas previamente realizadas sobre teléfonos celulares de la misma marca y modelo del celular que es objeto de estudio en la investigación; tomando la decisión de usar las herramientas UFED para el equipo móvil y *Paraben* SIM *Card Seizure* para la tarjeta SIM.

2. Proceso de Extracción

Cumpliendo con la sección 4.2.4.2 se procede al llenar el Formulario de Análisis del dispositivo.

FORMULARIO DE ANÁLISIS DEL DISPOSITIVO												
Caso Número:	1001-1					Código de Evidencia:					1001-1	
Investigador: Karina Sandoval												
Examinador: Jorge Peñaherrera												
Descripción del Caso:												
Recepción para el análisis:												
Día	1	7	Mes	0	5	Año	2	0	1	1	Hora:	
Análisis:												
Día	1	7	Mes	0	5	Año	2	0	1	1	Hora:	
Detalles del Teléfono Celular												
Propietario (si es conocido)						Daniel Peñaherrera						
Condición						Dispositivo encendido						
Fabricante						Nokia						
Modelo						5130c *Xpress Music*						
Serial						0581269BR06GH						
IMEI						352717049930525						
Número de Teléfono						084139408						
Operadora						Movistar						
PIN						12345						
Número de Tarjeta SIM						8959300500625551713						

IMSI	740000107574346
Interfaz de Conexión	Lector propietario
Fecha/Hora Dispositivo	17/05/2011 14:20
Fecha/Hora Examinador	17/05/2011 14:20

Características del Teléfono Celular

☐ *Ringtones* Personalizados	☐ Notas/Memos	☐ SMS	☐ Cap. de Almacenamiento
☐ *Ringtones*	☐ FDN	☐ MMS	☐ Múltiples Lenguajes
☐ Cámara	☐ Agenda Telefónica	☐ EMS	☐ Notas de Voz
☐ Capacidad de Imagenes ID	☐ Registros de llamadas	☐ USB	☐ Bluetooth
☐ Capacidad de Video	☐ LND	☐ Disco Duro	☐ Reenvío de Datos
☐ Voz recoder	☐ Gráficos personalizados	☐ Comandos de Voz	☐ Soporta varios numeros por contacto
☐ Calendario	☐ Tarjeta Externa	☐ GPS	

Particularidades

Teléfono Bloqueado	Soporta Modo de Vuelo	Saludo Inicial	Telefono Encendido	PUK Obtenido
☐ Si	☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No	☐ No
	Esta habilitado? Si No			
	☐ _____	☐ _____		☐ _____

Clave del Dispositivo: 12345 Cargador: Nokia

Cable: USB Programa: UFED

Detalles de la Batería

Fabricante de la Batería: Nokia

Capacidad de Voltaje de la Batería: 3.7 V

Número de Serie Batería: 0670398462040

Batería Removida	Dispositivo Cargado
☐ Si	☐ Si
☐ No	☐ No

Resultados Voltímetro de la Batería: 3.6 V

Notas:

Características de la Tarjeta SIM

Información de la Tarjeta SIM:

Número ICCID en la Tarjeta SIM: 8959300500625551713	SIM Card Dañada	Si __
Proveedor: Movistar		No: X

Describa el daño:

N/A

Errores durante la adquisición:

Datos Básicos:

IMSI	ICCID	MSISDN	SPN
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

SDN	EXT3	ADN	LDN
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

EXT1	FDN	EXT2	SMS
☐ Si	☐ Si	☐ Si	☐ Si
☐ No	☐ No	☐ No	☐ No
☐ N/A	☐ N/A	☐ N/A	☐ N/A

Información de Localización

LOCI ☐ Si ☐ No ☐ N/A	LOCIGPRS ☐ Si ☐ No ☐ N/A	FPLMN ☐ Si ☐ No ☐ N/A
Observaciones y Conclusiones:		
Las herramientas muestran a través de los mensajes de texto (almacenados, borrados, enviados y transmitidos) tanto del dispositivo móvil como en la tarjeta SIM, información relevante para el caso. Mostrando frecuencia en las comunicaciones entre la parte acusadora y el acusado. Como Investigador del Caso 1001, y observando los datos obtenidos en la investigación por el examinador, se puede observar mensajes de la parte acusadora al implicado y viceversa, con carácter amoroso, dando a pensar una aparente relación.		

Tabla G.8: Formulario de Análisis del Dispositivo

3. *Preservar la integridad de la evidencia digital*

Como se muestra en la Figura G.6 se obtiene los valores Hash de la información almacena en el teléfono celular.

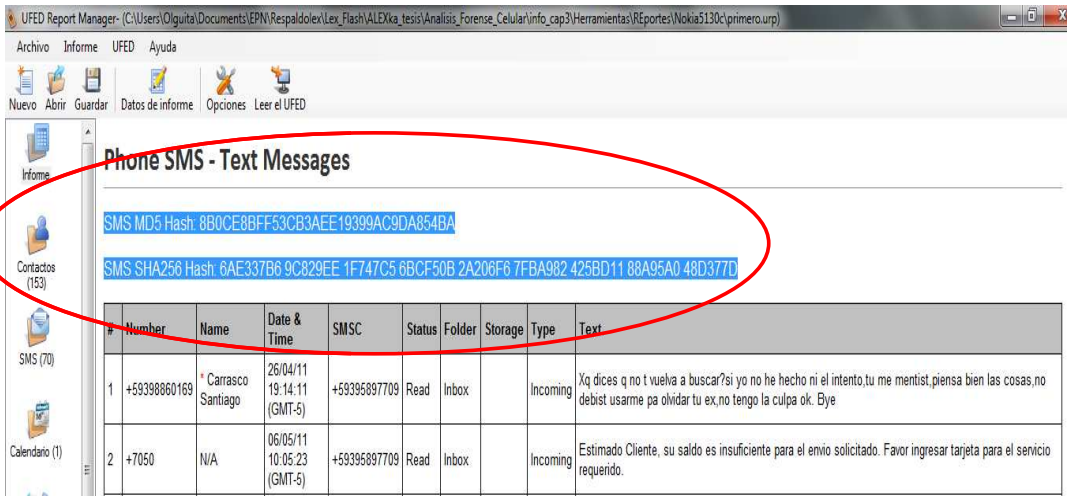


Figura G.6: Valores *Hash* calculados del Equipo Móvil por la Herramienta UFED

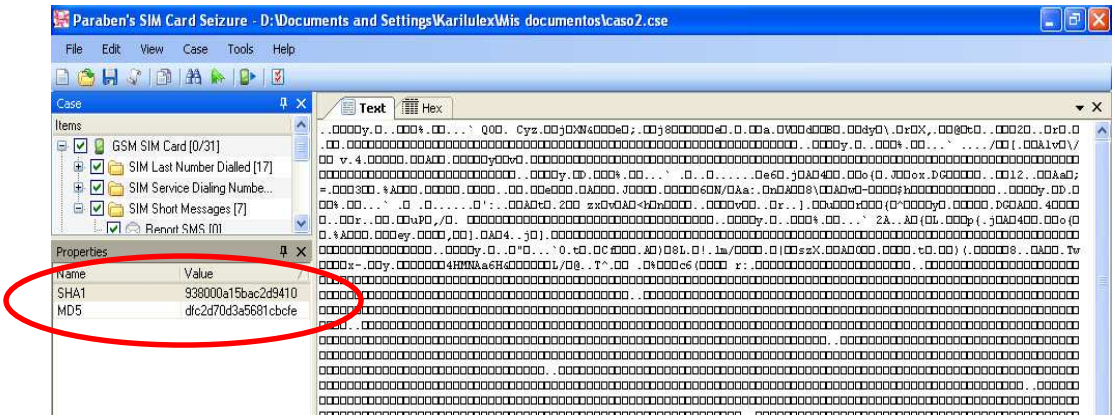


Figura G.7: Valores *Hash* calculados por la Herramienta Pareben SIM Card Seizure

III. Filtrado

1. *Fase de Filtrado de Evidencia Digital*

Respecto al caso se deduce que los elementos de interés son los mensajes de texto y llamada realizadas y recibidas, puesto que el celular no tiene imágenes.

IV. Presentación

1. *Fase de Presentación de Evidencia Digital*

Para el desarrollo de la presente investigación, la totalidad de reportes fueron creados manualmente por el personal de Primera Respuesta y digitalizados por los Examinadores Forenses. A continuación se muestra el listado de los reportes realizados, los cuales serán entregados al Fiscal, conjuntamente con las conclusiones del Investigador.

- Formulario de identificación de personal.
- Formulario de identificación y detección de la escena del hecho.
- Formulario de Identificación del Dispositivo.
- Formulario de Elementos Incautados.
- Cadena de Custodia.

- Formulario de Análisis del dispositivo.
- Conclusiones de la investigación (Dentro del Formulario de Análisis del Dispositivo).

D. INFORMES DE LAS HERRAMIENTAS FORENSES UTILIZADAS

Revisar anexos H e I.

ANEXO H

INFORME DE LA HERRAMIENTA UFED

(*UNIVERSAL FORENSIC EXTRACTION DEVICE*)

Phone Examination Report Properties

Selected Manufacturer:	Nokia GSM
Selected Model:	Nokia 5130c XpressMusic
Detected Manufacturer:	Nokia
Detected Model:	Nokia 5130c-2
Revision:	V 07.91 29-10-09 RM-495 (c) Nokia
IMEI:	352717049930525
IMSI:	740000107574346
User Code:	12345
Extraction start date/time:	17/05/11 14:07:37
Extraction end date/time:	17/05/11 14:09:20
Phone Date/Time:	17/05/11 14:07:20
Connection Type:	USB Cable
UFED Version:	Software: 1.1.7.0 UFED , Full Image: 1.0.2.4 , Tiny Image: 1.0.2.1
UFED S/N:	5571002

Phone Examination Report Index

Contacts	Selected
SMS - Text Messages	Selected
Calendar/Notes/Tasks	Selected
Call Logs	Selected
Images	Selected
Ringtones	Selected
Audio	Not Selected
Video	Selected

Phone Incoming Calls List

CLOG MD5 Hash: DC1426A7D0E5126994B76915170633DB

CLOG SHA256 Hash: 19A2580E 94ADD27 DE475C4 9177777 7DAF951 787F7BA 1324BB3 05E115E 21A96FB

#	Type	Number	Name	Date & Time	Duration

Incoming Calls Information Not Available

Phone Outgoing Calls List

CLOG MD5 Hash: DC1426A7D0E5126994B76915170633DB

CLOG SHA256 Hash: 19A2580E 94ADD27 DE475C4 9177777 7DAF951 787F7BA 1324BB3 05E115E 21A96FB

#	Type	Number	Name	Date & Time	Duration
1	Outgoing	095038914	Carlos Ramos	17/04/11 10:19:07	0:00:07
2	Outgoing	084971546	Amoshy	17/04/11 10:18:37	N/A
3	Outgoing	098399845	Dianita F	17/05/11 10:17:39	N/A

Phone Missed Calls List

CLOG MD5 Hash: DC1426A7D0E5126994B76915170633DB

CLOG SHA256 Hash: 19A2580E 94ADD27 DE475C4 9177777 7DAF951 787F7BA 1324BB3 05E115E 21A96FB

#	Type	Number	Name	Date & Time	Duration

Missed Calls Information Not Available

* Phonebook name lookup used to retrieve names

Phone SMS - Text Messages

SMS MD5 Hash: 6CBD87598ABB9C2D48B4AE2ECC344A28

SMS SHA256 Hash: 9EBA5D7F C410F62 004BAF6 D9ACF4A C4868E8 36E3AAC 8FACA3D 12728A6 ADC8DCC

#	Number	Name	Date & Time	SMSC	Status	Folder	Storage	Type	Text
1		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Blanco cédula
2		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Si lees st mnsaj: ¡T BESO! Si m rsponds: ¡T BESO! Si lo borras: ¡T BESO! Si lo guardas tambien: ¡T BESO! No se, ¿Q s lo q vas hacer? Pero.. D q t beso, ¡T BESO! Y... no t rias x q tambien.. ¡T BESO! Dulces sueños amor t amo muchísimo..

3		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Hay 2 tipos d prsonas: 1. Las lindas x dntro 2. Las lindas x fuera .....GRACIAS X SER REVRSIBLE!... un abrazo tqm lindo dia..
4	0849715 46	N/A	N/A		Delete	Drafts	Phone	Outgoing	Se feliz x dspertar cada nañana...x percibir el aroma d las flores.....x cumplir 1 dia + d vida...x tener el amor + bello y valioso... el d Dios... Linda noche
5		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Dicen q el cielo s como l cariño, un lugar infinito, hermoso y sin maldad, gracias x ser ese pedacito d cielo y compartirlo conmigo TQM... linda noche..
6		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Www.pee.UFRJ.BR/info
7		N/A	N/A		Unsent	Drafts	Phone	Outgoing	Bolivar Ledesma
8		N/A	N/A		Unsent	Drafts	Phone	Outgoing	26v2t0d45
9		N/A	N/A		Unsent	Drafts	Phone	Outgoing	No kiero sr pa ti1#+n tu lista d contactos o 1 mensj n tu buzon d entrada mucho menos una simpl llamada Kiero sr la prsona q sin sr la q+kiers s la q+t aprecia, t considera y t desea lo mejor Y aunq a vecs no stmos cerk recuerda q cuents conmigo 100pr... Un besito y linda noche...

10	+59399013968	N/A	14/09/10 12:01:30	+593958977709	Read	Inbox	Phone	Incoming	Repite en voz alta: Soy lo que DIOS dice que soy, tengo lo que DIOS dice que tengo, y puedo hacer lo que DIOS dice que puedo hacer, xq la gracia de DIOS carta en mi vida. Con cariño. Martha
11	+59398544605	N/A	30/08/10 16:06:45	+593958977709	Read	Inbox	Phone	Incoming	1 AMIGO s la part q complementa el alma, t apoya, t diviert, t recuerda y 1 dia como hoy sin motivo alguno t scrib pa decirt q eres muy important.... li
12	+59384970090	N/A	29/08/10 20:05:15	+593958977709	Read	Inbox	Phone	Incoming	Tngo k reconocer (",,(")k n l mundo ("('0',),hay gente (")(")(,) linda, buena, inteligente, dulc pero sabs tu exageras xq ers GENIAL tqm. Linda noch...
13	+59384971546	N/A	05/09/10 11:19:21	+593958977709	Read	Inbox	Phone	Incoming	Buenos dias amor solo te llamaba para decirte que te amo y deseo que nuestro amor siga creciendo cada dia feliz mesario....
14		N/A	N/A		Unsent	Drafts	Phone	Outgoing	1st71p65 isaías 54 4 10
15	+59383039551	N/A	14/04/11 20:35:41	+593958977709	Read	Inbox	Phone	Incoming	Te mando una almohadita de sueños lindos, una colchita llena de cariño para q' te abrigue y este (',,(') osito pa ('o') q te cuide (,,)(,,) linda noche!

16	+59399013968	N/A	28/07/10 21:03:33	+593958977709	Read	Inbox	Phone	Incoming	El que habita al abrigo bel Altísimo mora bajo la sombra del Omnipotente. Por eso DIOS cuida de ti porque te ama con amor eterno. Bendiciones:-)
17	098157586	N/A	08/05/11 20:50:13	+593958977705	Sent	Sent	Phone	Outgoing	Mami x cierto alex le mandó un saludo x el día d la madre.. Una buena noche y Dios le bendiga..
18	084971546	N/A	N/A	+593958977705	Delete	Sent	Phone	Outgoing	Ya llegué a la casa corazón.. Te amo muchísimo..
19	084794625	N/A	07/05/11 11:08:10	+593958977705	Sent	Sent	Phone	Outgoing	Contabilidad general, 5ta edición Mc Graw Hill interamericana, pedro zapata sánchez, Colombia 2005 Contabilidad general, teoría y práctica aplicada a la legislación nacional, Dr josé orozco cadena, oct 1997, Ecu Conta gene.. 4ta edición, rubén sarmiento, públingraf, sep 1999, sep

* Phonebook name lookup used to retrieve names

ANEXO I

INFORME DE LA HERRAMIENTA *PARABEN SIM CARD SEIZURE*

Case Information

Name	Value
Case Number:	1001-1
Property/Evidence Number:	Daniel Peñaherrera
Device Info:	
Company/Agency:	Fiscalia
Examiner:	Jorge Peñaherrera
Address1:	Fiscalia
Address2:	
City:	Quito
State:	Pichincha
Zip:	
Country:	Ecuador
Phone:	
Fax:	
E-mail:	a.maleza@ieee.org
Notes:	Caso 1001 evidencia 1001-1 (Acoso)

GSM SIM Card

Properties

Name	Value
Program timestamp	17/05/2011 10:37:26
Manufacturer	GSM
Model	GSM SIM card
Phone name	Not avail
Phone number	Not avail
Service provider name	movistar

SIM Last Number Dialled

SIM Last Number Dialled

Record number	Name	Phone	EXT1 Record number
1		*82	
2		098157586	
3		098157586	
4		084450804	
5		083039551	
6		084971546	
7		098841576	
8		098399845	
9		+59384462150	
10		099057967	

SIM Last Number Dialled (EXT1)

EXT1 Record number	Additional phone number
1	
2	8000
3	301975

4	
5	11111111111111111111

SIM Service Dialing Numbers

SIM Short Messages

Report SMS

Record number	Service Center	Recipient Address	Service center time stamp	Discharge time	User data

Submit SMS

Record number	Status	Service Center	Destination Address	Validation period	Text	Formatted Text	Reply Path	Status Report Request	Message Reference	Protocol Identifier	Coding Scheme	Is Completed

Deliver SMS

Record number	Status	Service Center	Originating Address	Service center time stamp	Text	Formatted Text	Reply Path	Status Report Request	Protocol Identifier	Coding Scheme	Is Completed
01, 02	Read	+5939589 7709	+5939839 9845	2011-04-26 08:03:24 GMT-5	uN AMIGo eS lA pArTe Q cOmPlEm EnTa l aLmA: T aPoyA T diViErT T rE KueRDa Y uN DiA SiN mOtiVo aLgU nO T eSCRiBe pArA dECiRtE Q tEnG aS uN LiNdO Dia... Tkm gRaCiAs x T u AmIsTaD mi KarY.. ^^	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
03, 04	Read	+5939589 7709	+5939977 7460	2011-04-26 08:37:28 GMT-5	Gracias mi corazon siempre llegas con tu mensaje oportuno , es que DIOS te usa para bendecirme , mi preciosa cuidate y que PAPITO del cielo te siga guardando y bendiciendo ; yo también TQM. Y Te bendigo con toda clace de bendiciones y do el Nombre del SEÑOR JESU CRISTO ¡ AMÉN ! .	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
05	Read	+5939589 7709	+5938479 4625	2011-04-02 14:47:57 GMT-5	El numero 59384794625 ha solicitado que lo llame.	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
06, 07	Read	+5939589 7709	+5938303 9551	2011-03-02 20:56:05 GMT-5	Miré al cielo y le pregunté a Dios: como es q crea persons specials? Y me respondio: No son persons son mis mejores angeles q stan d gira x l tierr n una mision...¡cuidarte en tus moments mas dificiles:-)tqm	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
08	Read	+5939589 770	+5938497 1546	2011-03-02 21:4	Buenas noches amor q descanses dulces sueños t amo mucho mucho hasta mañana	Data >>	Is not set	Is not requested	SME to SME prot	GSM	yes

		9		1:07 GMT-5					ocol		
09	Read	+5939589 7709	+5938497 1546	2011-03-03 20:28:55 GMT-5	Buenas noches amor yo estoy bien y a ti q tal t fue? q descanses dulces sueños mi angelita preciosa	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
11, 19	Read	+5939589 7709	+5939815 7586	2011-03-01 15:47:22 GMT-5	Que hoy sientas que primero esta el amor fiel eterno de Dios en tu corazon y que bendiga al niñ@ dentro de ti, y q siempre oro para q lo creas feliz dia niñ@. Bendiciones	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
12, 17	Read	+5939589 7709	+5938497 1546	2011-04-27 07:04:04 GMT-5	Buenos dias amor me gusta saber q sientes lo mismo q yo pues m encanta estar a tu lado besart saber con un beso lo mucho q m amas buen dia y buen viaje preciosa	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
14, 21	Read	+5939589 7709	+5939901 3968	2011-04-19 12:33:10 GMT-5	Dios esta delante d ti él sera tu guia Dios esta detras d ti, ningun mal podra aquejarte Dios esta junto a ti para reconfortarte y animarte. DTA con amor eterno B-) Gozate en Jehova tu creador. Martha	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes

Deliver SMS (deleted)

Record number	Status	Service Center	Originating Address	Service center time stamp	Text	Formatted Text	Reply Path	Status Report Request	Protocol Identifier	Coding Scheme	Is Completed
10, 18	Free space	+5939589 7709	+5939854 4605	2011-04-27 15:03:25 GMT-5	Anda a mi casa ya... Ahi nos vemos a las 4 si? O donde prefieres tu? Yo estoy ahorita en el recorrido y me demoro una hora hasta mi casa... Quiero dejar - mi maleta por eso digo ahi, sino usted que prefiere chikita?	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
13, 15, 16	Free space	+5939589 7709	+5938303 9551	2011-04-26 11:23:46 GMT-5	Una persona q t kiere no t promete un futuro,t regala un present.. No reprocha tus faltas,solo las olvida.. No recuerda un pasado,solo vive un present.. No t promet una vida,sino q pide a Dios x ti .. No t regala un sol,t regala una speranza..Nunk t exige nada spera x ti con paciencia..No solo se alegra x ti goza contigo.. No t señala el camino a seguir t guia y anda cntigo x el.. Kien t kiere Nunk se cansa d ti disfruta siempr d tu compañia.. Lindo dia	Data >>	Is not set	Is not requested	SME to SME protocol	GSM	yes
20	F	+5	+5	201	De 16h15 a 16h30 en el Quicentro chikita...	Da	Is	Is n	SM	GS	ye

	re s pa ce	939 589 770 9	939 854 460 5	1-04-27 15 :19: 52 G MT-5		ta > >	no t s et	ot r eque sted	E to SME prot ocol	M	s
22	F re s pa ce	+5 939 589 770 9	+5 939 854 460 5	201 1-04-27 16 :29: 48 G MT-5	Chikita ya te estoy esperando de repente...	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
24	F re s pa ce	+5 939 589 770 9	+5 938 497 154 6	201 1-04-18 21 :47: 58 G MT-5	Buenas noches amor q descanses dulces sueños pre ciosa hasta mañana no trabajara mucho te amo muc hisimo	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
25	F re s pa ce	+5 939 589 770 9	+0 052 044 127 74	201 1-04-04 10 :48: 34 G MT-5	Movistar te informa que tienes 1 llamada perdida: 04/06, del 05204412774 a las 10:48	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
26	F re s pa ce	+5 939 589 770 9	+5 938 497 154 6	201 1-03-04 23 :57: 50 G MT-5	Feliz mesario amor q tengas dulces sueños recuerd a q t amo mucho q descanses y yo tambien anhelo e star hasta viejito contigo	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
27	F re s pa ce	+5 939 589 770 9	+2 270	201 1-03-10 13 :25: 55 G MT-5	Pepe25, Dani18 y Pao326 estan cerca de ti y quiere n conocerte!!Marca gratis *110# y podras hablar co n ellos. Primer dia GRATIS. Marca YA!	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
28	F re s pa ce	+5 939 589 770 9	+5 938 303 955 1	201 1-04-08 12 :47: 56 G MT-5	Hola niños como estan!! Hoy les esperamos en la e ntrega del alelmo... A las 5 y media de la tarde	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
29	F re s pa ce	+5 939 589 770 9	+7 329	201 1-04-25 08 :07: 28 G MT-5	Tu tambien puedes respaldar tus SMS asi como lo hace el 084104309. Solo responde OK a este SMS y listo. USD 0.99+IVA al mes. Mas info *001	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
30	F	+5	+5	201	El numero 59384971546 ha solicitado que lo llame	Da	Is	Is n	SM	GS	ye

	re s pa ce	939 589 770 9	938 497 154 6	1-04-08 20 :33: 41 G MT-5	.	ta > >	no t s et	ot r eque sted	E to SME prot ocol	M	s
31	F re e s pa ce	+5 939 589 770 9	+5 938 497 154 6	201 1-04-08 21 :00: 23 G MT-5	El numero 59384971546 ha solicitado que lo llame .	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
32	F re e s pa ce	+5 939 589 770 9	+5 938 497 009 0	201 1-04-02 21 :48: 26 G MT-5	Ke el pincl d Dios dibuje en tu rostro la + linda son risa y salpike sobre tu vida las + bllas bendiciones y alegre tu corazon.... Linda noche mami hermosa!...	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
33	F re e s pa ce	+5 939 589 770 9	+5 938 303 955 1	201 1-03-09 18 :30: 27 G MT-5	Kary cuando ya te vayas me avisas pa ir a ver mis c osas Porfis??	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
34	F re e s pa ce	+5 939 589 770 9	+5 938 497 154 6	201 1-03-09 20 :21: 15 G MT-5	El numero 59384971546 ha solicitado que lo llame .	Da ta > >	Is no t s et	Is n ot r eque sted	SM E to SME prot ocol	GS M	ye s
35	F re e s pa ce	+5 939 589 770 9	+5 939 584 018 8	201 1-03-16 09 :45: 49 G MT-5	Gracias...	Da ta > >	Is no t s et	Re ques ted	SM E to SME prot ocol	GS M	ye s

Report SMS (deleted)

Record numbe r	Service Cente r	Recipient Addres s	Service center time stam p	Discharge tim e	User dat a

Submit SMS (deleted)

Record numb er	Sta tus	Servic e Cent er	Destinati on Addr ess	Validat ion peri od	Te xt	Forma tted Te xt	Repl y Pat h	Status Re port Req uest	Message Referen ce	Protoco l Identif ier	Coding Schem e	Is Co mplet ed

Generated by Paraben's SIM Card Seizure 2.1.3638.31695