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

Maleza Jorge, Sandoval Karina, Hidalgo Pablo

Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional

***Resumen*** **–** Se propone un sistema de análisis forense para teléfonos celulares con tecnología GSM (Global System For Mobile Communications). Este análisis permite obtener evidencias o pruebas auténticas e íntegras, que contribuyen a la investigación en un proceso judicial, pudiendo posteriormente 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 pueden estar involucrados en diferentes tipos de delitos.

En este trabajo se establece qué evidencia digital potencial puede ser proporcionada por el teléfono celular, para lo cual se analiza la información del Equipo móvil y la Tarjeta SIM.

Este análisis se desarrolla 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.

*Índices* – Análisis forense celular, evidencia digital, evidencia electrónica, dispositivos móviles celulares, tecnología GSM.

## I. INTRODUCCIÓN

La necesidad de comunicación del ser humano lo ha motivado a desarrollar sistemas altamente sofisticados, que incorporan conceptos inalámbricos y de movilidad. 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.

Los dispositivos móviles celulares no son solamente utilizados para tareas ordinarias como recibir y enviar mensajes o llamadas, sino que algunos de ellos 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].

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[2] 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 tienen leyes claras al respecto.

## II. MARCO TEÓRICO

### A. *Telefonía Celular GSM en el Ecuador y en el Mundo*

GSM de las siglas en inglés *Global System For Mobile Communications*, es un estándar mundial para teléfonos celulares, diseñado para utilizar señales digitales, así como también, canales de voz y canales de control digitales. Existen cuatro versiones principales, basadas en la banda de frecuencia que utilizan para su operación: GSM-850, GSM-900, GSM-1800 y GSM-1900.

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.

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].

Como muestra la Figura 1, la tecnología GSM es el estándar de telefonía celular más utilizado alrededor del mundo; según GSMA y la Firma de Industrias Móviles *Wireless Intelligence*, en un reporte de Julio del año 2010, se anunció que el número de conexiones móviles globales ha sobrepasado los 5000 millones en el mercado mundial, después de que a finales del 2008 se registraron 4000 millones de conexiones.

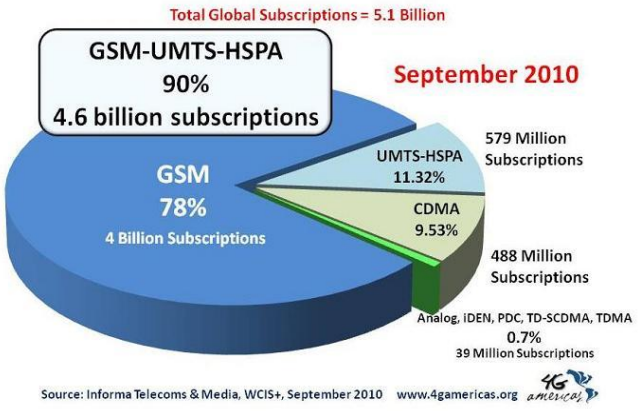


Figura 1: Comparación de la tecnología GSM con las tecnologías UMTS, HSPA, CDMA, entre otras tecnologías celulares en el mundo.

[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.

[2] *Evidencia Electrónica* se refiere al elemento material o hardware.

*Evidencia Digital* se refiere a la información contenida o almacenada en los dispositivos físicos o evidencia electrónica.

### B. *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.

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.

Por consiguiente, la evidencia digital no solo está limitada a lo que se encuentra en las computadoras, también se puede extender a los dispositivos electrónicos tales como MP3, memorias flash, Ipod, teléfonos celulares, entre otros aparatos de telecomunicaciones y multimedia.

## III. TÉCNICAS DE EXTRACCIÓN DE LA INFORMACIÓN

### A. *Evidencia Potencial en la Arquitectura GSM*

Dentro de la Arquitectura Instalada Fija de GSM, son de interés como evidencia digital los CDRs (*Call Detail Records*), que se crean y almacenan en el MSC (*Mobile Switching Center*) con el propósito de facturación e identificación de las BTS (*Base Transceiver Station*) sobre las cuales fueron efectuadas llamadas y mensajes de texto, además de información de tiempo y localización del suscriptor.

Este análisis requiere de la participación en su totalidad de la Operadora de Telefonía Móvil, quién muchas veces no está dispuesta a colaborar, por razones de seguridad o cuestiones 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.

### B. *Evidencia Digital Potencial en el Equipo Móvil*

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.

En general la evidencia digital lo constituye:

- IMEI (*International Mobile Equipment Identity*)
- Directorio Telefónico
- Historial de Llamadas
- Mensajes cortos, Mensajes multimedia, buscadores *Web*/WAP y correos electrónicos
- Calendario
- Otros dispositivos, por ejemplo memorias externas.

### C. *Evidencia Digital Potencial en la Tarjeta SIM*

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) o la raíz del sistema de archivos, los Archivos Dedicados (DF) que sirven como directorios, y los Archivos Elementales (EF) 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 dígitos hexadecimales que tienen una extensión de 2 *bytes*.

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. En la Tabla 1 se muestran los elementos de evidencia digital útil para el examinador forense.

### D. *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.

*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.

TABLA 1: EF'S QUE CONTIENEN EVIDENCIA DIGITAL DE LA TARJETA SIM

| 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, seguido de un código de país, un número de identificación del emisor, y un número de identificación de cuenta individual. |
| | **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 es 3 dígitos, y el MSIN asignado por el operador. |
| | **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. |
| | **SPN** | ***Service Provider Name*****,** Nombre del Proveedor de Servicios**,** es una EF opcional que contiene el |

| | | |
|---|---|---|
| | | nombre del proveedor de servicios. 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. |
| | **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.<br>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. 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.<br>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).<br>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.<br>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. |

*a) Extracción Manual:* Generalmente se utiliza cuando no se encuentran 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. 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.

*b) Extracción Lógica:* En general, usa protocolos propietarios de los fabricantes, con modificaciones para no alterar la 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.

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. Existen algunas técnicas disponibles para que el analista pueda recuperar los datos del teléfono celular.

*a) 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.

*b) 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 conocidos como JTAG (*Joint Test Action Group*).

### *E. Protección de la Información.*

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.

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.

## IV. HERRAMIENTAS DE EXTRACCIÓN DE LA INFORMACIÓN

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.

### *A. 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.

Estas herramientas suelen realizar adquisiciones lógicas de información utilizando protocolos comunes para la sincronización, la depuración, y las comunicaciones. 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; esto ocasiona que los fabricantes de herramientas forenses mantengan una lista de teléfonos y características compatibles con su software.

*1) Escenarios Bajo los cuales se analizan y comparan las Herramientas Forenses a Utilizar:* Para este estudio se utilizaron varios teléfonos GSM y se los analizó en dos conjuntos de escenarios; 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 escenarios definen un conjunto de actividades prescritas, utilizadas para medir las capacidades de la herramienta forense, para recuperar información de un teléfono celular, a partir de la conectividad y adquisición progresiva de información.

La Tabla 2 ofrece una visión general de estos escenarios que se analizan para todos los dispositivos meta. Para tener en claro cada escenario de la lista, se realiza una breve descripción de su objeto.

TABLA 2: ESCENARIOS DE ANÁLISIS DE HERRAMIENTAS FORENSES PARA EL DISPOSITIVO MÓVIL

| Escenario | Descripción |
|---|---|
| ***HEX DUMP*/ Extracción Lógica** | Determinar si la herramienta puede realizar una extracción lógica o volcado de memoria. |
| **Conectividad y Recuperación** | Determinar si la herramienta puede conectarse correctamente al dispositivo y recuperar el contenido del mismo. |
| **Aplicaciones PIM (*Personal Information Manager*)** | Determinar si la herramienta puede encontrar información aunque ésta se haya eliminado, además que encuentre aplicaciones PIM. |
| **Llamadas Marcadas/ Recibidas** | Determinar si la herramienta encuentra llamadas telefónicas marcadas, recibidas y perdidas, incluidas las llamadas que han sido eliminadas. |
| **Mensajes SMS/MMS** | Determinar si la herramienta encuentra los SMS/MMS realizados, recibidos y borrados. |
| **Mensajes de Internet** | Determinar si la herramienta puede recuperar correos electrónicos y mensajes instantáneos (IM), enviados y recibidos; incluyendo los mensajes borrados. |
| **Aplicaciones Web** | Determinar si la herramienta puede encontrar sitios Web visitados y la información que fue intercambiada a través del Internet. |
| **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. |
| **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. |
| **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).* |
| **Pérdidas de Energía** | Determinar si la herramienta puede adquirir cualquier información del dispositivo después de que éste ha perdido su energía. |

La Tabla 3 ofrece una visión general de los escenarios SIM, incluyendo su propósito, el método de ejecución, y los resultados esperados.

Se considera un conjunto de escenarios distintos para las herramientas forenses de tarjetas SIM; y para la adquisición de datos se usa un lector externo.

TABLA 3: ESCENARIOS DE ANÁLISIS PARA LAS HERRAMIENTAS FORENSES EN LA TARJETA SIM

| 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 borradas. |
| **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. |

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 las herramientas.

### *B. 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.

*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.

*a) ZRT 2:* Ayuda al investigador a extraer información específica del dispositivo electrónico, por medio de sus herramientas de *hardware* y *software*. 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.

*2) Herramienta de Extracción Lógica:* En este nivel de análisis, se detallarán herramientas forenses como:

*a) Oxygen Phone Manager Forensic Suite 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), entre otros.

*b) Device y SIM Card Seizure (Paraben):* Estas herramientas forenses sirven para la adquisición de información de varios dispositivos. 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. La versión para dispositivos móviles se denomina "*Device Seizure*" y el "SIM *Card Seizure*" es para el análisis de tarjetas SIM.

*c) Secure View 2.0 (SV2):* Es una herramienta forense de software que ayuda a analizar diferentes dispositivos. 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 pérdidas.

*3) Herramienta de Análisis Físico:* En este nivel de análisis, se detallará la herramienta:

*a) UFED (CelleBrite):* Es una herramienta capaz de adquirir datos desde dispositivos móviles y almacenar la información en una unidad USB, tarjeta SD o en el 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), grabaciones de audio, 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.

### *C. Análisis Comparativo de las Herramientas Utilizadas*

El propósito de las herramientas forenses para teléfonos celulares es el obtener datos del equipo móvil sin tener la necesidad de modificar o alterar los datos.

Al contar con diversas características, se analizó en un mismo entorno (escenarios) y con algunas marcas de teléfonos celulares, 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.

Para esta comparación es necesario considerar la siguiente descripción, bajo los escenarios de análisis:

( / ) 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.

En la Tabla 4, 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.

TABLA 4: HERRAMIENTAS VS ESCENARIOS (INFORMACIÓN CREADA Y RECOLECTADA)

| Escenario | Herramientas Analizadas | | | | | |
|---|---|---|---|---|---|---|
| | **Device Seizure** | **SIM Card Seizure** | **Secure View** | **ZRT 2** | **OPM** | **UFED** |
| **Hex Dump/ Extracción Lógica** | X | X | X | / | / | * |
| **Conectividad y Recuperación** | * | / | * | / | * | - |
| **Aplicaciones PIM** | X | - | - | X | * | X |
| **Llamadas Marcadas/ Recibidas** | X | X | X | X | * | X |
| **SMS/MMS** | X | X | X | X | * | X |
| **Mensajes de Internet** | - | / | / | X | * | - |
| **Aplicaciones Web** | - | / | / | X | - | - |
| **Formato de Archivos de Texto, Gráficos y Archivos Comprimidos** | X | / | / | X | * | X |
| **Tarjetas de Memoria Periféricas** | X | / | X | X | * | X |
| **Coherencia de Adquisición** | X | X | X | X | X | X |
| **Pérdidas de Energía** | * | / | / | / | - | - |
| **Datos Básicos** | / | X | X | / | X | X |
| **Información de Localización** | / | X | X | / | X | X |

Mientras que la Tabla 5 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.

TABLA 5: HERRAMIENTAS VS ESCENARIOS (INFORMACIÓN ELIMINADA Y RECOLECTADA)

| Escenario | Herramientas Analizadas | | | | | |
|---|---|---|---|---|---|---|
| | **Device Seizure** | **SIM Card Seizure** | **Secure View** | **ZRT 2** | **OPM** | **UFED** |
| **Hex Dump/ Extracción Lógica** | X | X | X | / | / | X |
| **Conectividad y Recuperación** | * | / | / | / | * | - |
| **Aplicaciones PIM** | X | - | - | / | - | - |
| **Llamadas Marcadas /Recibidas** | X | X | X | / | * | X |
| **SMS/MMS** | X | X | X | / | * | X |
| **Mensajes de Internet** | - | / | / | / | * | - |
| **Aplicaciones Web** | - | / | / | / | - | - |
| **Formato de Archivos de Texto, Gráficos y Archivos Comprimidos** | X | / | / | / | * | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Coherencia de Adquisición** | X | X | X | / | X | X |
| **Tarjetas de Memoria Periféricas** | X | / | X | / | * | X |
| **Pérdidas de Energía** | - | / | / | / | - | - |
| **Datos Básicos** | / | X | X | / | X | X |
| **Información Localizada** | / | X | X | / | X | X |

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*.

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 éstas presentan bajo ciertos dispositivos móviles.

## V. Procedimientos y Principios Técnico-Legales Aplicables Al Análisis Forense Celular En El Ecuador

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 cuál es la participación que tienen estas personas dentro de una escena del crimen o del hecho.

*a)* Personal de Primera Respuesta
*b)* Examinadores de Evidencia Digital
*c)* Investigadores del Delito
*d)* Peritos

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.

### *A. Validación de la Evidencia Digital*

Para dar validez a la evidencia digital la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas[3] 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 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 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.

### *B. Medio de Prueba*

El medio de prueba dentro del proceso es de vital importancia, ya que a partir de él 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

[3] Ley No. 67, publicada en el Registro Oficial Suplemento No. 577 de 17 de Abril del 2002.

existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables.

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.

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).

En este contexto los elementos físicos hacen referencia al hardware (Equipo Móvil y Tarjeta SIM), mientras que los elementos digitales, se refieren a todos los datos almacenados y transmitidos usando el hardware.

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.

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.

Para la admisibilidad de la evidencia digital de un teléfono celular se deben tomar en cuenta dos situaciones:

*a)* 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 custodia sobre los elementos físicos, "Elemento de Pertenencia de la Evidencia Digital".

*b)* 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 tanto para autenticar la evidencia obtenida en la escena del hecho, se deben 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.

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:

*a)* Cumplimiento de los principios básicos, reconocidos internacionalmente en el manejo de evidencias digitales.

*b)* Cumplir los principios constitucionales y legales.

*c)* El establecimiento de un Sistema de Operaciones Estándar.

*d)* Entender el trámite legal determinado principalmente en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Código de Procesamiento Penal.

### *C. Principios Aplicables a la Evidencia Digital*

Según la Asociación de Jefes y Oficiales Policiales de Reino Unido (ACPO, *Association of Chief Police Officers*), en su Guía de buenas prácticas de manejo de evidencia digital [3] se 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: 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.

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.

### *D. Colecta de Evidencia Digital en la Escena del Hecho*

Figura 2: Etapas y Fases dentro del Ciclo de Colecta de Evidencia

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 2.

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.

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.

*a)* 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[4] como el de Locard[5] y el de mismidad[6], aquí se da inicio al procedimiento pertinente de acuerdo a la infracción cometida.

Las siguientes fases se piden cumplir en esta etapa:

- Roles y funciones
- Detección de Evidencia
- Documentación relacionada con el dispositivo
- Documentación de los elementos incautados


*b)* 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, de forma tal, que permita el estudio posterior, la reconstrucción en una época alejada de la ocurrencia o utilizarla en un proceso judicial.

- Creación del registro de cadena de custodia[7]
- Aseguramiento de la evidencia electrónica
  - Embalaje
  - Transporte
  - Almacenamiento

### *E. Análisis de Evidencia Digital*

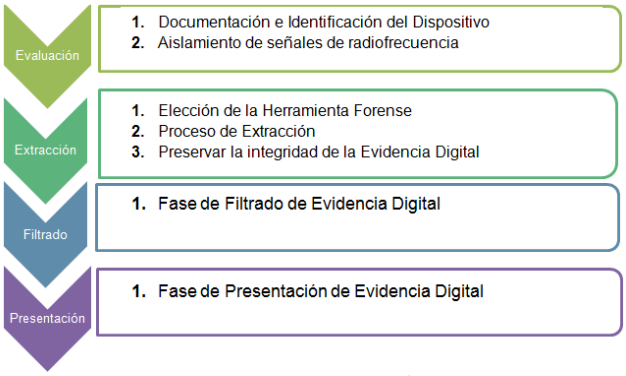


Figura 3: Etapas y Fases dentro del Ciclo de Análisis de Evidencia

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 siguen las etapas y fases mostradas en la Figura 3.

*a)* 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, por lo que se debe considerar:

- Documentación e Identificación del Dispositivo
- Aislamiento de señales de radiofrecuencia

[4] *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

[5] *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, 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.

[6] *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.

[7] *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.

*b)* 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; se debe considerar:

- Elección de la Herramienta(s) Forense(s) de Extracción
- Proceso de Extracción
- Preservar la integridad de la evidencia digital

*c)* 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.

*d)* 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.

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.

## VI. Documentación de un Caso

### *A. Definición del caso*

El escenario de prueba con el cual será ejemplificado el procedimiento de operaciones propuesto, se basa en la experiencia de los Investigadores y documentos que se tuvo acceso.

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.

### *B. Colecta*

*a)* Roles y funciones

Para el desarrollo de la presente investigación se realizará la asignación de roles 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.

TABLA 6: FORMULARIO DE IDENTIFICACIÓN DE PERSONAL

| **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 | | |
| _____<br>Firma<br>Responsable:_____<br>CI: :_____ | | |

*b)* Detección de Evidencia

Los datos llenados corresponden a un lugar ficticio puesto que no se pueden colocar las direcciones verdaderas del caso en investigación.

TABLA 7: FORMULARIO DE IDENTIFICACIÓN Y DETECCIÓN

| **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** | | | | | | | | | | | | |
| **Nombre y Apellido** | | | | | | Alex Maleza | | | | | | |
| **Nº de Identificación** | | | | | | 1718971456 | | | | | | |
| **Entidad** | Fiscalía | | | | | | | | | | | |
| **Cargo** | Investigador del Departamento de Investigación y Análisis Forense | | | | | | | | | | | |
| **Firma** | | | | | | | | | | | | |

*c)* Cadena de Custodia

Este paso nos da la idea general del proceso y las personas que estuvieron en contacto directo con la evidencia encontrada en la escena del hecho.

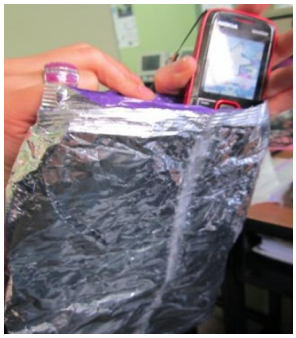

Figura 4: Aislamiento del dispositivo de señales de Radiofrecuencia

*d)* Aseguramiento de la evidencia electrónica

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 4.

Figura 5: Etiquetas y Almacenamiento de la Evidencia

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 5.

## *C. Evaluación*

TABLA 8: ELEMENTOS INCAUTADOS 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, junto a 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. |

*a)* Documentación e Identificación del Dispositivo

Se recepta los elementos incautados y formularios, con el fin de obtener un conocimiento general de la escena del hecho.

*b)* Aislamiento de señales de Radiofrecuencia

El dispositivo es recibido dentro de una bolsa de papel aluminio, con la carga del celular completa.

## *D. Extracción*

*a)* 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, 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.

*b)* Proceso de Extracción

Se procede al llenar el Formulario de Análisis del dispositivo.

TABLA 9: FORMULARIO DE ANÁLISIS DEL DISPOSITIVO

| **FORMULARIO DE ANÁLISIS DEL DISPOSITIVO** | | | |
|---|---|---|---|
| Código de Evidencia: | 1001-1 | Caso: | 1001-1 |
| Investigador: Karina Sandoval | | Examinador: Jorge Maleza | |
| Descripción del Caso: | | | |
| Recepción para el análisis (dd/mm/yy): 17 / 05/ 2011 | | | Hora: 13:00 |
| Análisis: | (dd/mm/yy): 17 / 05/ 2011 | | Hora: 14:15 |
| 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 | | | |
| Clave del Dispositivo: 12345 | | Cargador: Nokia | |
| Cable: USB | | Programa: UFED | |
| Teléfono Bloqueado ☐ Si ☐ No | Soporta Modo de Vuelo ☐ Si ☐ No Esta habilitado? Si No | Saludo Inicial ☐ Si ☐ No | Telefono Encendido ☐ Si ☐ No | PUK Obtenido ☐ Si ☐ No |
| Detalles de la Batería | | | |
| Batería Removida ☐ Si | Dispositivo Cargado ☐ Si | Fabricante de la Batería: Nokia | |
| | | Cap. de Voltaje de la Batería: 3.7 V | |
| | | Número de Serie Batería: 0670398462040 | |

| | | | |
|---|---|---|---|
| | Resultado Voltímetro/Batería: 3.6 V | | |
| Notas: | | | |
| Características de la Tarjeta SIM | | | |
| Información de la Tarjeta SIM: | | | |
| Número ICCID en la Tarjeta SIM: | 8959300500625551713 | | |
| Proveedor: Movistar | SIM Card dañada | SI: __ | No: x |
| Describa el daño: N/A | | | |
| Errores durante la adquisición: N/A | | | |
| Datos Básicos: | | | |

IMSI ☐ Si ☐ No ☐ N/A
ICCID ☐ Si ☐ No ☐ N/A
MSISDN ☐ Si ☐ No ☐ N/A
SPN ☐ Si ☐ No ☐ N/A
EXT1 ☐ Si ☐ No ☐ N/A
FDN ☐ Si ☐ No ☐ N/A
SDN ☐ Si ☐ No ☐ N/A
EXT3 ☐ Si ☐ No ☐ N/A
ADN ☐ Si ☐ No ☐ N/A
LDN ☐ Si ☐ No ☐ N/A
SMS ☐ Si ☐ No ☐ N/A
EXT2 ☐ Si ☐ No ☐ 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.<br>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. |

*c)* Preservar la integridad de la evidencia digital

Como se muestra en la Figura 6 se obtiene los valores *hash* de la información almacena en el teléfono celular.


Figura 6: Valores *Hash* calculados del Equipo Móvil por la Herramienta UFED

## *E. Filtrado*

*a)* 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.

## *F. Presentación*

*a)* 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.

# VI. CONCLUSIONES

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.

Sin embargo debido a los cambios rápidos en la tecnología los teléfonos celulares presentan un problema especial para la aplicación de la ley.

Además si consideramos que 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 el descubrimiento, recolección, análisis y presentación de la misma.

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.

Por lo que el sistema propuesto describe una transformación de los elementos obtenidos en un contexto físico mediante la colecta de evidencia en la escena del hecho, pasando luego a un contexto virtual mediante el análisis de evidencia y terminando en el contexto legal, proporcionando bases legales para que esta evidencia sea admitida.

# RECONOCIMIENTOS

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 Dr. Santiago Acurio del Pino, por su colaboración, excelente disposición y apertura en el desarrollo de este proyecto.

# REFERENCIAS

[1] MALEZA J., SANDOVAL K., “Estudio y análisis de Evidencia Digital en teléfonos celulares con tecnología GSM para procesos

judiciales". Proyecto de Titulación, Escuela Politecnica Nacional, Quito, Ecuador, 2011

[2] http://www.revistalideres.ec/2010-10-04/Informe.aspx, última visita Febrero 2010

[3] 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] ASSOCIATION OF CHIEF POLICE OFFICERS.: Good Practice Guide for Computer-Based Electronic Evidence, version 4.0.

[5] ACURIO DEL PINO, Santiago; PAEZ, Juan.: Derecho y Nuevas Tecnologías, Corporación de Estudios y Publicaciones (CEP), Junio 2010, Primera Edición.

## BIOGRAFÍA

**Jorge Alexander Maleza Peñaherrera**
Nació en Quito, el 4 de Enero de 1987. Realizó sus estudios secundarios en el Colegio Experimental "Juan Pio Montufar". Ingresó a la Escuela Politécnica Nacional en el 2005, para realizar sus estudios de pregrado los cuales terminó en el año 2011, obteniendo el título de Ingeniero en Electrónica y Telecomunicaciones. Actualmente trabaja en Sonda del Ecuador, Proyecto Movistar – Huawei, en el cargo de Ingeniero de Soporte para el área de Gestión de Red Movistar. Miembro IEEE.

**Karina Gabriela Sandoval Duque**
Nació en Salcedo, el 11 de Julio de 1986. Realizó sus estudios en el "Colegio de la Inmaculada" en la ciudad de Ambato. Los estudios superiores los desarrolla y culmina en la Escuela Politécnica Nacional en la Facultad de Ingeniería Eléctrica y Electrónica, obteniendo el título de Ingeniero en Electrónica y Telecomunicaciones en Diciembre 2011. Actualmente es miembro IEEE y trabaja en Sonda del Ecuador para el Centro Soporte de Datos de Movistar.

**Pablo Hidalgo Lascano (Director del Proyecto)**
Nació en Ambato en 1959. Obtuvo el título de Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional (1985) siendo declarado el mejor graduado de su promoción. Becado por el Gobierno Alemán y auspiciado por la E.P.N. realizó estudio de postgrado en Telecomunicaciones en el Deutsche Bundespost (1988 - 1990) en Alemania Federal. Adicionalmente ha realizado estudios en la Maestría de Conectividad y Redes de Telecomunicaciones en la E.P.N. (2000 - 2002). Actualmente se desempeña como profesor principal del Departamento de Electrónica, Telecomunicaciones y Redes de Información de la E.P.N. Fue promotor y Coordinador de la Carrera de Ingeniería en Electrónica y Redes de Información de la E.P.N. (2000 – 2007). Ha dirigido más de 70 tesis de grado y proyectos de titulación. Se ha desempeñado como consultor y asesor para algunas entidades públicas y privadas. Sus áreas de interés actuales son: Redes de Información, Comunicaciones Inalámbricas y Transmisión de Datos. Es miembro de la Association for Computing Machinery (ACM) y el Institute of Electrical and Electronics Engineers (IEEE).