UNIVERSIDAD NACIONAL DE LA MATANZA

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS DE MAESTRÍA

Título de tesis: Marco de referencia para el análisis forense de dispositivos Android

Autor: *Walter R. Ureta*
Director: *Mag. Jorge Eterovic*

Buenos Aires, Mayo 2013

Dedicado a
mi familia

Resumen

La investigación realizada en este trabajo de tesis de maestría se extiende a las bases y metodologías de la práctica forense general para tomar procedimientos específicos del área informática tanto técnicos como de proceso, y en función de estos, establecer un marco de referencia para el trabajo de análisis forense de dispositivos móviles que ejecuten el sistema operativo Android.

En este documento se buscará identificar las mejores prácticas de peritaje, para dispositivos móviles, con el fin de asociarlas con las diferentes etapas de los modelos de referencia y sobre esta selección realizar aportes a fin de establecer un procedimiento con coherencia procedimental, detalles técnicos y flexibilidad para adaptarse al amplio espectro de dispositivos móviles actualmente en uso.

Agradecimientos

Este trabajo no hubiera sido posible sin la contribución de todas aquellas personas que han participado directa o indirectamente de mi formación y desarrollo académico y profesional. Así mismo quiero extender mi agradecimiento a aquellos que han contribuido en el proceso de desarrollo de esta tesis con su paciencia, conocimiento y tiempo.

Muchas gracias
Walter R. Ureta

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Contexto de la investigación

Desde comienzos de esta década el mercado móvil tuvo una tendencia creciente en Latinoamérica; según *Informa Telecoms & Media*[lat, 2013] el mercado móvil latinoamericano crecería en un 7,1 % durante 2013 con aproximadamente 742 millones de suscripciones móviles activas para finales de ese año. Constituyendo un incremento notable, ya que en 2012 se reportó que había 630 millones de conexiones móviles en toda la región.

El crecimiento no se limitó a las suscripciones móviles: Informa pronostica que las conexiones de smartphones[1] en Latinoamérica aumentarían en un 35 % en 2013 para llegar a más de 140 millones.

Según *Pyramid Research*[pyr, 2013], el 42 % de los teléfonos móviles vendidos en Argentina durante 2012 fueron smartphones, y estimó que en 2013 el 53 % de los teléfonos móviles vendidos serian smartphones. Ya para 2017, se pronostica que más del 70 % de los teléfonos móviles vendidos en Argentina serán smartphones. Para el caso de los dispositivos LTE[2] la empresa generó un nuevo estudio[pyr, 2015] donde se relevó la existencia de 13.7 millones de subscriptores para Latinoamérica durante el año 2014, teniendo a Brasil como el principal actor con el 49.2 % de las mismas. El mismo estudio realiza una proyección de crecimiento a mas de 150 millones para el año 2019 en este mismo segmento.

[1] Smarthphones: Teléfonos inteligentes
[2] LTE: Long Term Evolution, o de evolución de termino largo

Además, según indicó la consultora *IDC*[pyr, 2013], en 2012 más de 5,9 millones de smartphones se venderían en Argentina; tratándose de un incremento del 44 % comparado con 2011. Cabe mencionar que *Pyramid Research* indico que el sistema operativo Android cuenta con una cuota del 57 % del mercado de smartphones en Argentina, al mismo tiempo que para *IDC* se vendieron 340.000 tablets en Argentina durante 2012, lo cual se trata de un incremento del 43 % comparado con 2011.

Alineados con estas previsiones, que se han cumplido en los últimos años, *eMarketer* muestra en su reporte del año 2015[mob, 2015] la importancia que han tomado los dispositivos móviles en los hábitos de vida de la población de la República Argentina, mostrando que se estima que los consumidores del país utilizan 3.5 horas diarias para conectarse a internet desde sus dispositivos móviles. Este relevamiento ha tomado como fuente a múltiples casos de estudio de *Cámara Argentina de Comercio Electrónico* y *TNS Argentina*, también indica que se estima que en el mismo año existan en el país 29.0 millones de usuarios de internet, 30.7 millones de usuarios de teléfonos móviles, 12.6 millones de smartphones y 6.6 millones de usuarios de tablets.

Otro factor de importancia que debe ser considerado antes de abordar la problemática es el desarrollado en "What's on the Horizon for Mobile"[hor, 2015], elaborado por *eMarketer* durante el año 2015 utilizando información de *GSMA Intelligence*, allí se observa como en esta década hay una marcada tendencia creciente tanto en operaciones M2M[3] como en el porcentaje de las mismas que corresponden a dispositivos móviles; particularmente se observa una situación inicial de 73 millones de operaciones con 1 % de agentes móviles para el año 2010, contra una proyección final de 980 millones de operaciones con un 10 % correspondiente a dispositivos móviles para el año 2020.

En este contexto de expansión en el uso de dispositivos móviles, y siendo el sistema operativo Android el mas importante y con mayor proyección en el mercado para los próximos años, es lógico que emerja la necesidad de poder aplicar las técnicas forenses de tecnología sobre estas plataformas tanto en procesos judiciales como particulares.

Desde la premisa citada por Darahuge y Arellano en Manual de Informática Forense

[3]M2M: Machine to Machine, o maquina a maquina.

[Darahuge, 2011] que enuncia que "La Informática forense es a la Informática lo que la Medicina legal es a la Medicina", nos es fácil comprender la necesidad del desarrollo de metodologías y prácticas para esta especialidad. Tanto en el ámbito judicial como comercial es necesaria la aplicación de esta disciplina, requiriendo procedimientos bien definidos y adaptables a los diferentes escenarios que pueden presentarse, abarcando tanto dispositivos convencionales como las nuevas tecnologías que han aparecido en el mercado y se integran en la vida de personas y empresas almacenando y gestionando su información.

Es justamente la reciente y constante penetración de los dispositivos móviles en nuestra sociedad lo que plantea la necesidad de disponer de un marco de trabajo bien definido y flexible para poder realizar prácticas forenses en relación a incidentes en los que se vean envueltos estos dispositivos.

Por lo tanto, la necesidad identificada previamente, planteada sobre la aparición de estos dispositivos junto con su rápida y creciente adopción social, toma mayor importancia no solo por la demanda de conocimientos y técnicas asociada a este escenario sino también porque estos dispositivos evolucionan y cambian constantemente por razones de mercado, definiendo el contexto y la complejidad general de la problemática abordada en este trabajo.

Debido a que la historia pericial coincide con la historia humana según la medicina legal, encontraremos un amplio registro de antecedentes y desarrollos en cuanto al aspecto metodológico de los procedimientos forenses como a la definición y requisitos de formalidades desde el aspecto jurídico. Dichos aspectos son la base del desarrollo de conocimiento en el área especifica del análisis forense informático a partir de las últimas décadas del siglo veinte.

Capítulo 2

Marco de estudio

2.1. Modelos

A continuación se describirán diferentes modelos de uso común en la metodología de la práctica forense dentro del paradigma actual, los mismos nos permiten apreciar que existen características comunes adoptadas por todos ellos y que deben estar presentes con su secuencia lógica a lo largo de cualquier actividad informática forense.

2.1.1. Casey, E., 2011

Eoghan Casey, en el año 2000 presenta un modelo para procesar y examinar evidencias digitales. Este autor señala que éste es un ciclo de procesamiento de prueba, porque al hacer la reconstrucción pueden hallarse pruebas adicionales que provoquen que el ciclo comience nuevamente. El modelo de Casey es general y se aplica exitosamente para ambos sistemas, las computadoras aisladas y conectadas a una red.

El modelo de Casey[Casey, 2004] ha evolucionado desde el primer modelo presentado en el 2002, se pueden resumir las siguientes etapas:

- *Autorización y Preparación*: Durante esta fase se obtiene autorización para proceder a recoger pruebas en la escena del delito, con este permiso se verifica la capacidad técnica y se ejecuta la recolección..

- *Identificación*: En escena del delito se identifica el hardware y software afectado al delito.

- *Documentación*: De manera continua se deben anotar todos los pasos realizados para ayudar a una reconstrucción final de los archivos y/o información vinculada al caso.

- *Adquisición*: Se debe obtener todo el hardware encontrado que pueda tener pruebas. Generalmente la prueba no es el hardware en sí (huellas digitales, números de serie de CPU[1]), sino el contenido de los mismos. De modo que se debe extraer una imagen de cada dispositivo encontrado.

- *Conservación*: El hardware debe conservarse de forma que no se altere su contenido y es primordial hacer varias copias de la imagen extraída de cada dispositivo y nunca manipular el original.

- *Examen y Análisis*: Con los datos obtenidos previamente se procede a elaborar una hipótesis, y a partir de ella recopilar datos que permitan confirmar o refutar la misma.

- *Reconstrucción*: Con los datos analizados se debe poder recomponer la situación en torno al delito en cuestión.

- *Publicación de conclusiones*: Los resultados de los análisis forenses deberían publicarse, en la medida de lo posible, para incrementar el conocimiento de otros investigadores y en último caso para posibles sistemas expertos que en el futuro puedan ayudar en este campo.

La siguiente imagen muestra como se vinculan las diferentes etapas del proceso

[1]Unidad Central de Proceso: es el componente principal de una computadora

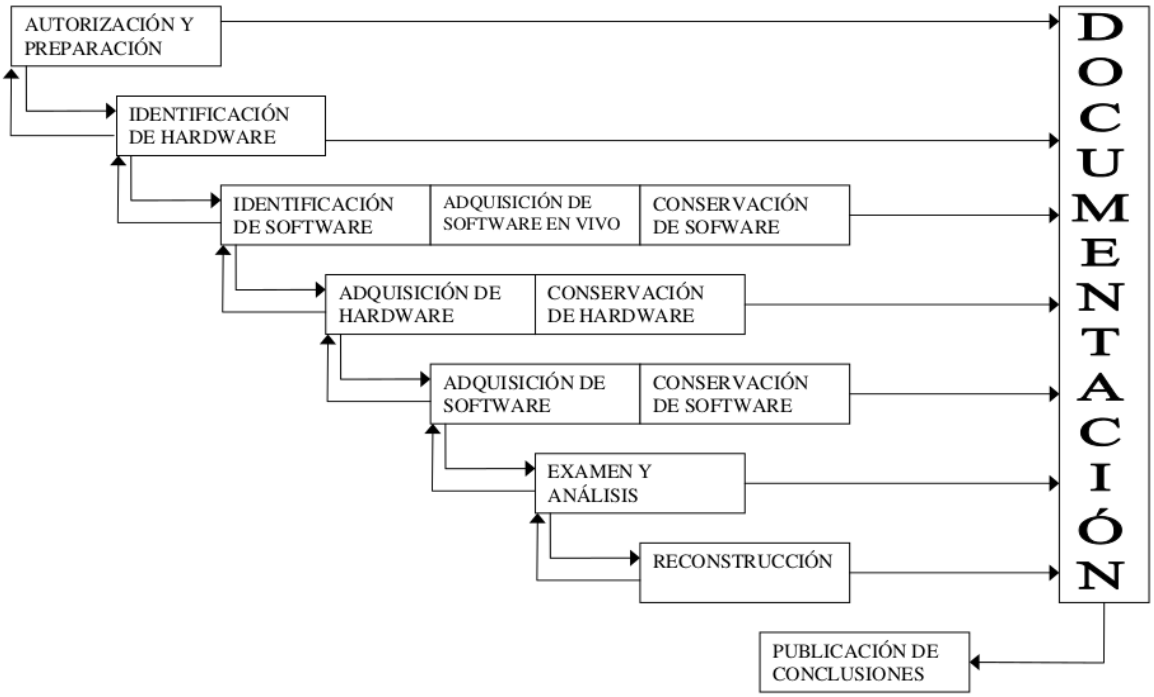

Figura 2.1: Etapas del proceso según Eoghan Casey

2.1.2. DFRWS-Digital Forensic Research Workshop, 2001

En Utica, Nueva York durante el año 2001 se desarrollo el primer "Digital Forensic Research Workshop - DFRWS". En este evento se creó y obtuvo consenso un documento[Trabajo colectivo de participantes del DFRWS por,] sobre el estado de la informática forense del momento. En sus conclusiones se logra establecer que la informática forense es un proceso, con un conjunto de etapas razonables y comunes.

Dichas etapas son:

1. La identificación
2. La preservación
3. La recolección
4. El examen o investigación
5. El análisis

6. La presentación

7. La decisión

El siguiente gráfico expande las mismas marcando con color gris el grupo de etapas principales o de"Core".

Identificación	Preservación	Recolección	Investigación	Análisis	Presentación	Decisión
Detección del Evento/Crimen	Gestión del caso	Preservación	Preservación	Preservación	Documentación	
Firma de resolución	Tecnologías de imágenes	Métodos Aprobados	Trazabilidad	Trazabilidad	Testimonio del experto	
Detección del perfil	Cadena de custodia	Software Aprobado	Técnicas de Validación	Estadísticas	Aclaración	
Detección de la anomalía	Sincronización del tiempo	Hardware Aprobado	Técnicas de Filtrado	Protocolos	Declaración del impacto de la Misión	
Quejas		Autoridad legal	Coincidencias de patrones	Minería de datos	Contra-medida Recomendada	
Monitoreo del Sistema		Comprensión sin pedidas	Descubrimiento de datos ocultos	Línea de tiempo	Interpretación de estadísticas	
Análisis de auditoria		Muestreo	Extracción de datos ocultos	Asociación		
Etc.		Reducción de datos		Espacial		
		Técnicas de Recuperación				

Figura 2.2: Etapas principales o de Core por el DFRWS 2001

2.1.3. Reith, M.; Carr, C.; Gunsch, G.; IJDE, 2002

Reith M., Carr C. y Gunsch G. han realizado una revisión de diversos modelos para la práctica forense en publicaciónes de la "International Journal of Digital Evidence", particularmente "An Examination of Digital Forensic Models"[Trabajo colectivo de participantes del DFRWS por,]. El resultado de este trabajo derivó en el aporte de un nuevo modelo que tiene una estrecha relación con el modelo DFRWS, detallado en Baryamureeba V. and Tushabe, F. "The Enhanced Digital Investigation Process Model"[V. and Tushabe, 2004]. En este modelo se identifican nueve etapas con un enfoque abstracto pretendiendo que pueda ser adaptado

a diferentes escenarios de la práctica informática forense, las mismas se enumeran a continuación:

1. La identificación
2. La preparación
3. La estrategia de acercamiento
4. La preservación
5. La recolección
6. El examen
7. El análisis
8. La presentación
9. La devolución de evidencia

2.1.4. Carrier, B. and Spafford, E. (2003).“Getting Physical with the Digital Investigation Process”

En este documento[Carrier and Spafford, 2003] los autores realizaron una revisión de trabajos previos y relacionan el proceso de investigación digital al proceso de investigación físico convencional. Como resultado de este análisis surge el “Proceso de Investigación Digital Integrado” o “Integrated Digital Investigation Process”, que define diecisiete fases organizadas en cinco grupos:

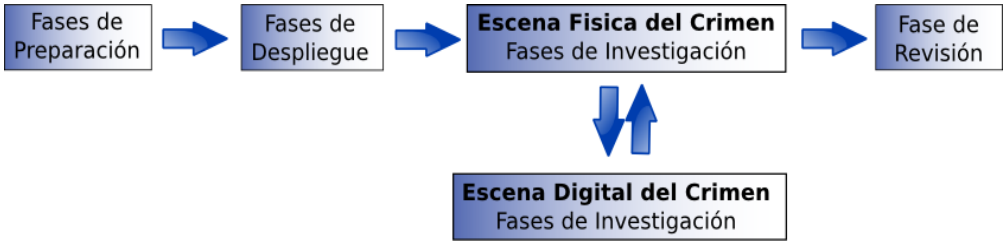

Figura 2.3: Fases del proceso según Carrier y Spafford

Fases de Preparación (Readiness)

Su objetivo es garantizar que las operaciones e infraestructura son capaces de soportar la investigación. Sus dos componentes son:

1. Fase de preparación de operaciones (Operations Readiness phase): que asegura que los investigadores están capacitados y equipados para manejar un incidente cuando ocurre.

2. Fase de preparación de infraestructura (Infrastructure readiness phase): que asegura que la infraestructura disponible es suficiente para tratar con los incidentes del caso. Por ejemplo, cámaras fotográficas, material de protección y transporte de hardware, etc.

Fases de Despliegue (Deployment)

El propósito es proveer un mecanismo para detectar y confirmar un incidente. Incluye dos fases:

1. Fase de Detección y Notificación: aquí se detecta el incidente y se notifica a las personas apropiadas.

2. Fase de Confirmación y Autorización: se confirma el incidente y se obtiene la aprobación legal para ejecutar una búsqueda.

Fases de Investigación Física de la escena del crimen

Estas fases tienen como finalidad recopilar y analizar las evidencias físicas para reconstruir las acciones que ocurrieron durante el incidente. Esta compuesta por seis fases:

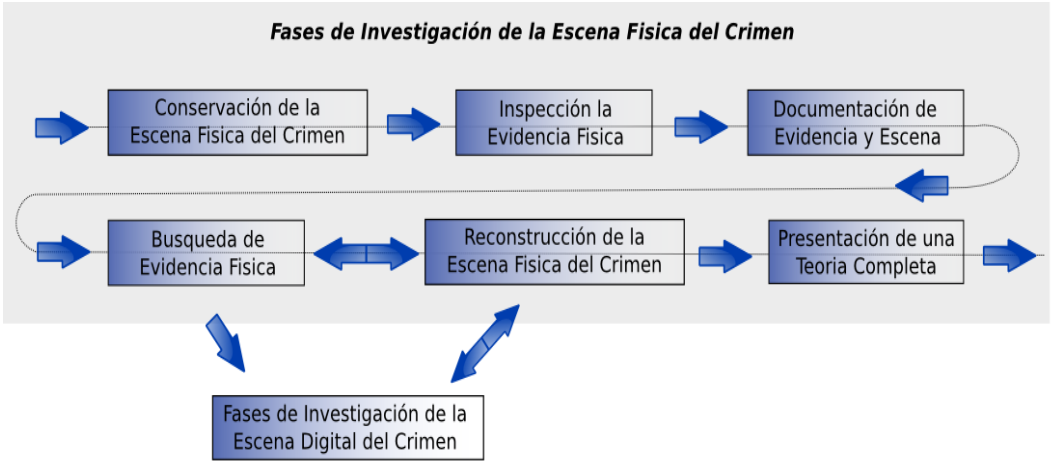

Figura 2.4: Fases de la investigación física de la escena del crimen

1. Fase de Conservación (Preservation Phase): su objetivo es conservar la escena del crimen para que la evidencia pueda ser identificada y recolectada posteriormente por personal capacitado en la identificación de evidencias digitales.

2. Fase de Inspección (Survey Phase): requiere que un investigador recorra la escena física del delito e identifique elementos de evidencia física.

3. Fase de Documentación (Documentation Phase): que incluye tomar fotografías y vídeos de la escena del delito y de la evidencia física. El objetivo es capturar tanta información como sea posible, de modo que el esquema y los detalles importantes de la escena del crimen sean conservados y grabados.

4. Fase de búsqueda y recolección (Search and Collection Phase): contiene una búsqueda y recolección en profundidad de la escena de modo que se identifican evidencias físicas adicionales y se establecen los caminos para comenzar la investigación digital.

5. Fase de Reconstrucción (Reconstruction Phase): incluye organizar los resultados del análisis realizado, usándolos para desarrollar una teoría sobre el incidente.

6. Fase de Presentación (Presentation Phase): presenta la evidencia digital y física en un juicio o ante la dirección de una empresa.

Fases de Investigación de la Escena Digital del Delito

El objetivo de estas fases es recolectar y analizar la evidencia digital que se obtuvo durante la fase de investigación física y a través de otras fuentes. Incluye fases similares a las de la investigación física, pero haciendo foco en la evidencia digital. Sus fases internas son las siguientes:

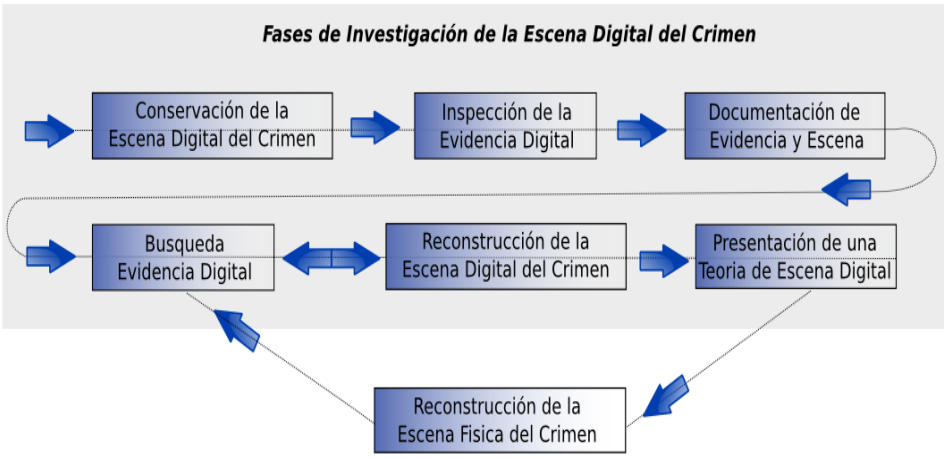

Figura 2.5: Fases de la investigación de la escena digital del delito

1. Fase de conservación (Preservation Phase): se conserva la escena digital del delito para que la evidencia pueda ser analizada posteriormente.

2. Fase de Inspección (Survey Phase): en la que el investigador transfiere los datos relevantes de una jurisdicción que está fuera del control físico o administrativo del investigador, a una posición controlada.

3. Fase de Documentación (Documentation Phase): se destina a documentar la evidencia digital encontrada. Esta información soporta la fase de presentación.

4. Fase de Búsqueda y Recolección (Search and Collection Phase): en esta fase se realiza un análisis profundo de la evidencia digital. Se usan herramientas de software para revelar ficheros ocultos, borrados, corruptos, lineas de tiempo, etc.

5. Fase de reconstrucción (Reconstruction Phase): durante esta etapa se ubican las piezas del rompecabezas para desarrollar una hipótesis de investigación.

6. Fase de Presentación (Presentation Phase): consiste en presentar la evidencia digital encontrada y anexarla a la evidencia física encontrada.

Fase de revisión

La investigación entera es revisada y se definen las áreas de mejora.

2.1.5. Baryamureeba V. and Tushabe, F. (2004). "The Enhanced Digital Investigation Process Model", DFRWS.

Tushabe ha sugerido modificaciones al trabajo de Carrier, B. y Spafford, E.[Carrier and Spafford, 2003]; las modificaciones descriptas en el documento de estos autores[V. and Tushabe, 2004] llamado "The Enhanced Digital Investigation Process Model" agregan dos nuevas fases "Trace back" y "Dynamite" con el objetivo de separar la investigación en la escena primaria del crimen (La computadora) y la escena secundaria (correspondiente al lugar físico del hecho). De esta forma se puede reconstruir ambas escenas en forma concurrente evitando inconsistencias.

El siguiente gráfico muestra las cinco fases principales de este modelo

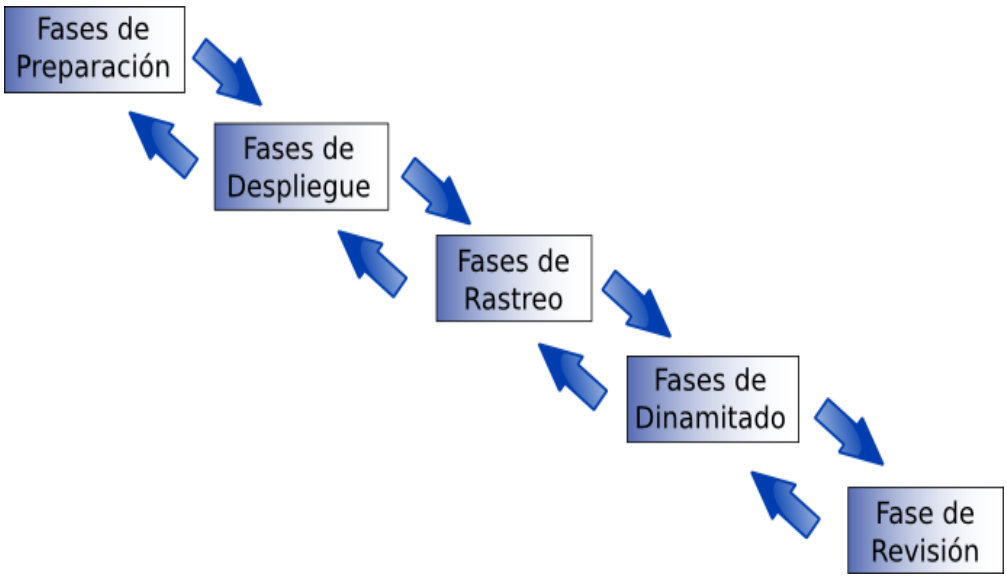

Figura 2.6: Fases de la investigación según Baryamureeba y Tushabe

Fases de Preparación (Readiness)

Su objetivo es garantizar que las operaciones e infraestructura son capaces de soportar la investigación. Sus dos componentes son:

1. Fase de preparación de operaciones (Operations Readiness phase): asegura que los investigadores están capacitados y equipados para manejar un incidente cuando ocurre.

2. Fase de preparación de infraestructura (Infrastructure readiness phase): asegura que la infraestructura disponible es suficiente para tratar con los incidentes del caso. Por ejemplo, cámaras fotográficas, material de protección y transporte de hardware, etc.

Fases de despliegue (Deployment)

Proveen un mecanismo para detectar y confirmar un delito. Se ejecutan en el lugar donde se detectó el delito y consta de cinco fases:

1. Fase de Detección y Notificación (Detection and Notification): cuando un incidente se detecta y se notifica a las personas apropiadas.

2. Fase de Investigación Física de la escena del delito (Physical Crime Scene Investigation): cuando se examina la escena física del delito y se identifican las potenciales evidencias digitales.

3. Fase de investigación Digital de la escena del delito (Digital Crime Scene investigation): cuando se realiza un examen de la escena y se extraen evidencias con la correspondiente estimación de impacto o daño causado al manipular el sistema en búsqueda de estas evidencias digitales.

4. Fase de Confirmación (Confirmation): cuando el incidente es confirmado y se obtiene autorización legal para efectuar una investigación en profundidad.

5. Fase de informe (Submission): supone presentar las pruebas físicas y digitales a las entidades legales o la dirección corporativa correspondientes.

Fases de Hipótesis (TraceBack)

En estas fases se intenta reconstruir los hechos cometidos en la escena física del delito de forma que se pueda identificar a los dispositivos que se usaron para cometer el acto. Consta de dos fases:

1. Investigación digital de la escena del delito (Digital Crime Scene Investigation): se define una primera hipótesis con las pistas obtenidas en fases anteriores. Por ejemplo, si se tiene una dirección IP sospechosa en el sistema se puede rastrear su origen buscando por internet.

2. Fase de Autorización (Authorization): se obtiene autorización de las entidades locales para permitir investigaciones más detalladas y acceder a más información.

Fases Dinamita (Dynamite)

Estas fases investigan la hipótesis elaborada previamente. El objetivo de recopilar y analizar los elementos que se encontraron en la fase previa es disponer de más evidencias y poder asegurar que el delito ocurrió allí y/o encontrar posibles responsables del hecho. Consta de cuatro fases:

1. Fase de Investigación Física de la escena del delito (Physical Crime Scene Investigation phase): se examina de nuevo la escena física bajo el punto de vista de la hipótesis inicial buscando nuevas evidencias digitales.

2. Fase de Investigación Digital de la escena del delito (Digital crime scene investigation phase): se examina la evidencia digital en busca de pruebas del incidente y permite hacer una estimación del momento en que ocurrió el incidente.

3. Fase de Reconstrucción (Reconstruction phase): busca reconstruir todas las piezas del rompecabezas digital para identificar las hipótesis más probables.

4. Fase de Comunicación (Communication phase): consiste en elaborar la presentación de las interpretaciones y conclusiones finales sobre la evidencia física y digital que ha sido investigada por un juicio o por una empresa.

Fase de Revisión (Review)

La investigación entera es revisada y se definen las áreas de mejora.

2.2. Términos y conceptos de la practica pericial

Esta sección abordará los conceptos de la practica pericial que serán de particular interés para la comprensión de este trabajo.

2.2.1. Criminalística y Criminología

Estos términos son relevantes para el desarrollo y usualmente confundidos en su significado o utilización, es por esta razón que a continuación se citan las definiciones de la Real Academia Española sobre los mismos:

Criminalística: (Del al. Kriminalistik). Estudio de los indicios de un hecho criminal con el fin de determinar todos los datos posibles relativos a la víctima o a las circunstancias del crimen.

Criminología: (Del lat. crimen, -ĭnis, crimen, y -logía). Ciencia social que estudia las causas y circunstancias de los distintos delitos, la personalidad de los delincuentes y el tratamiento adecuado para su represión.

Estas definiciones muestran la clara diferencia entre estos conceptos, ya que la criminalística es una disciplina basada en técnicas y procedimientos de rigor científico que persigue la reconstrucción de hechos delictivos estableciendo sus actores y pruebas; en contra-parte la criminología estudia desde el aspecto social interdisciplinario las causas de un crimen, con soporte de la medicina, psicología, sociología y antropología entre otras disciplinas.

2.2.2. Prueba

Basándonos en el texto de Darahuge y Arellano González [Darahuge, 2012][2], y en el contexto de este estudio se puede clasificar al termino prueba de diferentes maneras, con un enfoque amplio o restringido.

En sentido amplio, para el derecho procesal, la prueba es el subconjunto de actos y elementos interrelacionados cuya finalidad es cumplir un objetivo determinado. En resumen se logra definir a la prueba como un medio de verificación de las proposiciones que los litigantes formulan en un juicio.

Para el enfoque restringido procedo a citar la definición de Carnelutti adoptando un concepto de prueba como medio en sentido instrumental, indicando que probar significa determinar o fijar formalmente los hechos mismos mediante procedimientos determinados.

Para complementar los conceptos de base vinculados al análisis de este documento detallaré una clasificación del termino de prueba con enfoque procesal en el ámbito jurídico, la misma divide los tipos en "Prueba Documental Clásica" y "Prueba Documenta Informática".

La primera, como prueba documental básica, es aquella que se constituye mediante documentos. Un documento se comprende como una cosa con función representativa de hechos, esta definición puede verse ampliada según diferentes autores como:

- Chiovenda[Chiovenda, 1940]: toda representación material destinada e idónea para reproducir cierta manifestación del pensamiento.
- Devis Echandia[Echandia, 1969]: todo objeto o producto de un acto humano que represente a otro hecho u objeto.
- Kielmanovich[Kielmanovich, 2001]: todo objeto material originado por una acto humano, susceptible de representar por si mismo y para el futuro un hecho o una serie de hechos percibidos en el momento de su concepción.

La prueba documental o clásica puede clasificarse de la siguiente forma:

[2]Correspondiente al Capitulo 1, página 16

1. Según su condición material

    a) Bibliográfica: Compuesta por escritos ya sean manuscritos o impresos, suelen estar respaldados por pruebas periciales documentologicas, documentoscopicas o caligráficas.

    b) Foliográfica: En relación a gráficos, representaciones de lugares, esquemas cuya prueba asociada depende de su tipo y en función del mismo se puede incluir a agrimensores, arquitectos, ingenieros y otros expertos del campo especifico.

    c) Pictográfica: Se asocia a fotografía, vídeo y sonido, en general de fuentes no digitales.

2. Según su integración al proceso

    a) Aportados por el actor

    b) Aportados por la contra-parte

    c) Aportados por tercero

3. Según su autoría

    a) Generados por quien los acompaña

    b) Generados por la contra-parte

    c) Generados por terceros

El segundo tipo de prueba, conocida como prueba documental informática, deriva de la prueba documental clásica pero difiere en su soporte. Como se detalló previamente, la prueba documental clásica se respalda en medios físicos como el papel o contenedores analógicos como películas o cintas; sin embargo la prueba documental informática esta identificada por la digitalización de sus componentes en conjunto con los medios adecuados para esto.

Sus características propias son

- Principio de identidad atípico: a diferencia de la prueba clásica, la copia de un documento digital bit a bit es idéntica al original haciendo que no sea posible distinguirlos.

- Posibilidad de modificación por medios locales o remotos, accidentales, culposos o dolosos.

- Divisibilidad del documento: un documento digital puede ser parcialmente alterado por esta razón pueden existir impugnaciones parciales de un mensaje.

- La prueba documental informática lleva implícita la prueba pericial informática forense, para el caso de ser negativa. Es frecuente su convalidación mediante pruebas de informes como información del ISP[3] o proveedores de mensajería o correo. En algunos casos, en función de la jurisdicción internacional, se puede dar respaldo a la prueba mediante la firma digital que confiere al documento electrónico la misma credibilidad que el documento público clásico, permitiendo que se lo trate con las mismas condiciones legales y procesales.

2.2.3. Prueba anticipada

La prueba anticipada, según Darahuge y Arellano González[Darahuge, 2012][4], esta constituida por aquel material relevado antes de la presentación de una demanda, sin intervención judicial; ya sea para ser utilizado en la demanda o para una instancia de negociación previa o extrajudicial. Cabe destacar que para su utilización posterior se requiere tomar los siguientes recaudos:

1. Recolectar información personal o pública

2. La misma debe estar certificada ante escribano público

3. Para la prueba informática, debe estar autenticada mediante un código confiable de digesto matemático o hash

[3]ISP: Internet Service Provider, o Proveedor de Servicios de Internet
[4]Correspondiente al capitulo 2, página 24

4. Su correspondiente cadena de custodia

Este tipo de prueba consta de las siguientes características:

- Instrumentalidad: No tienen finalidad en si misma, sino que se obtienen con el fin de preservar la prueba, para ser utilizadas posteriormente en el proceso en función de los argumentos de cada una de las partes. No son medidas autónomas, porque su razón esta sujeta al contexto del fin pretendido.

- Sumariedad: La superficialidad del conocimiento judicial, por parte del tribunal al que le es requerida la medida, ya que no pueden establecerse con certeza los requisitos antes detallados, los que en todos los casos dependerán de una evaluación somera y en condiciones de incerteza, por parte de quien deba proveerla.

- Provisionalidad: Difieren de las medidas cautelares dado que no son definitivas y terminan con la sentencia consentida y ejecutada, mientras que la recolección efectuada constituye un hecho definitivo y difícil de repetir. A pesar de esto, son provisionales, debido a que generalmente requieren una prueba de informes complementaria y/o prueba pericial en su subsidio.

- Perennis in iudicium: Aunque son susceptibles de revisión por prueba de informes y pericial, no debería modificarse durante su empleo judicial, ya que en dicha inalterabilidad se funda gran parte de su poder probatorio. No caducan con el tiempo, porque una vez admitidas como elemento probatorio conservaran este carácter durante todo el desarrollo del litigio.

- Reserva: Por su necesidad de concesión *inaudita altera pars*, preservando los derechos procesales establecidos para estos casos; de lo contrario la medida carece de eficacia.

Es una acción judicial con características propias, cautelares en el sentido de preservación de la prueba con el fin de asegurar su sobre-vida durante el proceso. Aunque

carece de autonomía con respecto del proceso principal cuya eficacia garantiza, parece mantenerla al menos en el ámbito conceptual, anticipando la tutela del derecho invocado y la pretensión que funda al proceso en ciernes.

La prueba anticipada se asocia a los siguientes requisitos doctrinarios:

- Verosimilitud del derecho: Para que se conceda no es necesario un estudio exhaustivo y profundo de la materia controvertida en el proceso principal, sino de un conocimiento superficial; la certeza aparecerá a posteriori en la sentencia. No se requiere prueba plena y concluyente, sino un acreditamiento convincente para que se ordene la providencia solicitada.

- Peligro en la demora: Aunque en el caso de la prueba documental informática, el riesgo de su modificación, adulteración o eliminación es prácticamente evidente, en razón de su debilidad manifiesta frente a las acciones dolosas o culposas de los actores físicos, lógicos o humanos con los que se relaciona, siempre es necesario fundar con claridad este riesgo.

- Preservación de la privacidad: Cuanto menor sea la verosimilitud del derecho invocado, tanto mayor es la necesidad de asegurar este requisito. En el derecho penal, se justifica claramente por la doctrina del árbol envenenado. En el resto de los fueros, siempre es posible que como resultado de esta medida se produzcan violaciones al derecho a la privacidad del futuro demandado.

2.2.4. Cadena de custodia

El concepto de "Cadena de Custodia" constituye el conjunto de procedimientos formales realizados dentro de un proceso penal respecto al indicio. Estando determinado por actos y procesos mediante los cuales el Estado asegura la imparcialidad, la ecuanimidad, la resolución fundada a través de la determinación de la norma aplicada al caso concreto y la valoración de todos los elementos expuestos en la causa. Des esta forma, representa el respeto del Estado ante cumplimiento a las normas legales y a las garantías del debido proceso.

La prueba documental informática consiste en indicios digitalizados, codificados y resguardados en un contenedor digital especifico, a fin que comprende la información almacenada o en desplazamiento por un medio especifico. Para el caso en cuestión se debe diferenciar al objeto contenedor como los discos magnéticos u ópticos de su contenido que conforma la información real.

Ante este planteo se puede definir como:

1. Información: al conocimiento asociado a un objeto o hecho especifico, susceptible de almacenamiento y codificación.

2. Objeto: Conjunto físicamente determinable y lógicamente definible.

La información puede encontrarse en los siguientes estados:

1. Almacenada: la información en este estado se encuentra estática y permanece en un medio (primario, secundario o terciario) a la espera de ser accedida. Suele ser el estado mas utilizado durante el proceso de recolección y permite que se lo acceda de forma local o remota según cada caso.

2. En tránsito o desplazamiento: comprende a aquellos datos que se encuentran en transito sobre un medio físico, como por ejemplo cables de cobre, fibra óptica, ondas, láser, etc. Esta información debe ser interceptada para su recolección, con los recaudos legales correspondientes, como ejemplo práctico aplican al caso las comunicaciones telefónicas.

3. En proceso: corresponde a la captura de datos que se encuentran siendo procesados en concurrencia con la recolección de la prueba. Este es un estado complejo para la recolección y asociado a las circunstancias del escenario de relevamiento y la decisión del perito, ya que podría perderse información en la operación. Como caso práctico referenciaré a la captura de datos en memoria RAM[5] o la intercepción las teclas presionadas en el teclado del dispositivo por medios remotos. Se observa que el equipo a peritar debe estar en funcionamiento.

[5]RAM: Random Access Memory o Memoria de acceso aleatorio.

Otro concepto significativo vinculado a la prueba documental informática es su validez, la misma esta limitada a su inserción como elemento pertinente y conducente de la argumentación presentada como sustento para la pretensión jurídica manifestada.

Al mismo tiempo existe una característica particular y propia, debido a la naturaleza de la información un bit no es similar a otro sino que es exactamente igual, generando que la información copiada bit a bit sea imposible de diferenciarse de la información original; dicha característica constituye una ventaja sustancial para la cadena de custodia ya que se pueden generar una ilimitada cantidad de copias fieles y exactas de la evidencia sin degradación de la misma. Otro aspecto relevante que surge del concepto anterior es la posibilidad de que los peritos trabajen sobre copias de la evidencia original sin afectar su capacidad para obtener resultados en el proceso de análisis y manteniendo su validez como elemento probatorio.

La cadena informático forense cumple con los requisitos procesalmente exigibles asegurando los siguientes aspectos:

1. Trazabilidad

    a) Humana: determinación de responsabilidades en la manipulación de la prueba desde su detección y recolección hasta su disposición final.

    b) Física: incluyendo la totalidad de los equipos locales o remotos involucrados en la tareas, sean estos de almacenamiento, procesamiento o comunicaciones.

    c) Lógica: descripción y modelización de las estructuras de distribución de la información accedida y resguardada.

2. Confiabilidad

    a) Garantizando integridad, autenticidad, confidencialidad y no repudio.

La cadena de custodia aporta a la práctica informático forense cuando el profesional se encuentre en condiciones de demostrar integridad material y formal desde los siguientes puntos de vista:

1. Validez técnica informática: abarca el control, revisión y auditoría de las operaciones técnicas informáticas que se han realizado desde el momento de la identificación de la prueba documental recolectada. Para esto se debe incluir a la totalidad de los recursos que directa o indirectamente estén asociados al proceso ya sean edilicios, instrumentales, lógicos o humanos.

2. Validación técnica criminalistica: Cubre el control, revisión y auditoría de las operaciones técnicas criminalisticas que se han realizado desde el momento de la intervención de los diferentes actores involucrados en las tareas periciales. Temporalmente se extenderá mas allá de las actividades de validez técnica informática ya que incluirá a las interacciones multi y trans-diciplinarias de los peritos. Al comprobarse que los procedimientos criminalisticos utilizados mediante metodología criminalistica y convalidado los mismos, la prueba indiciaria informática recolectada podrá ser considerada como valida para su uso pericial, de no ser así deberá ser descartada.

3. Validación técnica legal: Surge del análisis de las validaciones previamente enumeradas, las mismas podrán ser realizadas independientemente y sin orden previsto, pero la validación técnico legal solo procederá cuando las anteriores tengan resultados positivos. En síntesis, será un análisis integrador de la prueba indiciaria informática recolectada y disponible para determinar su confiabilidad probatoria legal. Implica el control, revisión y cotejo de los mecanismos utilizados desde el punto de vista legal, acorde con la normativa, doctrina, jurisprudencia vigente, y objeto jurídico principal a preservar mediante la intervención judicial del debido proceso. Su violación implica la inmediata nulidad de la prueba recolectada.

La cadena de custodia forma un elemento que permite asegurar la confiabilidad de la información recolectada, implica su trazabilidad estricta pero no protege por si sola el derecho de la privacidad. En síntesis, demuestra que la prueba puede ser recolectada metodológica y procesalmente desde su origen hasta el destino final, pero esto no garantiza la legitimidad o legalidad del proceso de recolección autorizado. Se

podría estar en presencia de una cadena de custodia correctamente implementada desde lo criminalistico, técnico y procesal pero cuyo origen se encuentre relacionado con una acción ilegal como la falta de orden de allanamiento, un secuestro previo de prueba documental o una recolección ilegitima por no estar determinada específicamente o excediendo lo solicitado.

2.2.5. Participación del perito en el proceso

La participación del perito en un proceso judicial esta limitada estrictamente a su condición de testigo experto en un área especifica, por esta razón es fundamental que se abstenga de emitir juicios personales, determinar autorias o investigar mas allá de su área de especialización sujeta al alcance de la pericia solicitada.

Su aporte debe basarse en consideraciones científicas, tecnológicas y técnicas obtenidas mediante métodos de análisis de la prueba indiciaria sujetos a cada disciplina criminalística; por lo que en general se observaran métodos que se soportan en comparaciones. Como resultado de este proceso de comparación, cotejo, análisis y registro de resultados el perito entregará un informe imparcial que se utilizará como elemento de soporte a la decisión del juez que ha solicitado la pericia.

Es importante destacar que los resultados periciales sujetan su credibilidad a la relación con la ciencia y metodología que brinda el soporte; un ejemplo concreto es la confiabilidad que tiene la identidad genética que provee un análisis de ADN.

La expectativa sobre la participación del perito en el proceso puede definirse en términos generales con la declaración del Código Procesal Civil de la Nación Argentina:

> "Sección 6 - Prueba de peritos. Procedencia, art. 457. - Sera admisible la prueba pericial cuando la apreciación de los hechos controvertidos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada"

Dicha declaración se encuentra en concordancia con el Código Procesal de la Nación Argentina que establece:

> "Capitulo V – Peritos. Facultad de ordenar las pericias, art. 253.- El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica".

Para la ley 18.345 (Ley De Organización Y Procedimiento De La Justicia Nacional Del Trabajo) citaré:

> "Prueba pericial, art. 91 – Si la apreciación de los hechos controvertidos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada, se podrá posponer prueba de peritos, indicando los puntos sobre los cuales habrá que expedirse. Los peritos serán nombrados de oficio en todos los casos y su número podrá variar de uno a tres a criterio del juez y de acuerdo con la índole o monto del asunto, circunstancias que también se tomaran en cuenta para fijar el plazo dentro del cual deberán expedirse. Únicamente en los casos excepcionales los peritos podrán pedir y el juez ordenar que, con carácter previo, la o las partes interesadas depositen la suma que se fija para los gastos de las diligencias. Los peritos podrán ser recusados con causa en el plazo de tres días posteriores a su designación"

2.3. Características tecnológicas de los dispositivos móviles

Los dispositivos móviles cuentan con diversas características propias que los diferencian del resto de los equipos informáticos por su naturaleza y las particularidades de su utilización.

Un gran porcentaje de dispositivos móviles corresponden a teléfonos celulares avanzados o inteligentes, los mismos han incluido nuevo hardware y extendido sus capacidades a fin de proveer funcionalidades que exceden la comunicación de voz que fuera su

fin original. En este contexto, se observa que en la actualidad los dispositivos móviles acompañan de manera permanente las actividades diarias de gran cantidad de personas constituyendo un repositorio de información especifica y de contexto.

En términos generales se puede identificar algunos componentes comunes o de existencia frecuente en este tipo de dispositivos, como son:

- Placa central (Microprocesador, memorias)
- Memoria de almacenamiento
- Antena de telefonía
- Antena Wifi
- Antena NFC[6]
- Bluetooth[7]
- Conexiones por puerto infrarrojo, IrDA[8]
- Pantalla
- Teclado
- Micrófono
- Altavoz
- Batería
- Puertos de comunicación por cable
- Sensores (acelerómetros, brújula, giroscopios)

[6]NFC: Near Field Communication o Comunicación de campo cercano, es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Los estándares de NFC cubren protocolos de comunicación y formatos de intercambio de datos.

[7]Bluetooth: es una tecnología de comunicación entre dispositivos de corto alcance.

[8]IrDA: Infrared Data Association o Asociación de Datos Infra-rojos, define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojos.

- Sistemas de posicionamiento GPS[9]
- Cámaras

Los equipos móviles cuentan con CPUs[10] análogas a las de una computadora convencional, pero la industria ha trabajado para desarrollar componentes que se desempeñen mejor con las limitaciones propias del formato de estos dispositivos, es común en la actualidad encontrar dispositivos móviles con procesadores de bajo consumo, multi-nucleo y con arquitecturas particulares como ARM, Atom o Fusion.

En cuanto a memoria, se observa una composición del uso de memoria RAM[11], ROM[12] y de almacenamiento interno persistente; esto se debe a que algunos dispositivos almacenan su sistema operativo y/o programas en una memoria interna no removible de tipo flash, adicionalmente la memoria con capacidad de re-escritura es utilizada para el almacenamiento de información del usurario (contactos, mensajes, etc.).

La capacidad de transmisión de datos ha sido clave en la evolución de dispositivos móviles ampliando sus funcionalidades mas allá de lo esperado. Existen diversas tecnologías involucradas, aquí se presentan las tecnologías inalámbricas mas frecuentes en los dispositivos móviles actuales:

Infrarrojo o IrDA: Es un estándar físico de transmisión y recepción de datos por medio de rayos infrarrojos. Esta tecnología se basa en los rayos que viajan a través del espectro infrarrojo.

Esta tecnología es limitada por que la longitud de las ondas es pequeña y por esta razón no puede cubrir aéreas amplias. También se encuentra limitada porque el enlace entre los dos puntos debe realizarse con una línea de vista y no pueden existir obstáculos ya que esto genera la pérdida de la conexión.

Bluetooth: Es el estándar 802.15 de la IEEE[13] de comunicación, que facilita la

[9]Global Positioning System o Sistema de Posicionamiento Global. Es un sistema global de navegación por satélite que permite localizar con precisión un dispositivo en cualquier lugar del mundo.
[10]Unidades Centrales de Procesamiento
[11]RAM: Random Access Memory o Memoria de acceso aleatorio.
[12]ROM: Read Only Memory o Memoria de Solo Lectura.
[13]IEEE: Institute of Electrical and Electronics Engineers o Instituto de Ingeniería Eléctrica y Electrónica

creación de Redes Inalámbricas de Área Personal o WPAN, permitiendo la trasmisión de datos y voz, utilizando un enlace de radiofrecuencia.

Esta tecnología es la más utilizada en los dispositivos móviles, porque permite la creación de redes entre los diferentes dispositivos y la velocidad de trasmisión es bastante alta, además de la mayor cobertura que ofrece por la banda que utiliza para enviar y recibir los datos.

Wi-Fi o Wireless Ethernet Alliance: Es el estándar 802.11 de tecnologías de comunicación inalámbrica que utiliza ondas que viajan por el espectro electromagnético.

Esta tecnología es la más utilizada para la creación de Redes Inalámbricas de Área Local o WLAN, una de sus características más importantes es la velocidad de transmisión de la información y la cobertura que ofrece.

En cuanto a los teléfonos inteligentes esta tecnología ha sido implementada y permite la conexión y navegación en internet utilizando la tecnología WiFi.

NFC o Near Field Communication: Es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Los estándares de NFC cubren protocolos de comunicación y formatos de intercambio de datos, y están basados en ISO 14443 (RFID, radio-frequency identification) y FeliCa. Los estándares incluyen ISO/IEC 18092[14] y los definidos por el NFC Forum, fundado en 2004 por Nokia, Philips y Sony, y que hoy suma más de 160 miembros.

El siguiente gráfico muestra las características de transferencia y alcance de diferentes tecnologías de comunicación inalámbrica

[14]ISO: International Organization for Standardization o Organización Internacional de Normalización. IEC: International Electrotechnical Commission o Comisión Internacional Electrotécnica.

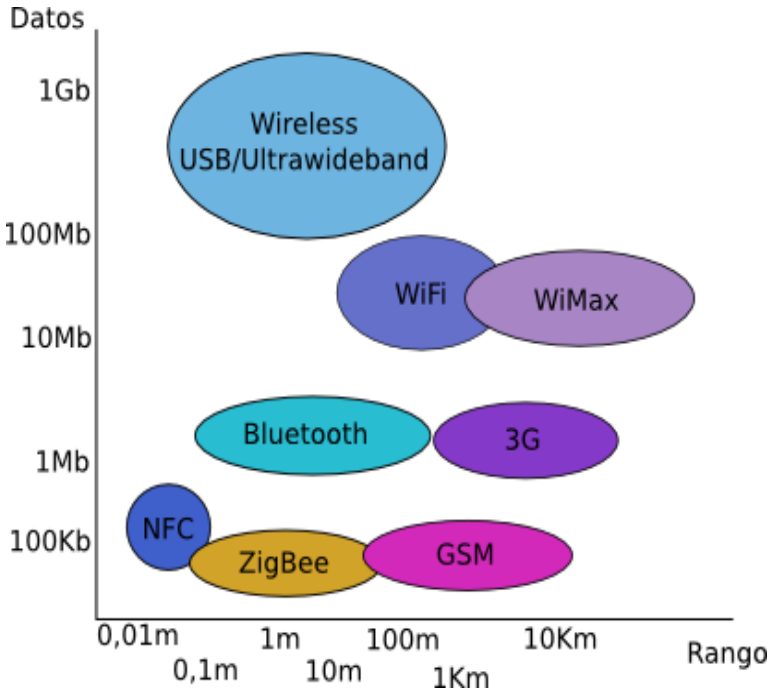

Figura 2.7: Características de transferencia y alcance de tecnologías inalámbricas

2.4. Orígenes y características del Sistema Operativo Android

Android es un sistema operativo Open Source, basado en Linux y diseñado para dispositivos móviles con pantalla táctil; su creación se origina en la compañía Android Inc. que posteriormente fue adquirida por Google. Desde el año 2007 ha sido el sistema de referencia para el "Open Handset Alliance" que agrupa a diferentes empresas de telefonía, software y hardware para la definición de estándares del sector. Este sistema operativo comenzó a comercializarse con equipos en el año 2008 y su importancia radica en el gran impacto y rápida adopción que ha tenido en el mercado actual, y la gran cantidad de aplicaciones disponibles para esta plataforma en conjunto con la facilidad de acceso y comercialización de las mismas.

2.5. Arquitectura y diseño del sistema operativo Android

El sistema operativo para dispositivos móviles Android esta basado en una arquitectura de pila compuesta de múltiples capas, cada una de ellas contribuye a facilitar el acceso a funcionalidades comunes manteniendo un buen nivel de abstracción con el resto del entorno.

El siguiente gráfico muestra las diferentes capas que componen la arquitectura y los componentes principales de cada una de ellas:

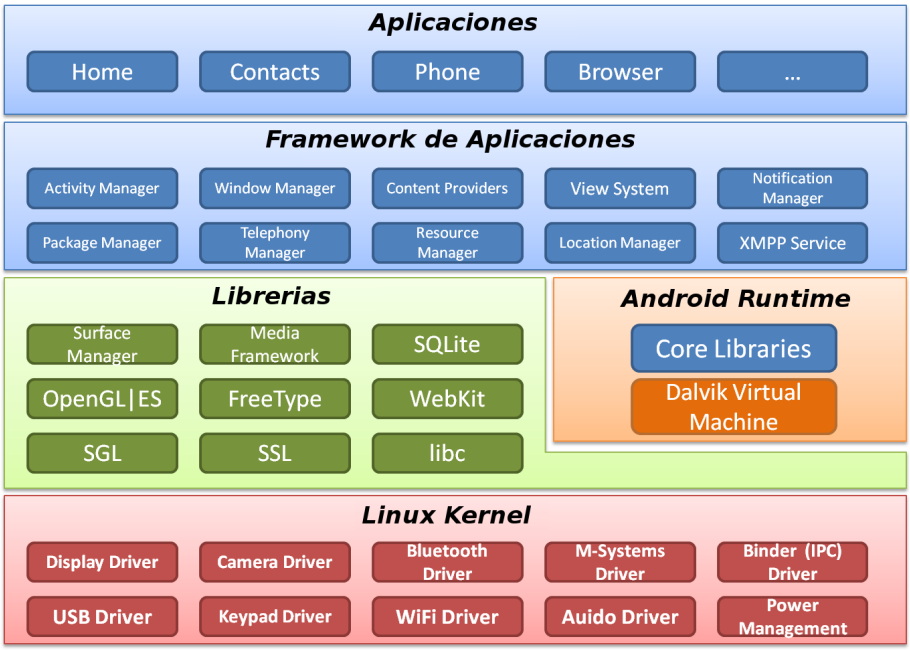

Figura 2.8: Componentes del sistema operativo Android

En las siguientes secciones se detallará las funcionalidades contenidas en cada capa de la arquitectura adoptada.

2.5.1. Linux Kernel

Corresponde al núcleo del sistema operativo basado en la versión 2.6 de Linux, esta capa contendrá las funcionalidades básicas del sistema mas el conjunto de drivers para

el hardware especifico de la plataforma. Dada la naturaleza y finalidad de Android se observa que esta capa ha sido adaptada al hardware disponible en plataformas móviles.

Las funciones principales o primarias del núcleo serán, al igual que el el sistema Linux convencional, la gestión de recursos básicos del entorno como memoria, gestión de procesos, energía entre otros mientras que mediante drivers se administrará el acceso al hardware, como por ejemplo, dispositivos de comunicación (modems GPRS/GSM[15], redes WiFi, bluetooth[16]), cámaras, sensores, etc.

Bajo este modelo, la capa de kernel provee abstracción para el acceso a hardware evitando que el código de las capas superiores acceda directamente al mismo, de hecho, las aplicaciones del nivel superior interactúan con las librerías de las capas intermedias para acceder al hardware desconociendo los detalle técnicos del manejo del mismo que descansan en las implementación de drivers y lógica de gestión del kernel.

2.5.2. Librerías

Esta capa corresponde a las librerías nativas que se comunican directamente con el kernel. Usualmente están desarrolladas en C o C++[17] y compiladas para el hardware especifico del dispositivo móvil por cada proveedor o fabricante.

Estas librerías proveen funcionalidades de uso común a las capas superiores permitiendo mantener la abstracción del acceso a la capa inferior y reduciendo la necesidad de que las aplicaciones implementen dichas funciones. Como se puede observar en el cuadro de arquitectura anterior, muchas de estas librerías corresponden a utilidades tan genéricas como: OpenGL[18], SSL[19], LibC[20], SQLite[21], etc.

[15]GPRS/GSM: General Packet Radio Service/Global System for Mobile communications o Radio Servicio General de Paquetes/Sistema Global para Móviles; ambas son tecnologías de comunicación inalámbrica utilizadas por dispositivos móviles de tipo celular.
[16]Bluetooth: es una tecnología de comunicación entre dispositivos de corto alcance.
[17]C y C++: Lenguajes de programación
[18]Manejo del motor gráfico
[19]Cifrado de comunicaciones
[20]Librería de funciones estándar de C
[21]Motor de base de datos

2.5.3. Android Runtime (Entorno de ejecución Android)

El entorno de ejecución de Android se basa en una maquina virtual(VM) denominada "Dalvik", la misma ha sido optimizada para su uso en dispositivos de recursos limitados; por esa razón se observan características particulares como las siguientes:

- Cada aplicación se ejecuta como un proceso independiente del S.O, con su propia instancia de la maquina virtual.
- Ejecuta archivos de tipo Dalvik (con extensión .dex) optimizados para el uso reducido de memoria.
- Los procesos de gestión multi-thread y de memoria a bajo nivel se delegan al sistema operativo.
- El runtime contiene las "Core Libraries" que contiene la mayoría de las librerías disponibles en Java.
- Dalvik no es compatible con java byte code. Es importante aclarar que el lenguaje que se utiliza para la programación de aplicaciones para esta VM es java, pero el código compilado resultante no es "byte code" estándar.

La maquina virtual de Dalvik acepta "Dalvik byte code" usualmente almacenado en archivos de extensión "dex". Dichos archivos son creados con la herramienta "dxtool" incluida en el sistema Android, esta herramienta toma archivos de clases java creados por el compilador como entrada. En el siguiente gráfico se representa la relación entre estos componentes:

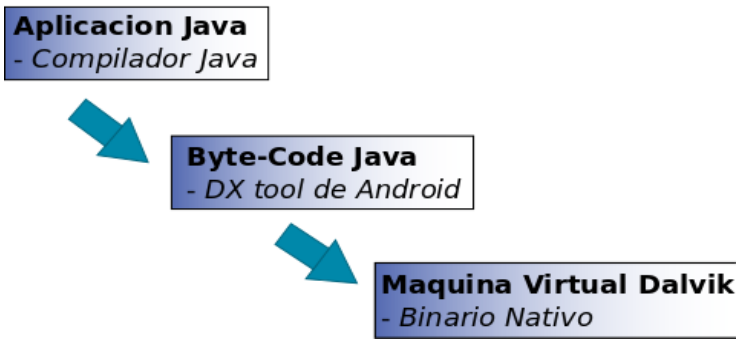

Figura 2.9: Relación de componentes en Dalvik VM

Su proceso de funcionamiento se comienza con la ejecución de init en el sistema operativo, este proceso que es el raíz o padre invocará a los "Daemons" del sistema y hará una bifurcación (Fork) del proceso "zygote". El proceso "zygote" tendrá la finalidad de crear una instancia de la maquina virtual de Dalvik y los servicios de base o "core services". Una vez realizado esto se establece un canal de lectura para notificarse de nuevas aplicaciones.

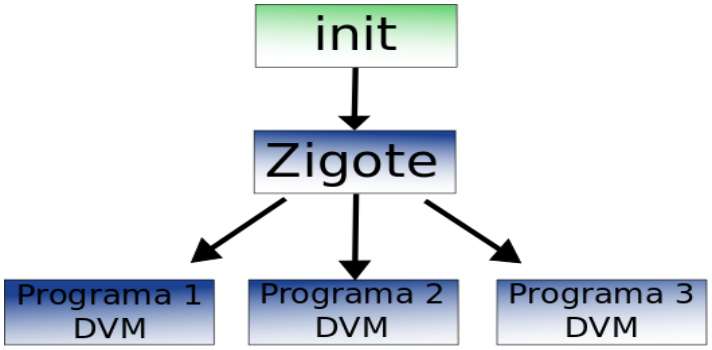

Figura 2.10: Funcionamiento del proceso de init en Dalvik VM

Al iniciarse una aplicación, ésta envía un mensaje al proceso "zigote", el cual contacta al servicio "Android Activity Manager", que hará una bifurcación de proceso y ejecutará la clase java en cuestión. De esta forma los procesos comparten una copia de la DVM (Dalvik Virtual Manager) creado por "zigote" y evitan duplicar las páginas de la DVM.

Las páginas de la DVM son de tipo COW (Copy On Write, o copia ante escritura) y de solo lectura, de esta forma cuando una aplicación intenta escribirla, se obtiene una copia local vinculada exclusivamente a ese proceso para que opere de forma desacoplada al original y otros procesos.

2.5.4. Framework de Aplicaciones

El Framework o entorno de aplicaciones de Android facilita una serie de componentes para acceder a las funcionalidades provistas por el sistema y otras aplicaciones, dando oportunidad a la reutilización de los mismos. Las aplicaciones pueden publicar sus capacidades para que otras puedan hacer uso de las mismas, siempre que los niveles

de seguridad lo permitan.

Algunos de estos componentes son:

- Activity Manager - Administra el ciclo de vida de las aplicaciones y facilita el acceso a ellas.
- Windows Manager - Organiza la información mostrada en pantalla. Creará la áreas de la pantalla que serán utilizadas por las actividades de las aplicaciones en ejecución.
- Content Provider - Este componente encapsula datos para que sean compartidos entre las aplicaciones y de esta manera nos permite gestionar el control de acceso a dicha información.
- Views - Son componentes que nos permiten construir interfaces de usuario donde se ubicarán los widgets[22] que utilizará la aplicación, como pueden ser botones, cuadros de entrada de texto, combos, listas o elementos complejos como un visor de mapas, editores de texto o componentes de HTML[23].
- Notification Manager – Facilita el acceso a los servicios que permiten notificar al usuario mediante llamadas de alerta en la barra de estado de la interfaz gráfica; adicionalmente puede utilizar otras características como la ejecución de sonido o vibración del dispositivo para incrementar la efectividad en la notificación.
- Package Manager - Corresponde a la librería que gestiona la instalación de aplicaciones y provee información sobre los paquetes instalados en el dispositivo, además de gestionar la instalación de nuevos paquetes. Las aplicaciones de Android se distribuyen en archivos de tipo ".apk" que contienen los archivos ".dex" con los recursos asociados.
- Telephony Manager - Esta librería expone los servicios para realizar llamadas o

[22]widgets: elementos de la interfaz gráfica.
[23]HTML: Hiper Text Markup Language

acciones con SMS[24]/MMS[25], pero no permite reemplazar o eliminar la actividad que se muestra cuando una llamada está en curso.

- Resource Manager - Permite gestionar los elementos que componen la aplicación y pero se encuentran fuera del código, como bloque de texto idiomas diferentes, imágenes, sonidos o layouts[26].

- Location Manager - Permite el acceso a los dispositivos de geo-posicionamiento del equipo móvil, para determinar la ubicación del mismo mediante GPS u otros métodos disponibles en el entorno.

- Sensor Manager - Esta librería permite el acceso a diverso hardware de medición disponible en el dispositivo, como pueden ser: acelerómetros, giroscopios, sensores de luminosidad, sensores de campo magnético, brújulas, sensores de presión, sensores de proximidad, sensores de temperatura, etc.

- Cámara - Facilita el acceso a las cámaras de vídeo del equipo para capturar imágenes o vídeo.

- Multimedia - Este componente permite la reproducción de audio, vídeo e imágenes en el dispositivo.

2.5.5. Aplicaciones

Esta es la capa superior de la arquitectura donde se encuentran las aplicaciones específicas del sistema. Estas aplicaciones se ejecutarán en la máquina Virtual Dalvik anteriormente descripta, por lo que operarán como procesos con permisos independientes.

Estas aplicaciones pueden ser desarrolladas en Java con el ADK (Android Development Kit) o alternativamente en C/C++ con el NDK (Native Development Kit). Su distribución se realiza en el formato de extensión ".apk" (Application Package), el

[24]SMS: Short Message Systems, o Sistema de Mensajes Cortos
[25]Multimedia Messaging Service, o Servicio de Mensajería Multimedia
[26]Layout: disposición de los componentes.

mismo es una variable del tipo "jar" de java que almacena su información en formato "zip" estándar conteniendo la siguiente estructura de referencia:

- AndroidManifest.xml
- classes.dex
- resources.arsc
- res (Directorio)
- META-INF (Directorio)
- lib (Directorio)

2.6. Herramientas y accesorios de interés

En base a las características comunes de diversos modelos de la práctica forense detallados previamente, se comprende que su aplicación en el ámbito informático, particularmente sobre el objeto de análisis de este trabajo, requerirá de diversas herramientas de software para realizar tareas en etapas vinculadas a la recolección y análisis del objeto a peritar. Por este motivo se procede a detallar la finalidad y características de algunas de estas herramientas que formarán parte del conjunto utilizado para la aplicación del desarrollo de este trabajo.

2.6.1. ADB (Android Debug Bridge)

El ADB (Android Debug Bridge) es una herramienta de línea de comandos que permite la comunicación con un emulador o un dispositivo Android. Este programa esta formado por tres componentes:

- Un cliente, que se ejecuta en el equipo de desarrollo, utilizando la consola con el comando ADB.

- Un servidor, que corre como un proceso de fondo o segundo plano en el equipo de desarrollo. Este servidor administra la comunicación entre el cliente y el demonio de ADB que se ejecuta en el emulador o dispositivo objetivo.

- Un demonio, que se ejecuta como un proceso de fondo o segundo plano en cada emulador o dispositivo objetivo.

Cada vez que se inicia un cliente de ADB el proceso verifica la existencia de un proceso servidor en ejecución, cuando este no existe, procede a iniciarlo. En el inicio del servidor se abre el puerto local numero 5037 que quedará a la escucha de las instrucciones enviadas por los clientes de ADB.

Es el servidor quien establece las comunicaciones con los emuladores o dispositivos móviles, ubicando a los mismos mediante el escaneo de puertos impares en el rango del 5555 al 5585. Cuando el servidor encuentra un demonio de ADB establece una conexión en dicho puerto. De esta forma cada emulador o dispositivo obtendrá conexiones con un par de puertos secuenciales de número par para la consola e impar para la conexión adb.

Una vez establecidas estas conexiones con todas las instancias de emuladores o dispositivos, se podrán utilizar los comandos de ADB para operar con ellos. Debido a que el servidor administra las conexiones a los dispositivos o emuladores al mismo tiempo que maneja los comandos de múltiples clientes ADB, se puede operar con muchos dispositivos/emuladores en simultáneo y con cualquier cliente.

Las sintaxis de uso general del comando adb es la siguiente:

```
adb [-d|-e|-s <serialNumber>] <command>
```

Cuando hay solo un emulador en ejecución o un solo dispositivo conectado el cliente ADB es direccionado a éste en forma automática y por defecto. De no ser así, se necesita especificar el objetivo utilizando el parámetro -d para dispositivos de conexión directa(USB[27]), -e para emuladores o -s <código de serie> para seleccionar uno con

[27]USB: Universal Serial Bus

el código de serie asignado por el ADB (ejemplo: "emulator-5556"). Para este último caso se necesitará conocer los números de serie, dicha tarea se realiza con el comando

```
adb devices
```

No es la finalidad de este apartado cubrir todas las funcionalidades y el uso de esta herramienta, sino proveer una introducción a la misma y su arquitectura básica, pero cabe destacar que esta herramienta facilitará operaciones para el manejo de la instancia Android, incluyendo manejo de datos (ingreso y extracción), instalación/remoción de programas, ejecución de procesos, acceso a información del dispositivo y su estado.

2.6.2. dd

Este programa es un comando perteneciente a la familia de sistemas operativos basados en UNIX. Su finalidad es copiar y convertir datos manejando archivos a bajo nivel. La herramienta permite transferir datos específicos en modo raw (en crudo) y realizar conversiones relacionadas a codificación o caracteres predefinidos.

Su flexibilidad permite que sea utilizado para diversas tareas como creación de copias de seguridad por imagen raw o copia exacta, creación de dispositivos autoarrancables, borrado o formateo de nivel medio para dispositivos, entre otros usos.

La especificación POSIX define que dd copia un archivo de origen (parámetro if) a uno de destino (parámetro of), considerando los parámetros de conversión de datos (parámetro conv) y tamaño de bloques (parámetro bs). Es de importancia destacar que este tipo de sistemas operativos manejan sus dispositivos como archivos por lo que el comando podrá operar con cualquier dispositivo como un discos rígidos, partición, memoria SD[28], pendrive[29], etc.; de hecho, cuando no se especifica entrada o salida para la ejecución, utilizará la entrada y salida estándar de la consola por defecto (que también es un archivo).

Un ejemplo de su sintaxis de uso para eliminar datos de un dispositivo es:

```
dd if=/dev/zero of=/dev/sdn bs=512
```

[28]SD: Secure Digital es un formato de tarjeta de memoria portátil
[29]Pendrive: Unidad de memoria removible con interfaz USB

Ejemplo de su utilización para la copia fiel de un dispositivo a un archivo convencional:

```
dd if=/dev/sdn of=/dev/copia.raw bs=512 conv=noerror
```

2.6.3. dc3dd

Es una versión mejorada de la implementación de GNU dd con características orientadas al uso de la herramienta en procesos de informática forense. La misma se encuentra disponible para múltiples sistemas operativos bajo licencia GPL[30] y fue desarrollada en el año 2008 por Jesse Kornblum para el "DoD Cyber Crime Center" o DC3 perteneciente al Departamento de Defensa de los Estados Unidos.

Las mejoras mas relevantes sobre la versión de base de dd son:

- Hashing embebido en el proceso con tamaño de muestra variable (piecewise hashing) y soporte de diversos algoritmos como MD5, SHA-1, SHA-256 y SHA-512
- Registro de errores en archivo
- Registro de errores combinado y agrupado
- Borrado con patrones. Limpiando los archivos de salida con un solo dígito hexadecimal o un patrón de texto.
- Modo de verificación
- Reporte de progreso en ejecución
- Archivo de salida fraccionado

2.6.4. dcfldd

Es una versión mejorada de dd distribuida bajo licencia GPL y desarrollada por el Defense Computer Forensics Lab (DCFL) que es parte del DC3 del Departamento de

[30]GPL: GNU Public License, o Licencia Pública de GNU

defensa de los Estados Unidos. Al igual que dc3dd, sus mejoras están orientadas al uso de procedimientos propios de la informática forense.

Algunas de sus mejoras sobre el dd original son

- Hashing durante el proceso
- Indicador de progreso
- Limpieza de discos con patrones definidos
- Verificación de integridad bit a bit
- Salida simultanea a mas de una unidad o archivo
- Fraccionamiento de la salida en múltiples archivos
- Posibilidad de redireccionar datos y registros de actividad a aplicaciones externas

2.6.5. NANDdump

Es una herramienta utilizada para copiar información almacenada en dispositivos de tipo flash. Es parte de la utilidad llamada Mtdutils[31] que contiene una colección de herramientas para interactuar con dispositivos flash.

2.6.6. Xrecovery

xRecovery (xRecovery 0.3 xda-developers, 2010) es una herramienta de recuperación personalizada para teléfonos inteligentes de la linea Sony Ericsson Xperia. La misma permite al usuario generar copias de seguridad completas del dispositivo y restaurarlas.

2.6.7. Yaffs2utils

Es una colección de herramientas para crear y extraer archivos de imagen tipo YAFFS2[32]. Esto incluye a: mkyaffs2 que crea imágenes YAFFS2 desde un conjunto de

[31] Mtdutils - Texas Instruments Embedded Processors Wiki, 2009

[32] Yet Another Flash File System (Sólo otro sistema de ficheros flash), es el primer sistema de ficheros que fue diseñado específicamente para Memoria Flash NAND

archivos y directorios, unyaffs2 que extrae una imagen YAFFS que haya sido creada por mkyaffs2, y unspare2 que extrae el espacio spare (Fuera de banda) de un dispositivo flash.

2.6.8. Sleuth Kit

El Sleuth Kit (TSK) es una colección de herramientas basadas en linea de comandos UNIX que permiten realizar investigación forense sobre información de una computadora, soportando imágenes con diferentes tipos de sistemas de partición. Se encuentra disponible para múltiples sistemas operativos y es distribuido bajo licencia GPL/Common Public License/IBM Open Source.

La herramienta está organizada en capas, donde la capa de datos se ocupa de cómo está almacenada la información en el disco o la imagen y la capa de metadatos maneja la información vinculada a la estructura como inodos y directorios. Los comandos para manejar la capa de datos utilizan como prefijo la letra d mientras que aquellos que referencias a la meta-data usan la letra i.

A continuación se listan algunos de los comandos comunes de esta herramienta:

- blkcat - Muestra el contenido de un bloque
- blkls - Muestra una lista de bloques no asignados. Permitiendo búsquedas por palabras claves en un modo mucho mas eficiente
- blkcalc - Indica donde existen bloques sin asignar
- blkstat - Facilita los detalles de un bloque determinado
- icat - Muestra los contenidos de un archivo dado el valor de su inodo o el número de cluster correspondiente. No lista directorios
- iss - Lista los archivos de un disco
- istat - Provee información acerca de un número de inodo

Esta herramienta facilita la realización de búsquedas, incluso indexadas, de archivos en base a la asignación de espacio, tipo de archivos, datos en relación a sus indicadores cronológicos de creación y cambios, y palabras claves.

Los comandos *fls* e *ils* pueden ser usados para obtener un listado completo de las fechas y horas del sistema de archivos. Esta salida puede ser utilizada como entrada del comando mactimes para generar una línea de tiempo sobre los archivos del sistema.

2.6.9. Autopsy

Autopsy Forensic Browser es una interfaz gráfica para las herramientas de linea de comandos de Sleuth Kit. En conjunto permiten analizar discos y particiones de diversos sistemas operativos. Al igual que Sleuth Kit, es open source, distribuido bajo licencia GPL y puede correr en diferentes sistemas operativos, ya que es un producto basado en HTML, de esta forma despliega un servidor local al que se puede acceder con cualquier navegador web. La interfaz gráfica de Autopsy ayuda a organizar el proyecto de investigación forense y facilita un gestor de archivos que mostrará la estructura del sistema de archivos con detalles sobre cada directorio y su, contenido inclusive los elementos que han sido eliminados.

2.6.10. SQLite

Es un motor de base de datos relacional escrito en C, de tamaño reducido, bajos requisitos de recursos, Open Source y distribución por licencia de dominio publico. Su arquitectura se diferencia del modelo clásico de bases de datos cliente servidor dado que este producto no opera como un proceso independiente, sino que la librería se vincula al programa desarrollado, ejecutándose como parte del mismo, para de esta manera simplificar su comunicación y operar con llamadas directas a sus métodos y subrutinas. En cuanto al almacenamiento de datos, se centraliza en un único archivo alojado en el equipo de ejecución del programa.

Este producto implementa el estándar SQL-92 casi en su totalidad, con manejo de transacciones atómicas, vistas, índices, triggers y consultas complejas entre otras de

sus funcionalidades.

SQLite puede ejecutarse en múltiples plataformas, disponiendo de la posibilidad de ser utilizado por una gran cantidad de lenguajes. Estas características y su tamaño reducido lo hacen ideal para operar embebido en diversos productos, entre ellos el sistema operativo Android que esta involucrado en el desarrollo de este documento.

También existe una herramienta independiente con interfaz de línea de comandos que provee soporte al usuario para operar con la librería de forma interactiva, su nombre es sqlite y se la utilizará como cliente de acceso a los datos almacenados con SQLite.

2.6.11. jhead

Este producto permite manipular la información almacenada como meta-datos de imágenes Exif[33] jpeg; el mismo tiene soporte multi-plataforma con interfaz de línea de comandos, código Open Source y licencia de dominio publico.

Estos datos contienen información relevante como equipo utilizado para capturar la imagen, fecha, hora, ubicación geográfica de la toma, etc. A continuación se muestra un ejemplo del reporte básico generado por la herramienta para una imagen:

File name : 1.jpg
File size : 9823764 bytes
File date : 2013:04:06 02:42:47
Camera make : NIKON CORPORATION
Camera model : NIKON D3200
Date/Time : 2013:04:01 19:01:36
Resolution : 5744 x 3824
Flash used : No
Focal length : 36.0mm (35mm equivalent: 54mm)
Exposure time: 0.025 s (1/40)
Aperture : f/5.0
ISO equiv. : 1600

[33]Exchangeable image file format

Whitebalance : Auto

Metering Mode: pattern

Exposure : program (auto)

GPS Latitude : ? ?

GPS Longitude: ? ?

2.6.12. AFLogical

Es una herramienta de la empresa *Viaforensic* para la extracción de información de sistemas Android. Este desarrollo se distribuye con versiones gratuitas y una versión Open Source bajo licencia GPL.

Este software realiza una adquisición lógica de información como SMS, MMS, imágenes, contactos, registros de llamadas, etc. sobre dispositivos Android 1.5 o superiores; los datos extraídos son procesados y almacenados en la memoria SD en formato CSV (valores separados por coma) para que posteriormente puedan ser importados a cualquier herramienta que maneje este formato.

Esta herramienta consiste en un programa para la plataforma móvil que se instala y se ejecuta en el móvil para realizar la extracción en cuestión.

Capítulo 3

De la situación problemática a la solución

Este estudio busca determinar un marco de referencia formal para adaptar las practicas de la investigación forense a los dispositivos móviles basados en el sistema operativo Android.

3.1. Hipótesis

Ante la situación actual de los dispositivos móviles y su injerencia en la sociedad, particularmente en para gestión de la información diaria de las personas, es de gran importancia para el ámbito civil y judicial disponer de métodos forenses comunes y flexibles para el trabajo de peritaje sobre los mismos.

Considerando la existencia y disponibilidad de diferentes modelos de trabajo para la practica forense y su adaptación y/o aplicabilidad en el área informática. En conjunto con el conocimiento y material disponible sobre los detalles técnicos del sistema operativo Android es posible relacionar este conocimiento con las buenas practicas y herramientas de la actualidad. En este contexto el trabajo plantea que es posible establecer un marco de referencia genérico para el análisis forense de dispositivos móviles con sistema operativo Android para ser utilizado en la República Argentina conforme

con las metodologías de trabajo utilizadas en otras áreas de esta especialización.

3.2. Objetivos

El desarrollo de este trabajo se ha realizado en función de los siguientes objetivos:

- Establecer un marco de trabajo para la investigación forense de dispositivos Android.
- Identificar los procesos generales comunes para el caso.
- Indicar los procedimientos técnicos a aplicar en cada etapa.

3.3. Limites

Este trabajo se encuentra limitado por la dificultad de disponer con todas las plataformas de hardware que cumplen con las condiciones de análisis, que son particularmente dispositivos móviles con sistema operativo Android.

Al mismo tiempo encuentro que existen otras herramientas de hardware y software alternativas a las evaluadas pero que no serán utilizadas por razones de costo y/o disponibilidad.

Los contenidos de este documento se encuentran acotados por los siguientes puntos:

- Este documento solo considera a las versiones de Android 2.X y 3.X.
- El análisis excluye las particularidades de la extracción de datos de los dispositivos.
- El ámbito de análisis para la aplicación del marco de trabajo queda restringido al dominio de la legislación local.

Quedaran fuera del ámbito de control del material de esta investigación:

- Alteraciones en el kernel, drivers o software instalados en los equipos introducido por el fabricante.
- Diferencias en las versiones de las aplicaciones ejecutadas en cada dispositivo real o virtual que difieran debido a incompatibilidad con la plataforma.
- Capacidad de extracción directa de datos de los medios de almacenamiento internos.
- Metodologías para escalar privilegios en los dispositivos.

3.4. Recursos

El objeto de estudio se compondrá por el marco de trabajo desarrollado en este documento y los dispositivos físicos o virtuales que ejecuten la versión de Android correspondiente al caso de análisis, el mismo sera evaluado en conjunto con sus repositorios de datos (memoria de almacenamiento interna y/o externa) ya sean físicos como memorias microSD o lógicos para el caso de archivos.

La población alcanzada en este trabajo cubre a las versiones de Android de la serie 2.x y 3.x ejecutándose en entornos físicos o emulados, comprendiendo las siguientes productos:

- Android 2.0/2.1 Eclair - Octubre del 2009, SDK de Android 2.0 basado en el núcleo de Linux 2.6.29.
- Android 2.2.x Froyo - Mayo del 2010, SDK de Android 2.2 Froyo basado en el núcleo de Linux 2.6.32.
- Android 2.3.x Gingerbread - Diciembre del 2010, SDK de Android 2.3 Gingerbread basado en el núcleo Linux 2.6.35.
- Android 3.x Honeycomb - Febrero del 2011, SDK de Android 3.0 (Honeycomb) basada en el núcleo de Linux 2.6.36.

Emulador y herramientas de Android El SDK[1] que incluye estos productos fue obtenido del sitio oficial ubicado en *http://developer.android.com* . Luego de descargar el paquete del *SDK*, este debe descomprimirse en una ubicación accesible por el usuario que ejecutará estas herramientas. El software descargado no contiene los archivos correspondientes a las librerías que utiliza el emulador para ejecutar cada versión de Android; a fin de obtener estos archivos se debe ejecutar el programa *tools/android* e instalar las APIs[2] y *SDK platform* para cada versión de Android bajo el alcance de esta investigación, las mismas son:

- Android 2.1 (API 7)
- Android 2.2 (API 8)
- Android 2.3.3 (API 10)
- Android 3.0 (API 11)

Finalizado este paso y con todas las librerías requeridas por el emulador se procederá a crear los AVD(Android Virtual Device) correspondientes, generando uno para cada versión del sistema operativo, las características del hardware emulado no están alcanzadas por esta investigación.

3.4.1. Hardware, Dispositivos móviles con sistema operativo Android

Los dispositivos físicos han sido conseguidos de forma independiente para llevar adelante este trabajo de investigación. Para su preparación los dispositivos atravesarán el mismo proceso que los entornos virtuales o emulados sujetos a las limitaciones de cifrado y bloqueo de nivel de acceso de cada dispositivo.

[1]SDK: Software Development Kit, o Kit de desarrollo de software
[2]APIs: Application Programming Interface, o interfaz de programación de aplicaciones

3.4.2. Software para la preparación del objeto de análisis

Este software ha sido desarrollado para esta investigación. Se ofrecen mas detalles en el Anexo A de este documento.

El software se ejecutará sobre los dispositivos físicos o virtuales que serán objeto de análisis. Su utilización permite que se escriba un conjunto de datos predefinidos en el dispositivo objetivo, y de esta forma garantizar que esta información correspondiente a los servicios básicos y de uso común estará disponible en todos los dispositivos, permitiendo así una comparación mas confiable sobre los resultados emergentes del trabajo sobre cada elemento.

El software se limitará a incluir entradas para los siguientes tipos de datos:

- Contactos en el directorio telefónico del sistema, compuestos por nombre y número de teléfono.
- Mensajes de texto recibidos y enviados por el sistema.
- Llamadas telefónicas realizadas, recibidas y perdidas.

El programa utiliza la aplicación ADB[3] para comunicarse con el dispositivo móvil real o virtual, por lo que se deberá configurar el programa con la ubicación de ADB. Posteriormente se procederá a conectar el dispositivo físico al puerto correspondiente o iniciar el emulador para el caso de dispositivos lógicos, esta conexión sera exclusiva, solo un dispositivo por vez. Una vez conectado el dispositivo se ejecuta el programa desde la linea de comandos y el mismo cargara el conjunto de datos predefinido automáticamente.

[3]ADB: Android Debug Bridge

Capítulo 4

Solución

Sobre la hipótesis definida en este documento, la investigación buscará utilizar el conocimiento criminalístico, legal y técnico disponible para definir un marco de trabajo basado en la investigación forense de dispositivos móviles con sistema operativo Android conforme a las necesidades de la legislación de la República Argentina, identificando procesos de uso general y los procedimientos técnicos a ser aplicados en cada etapa. La validez de la hipótesis en cuestión sera evaluada en base a los resultados obtenidos de pruebas empíricas con dispositivos físicos o virtuales que permitan demostrar la viabilidad de uso y alcance real de dicho marco de trabajo al ser utilizado para el análisis forense.

4.1. Marco de trabajo para la evaluación de muestras

El marco de trabajo desarrollado para esta investigación tomará como referencia el modelo de Casey y en concordancia con éste he definido cinco etapas de procedimiento para ser ejecutadas en forma secuencial. Con fines prácticos identificaré estas etapas numéricamente en orden creciente del uno al cinco.

El proceso de documentación se implementará de manera transversal a las cinco etapas, con la finalidad que las acciones tomadas en cada una de ellas cuenten con una

bitácora cronológica y evidencia de respaldo al finalizar la pericia.

El siguiente gráfico muestra la correspondencia de las etapas del marco de trabajo con el modelo de Casey.

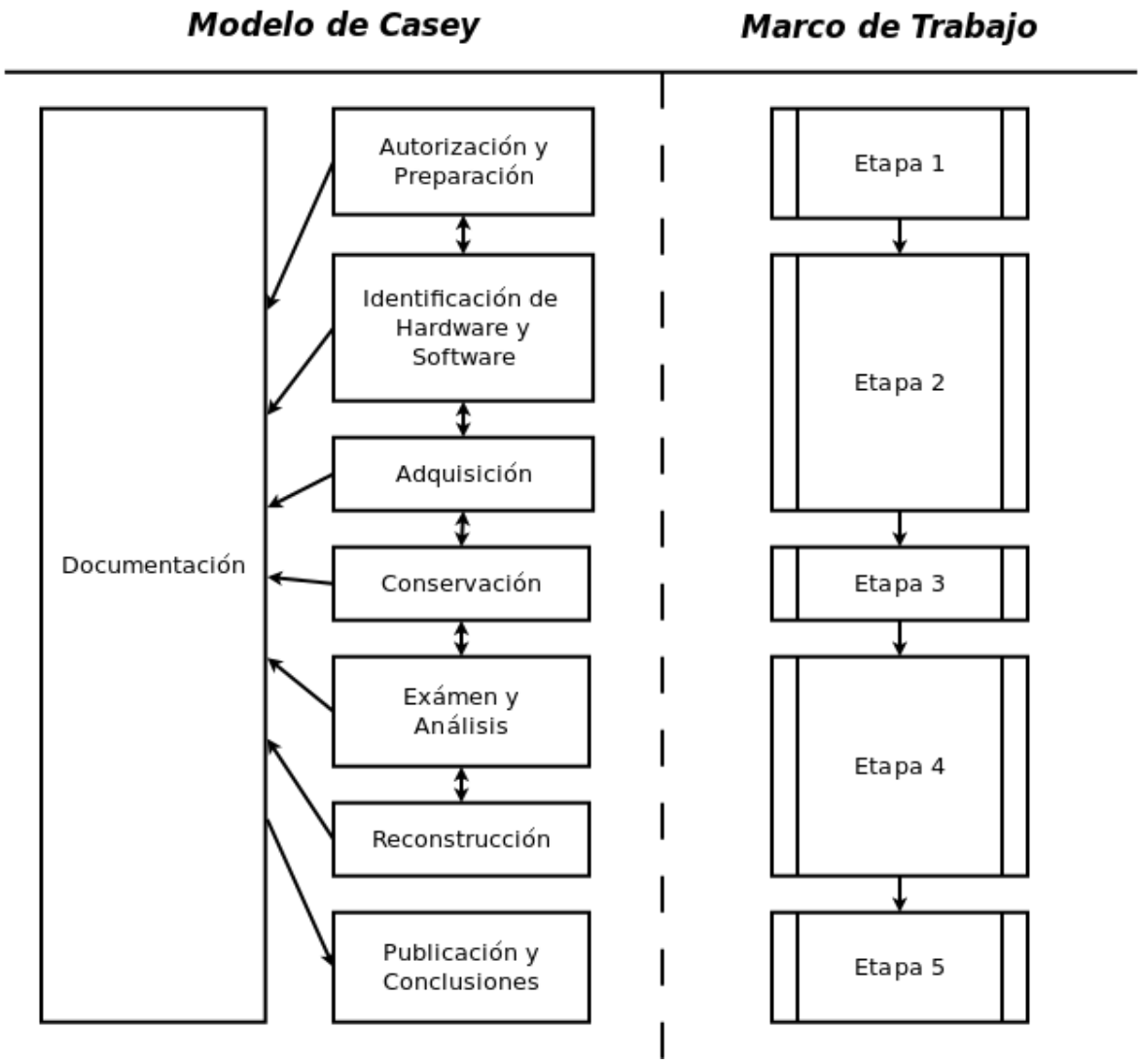

Figura 4.1: Etapas del marco de trabajo

Las siguientes explicaciones sobre el propósito y procedimientos de cada etapa del marco de trabajo contendrán referencias y ejemplos técnicos para concretar cada tarea, sin embargo trabajo busca definir la metodología de procedimiento y documentación exclusivamente, siendo los ejemplos y citas técnicas solo elementos de sugerencia u orientación, pudiendo ser reemplazados por otras herramientas o productos que satis-

fagan la necesidad planteada.

Para la definición de estas etapas se han considerado trabajos previos dedicados al análisis de información en dispositivos y aspectos legales. Entre ellos se encuentran las siguientes referencias bibliográficas [André Morum de L. Simao, 2011], [Darahuge, 2012], [Jeff Lessard, 2010], [Cabrera, 2011], [D. Brezinski, 2002], [Jansen and Ayers, 2007].

4.1.1. Etapa 1

En esta primer etapa se verificarán las condiciones, datos y detalles del caso para cumplir con los requisitos legales y procesales de la pericia, con foco en garantizar la correcta autorización para el accionar del perito con su alcance definido y el contexto necesario para la adecuada preparación de la evidencia afectada.

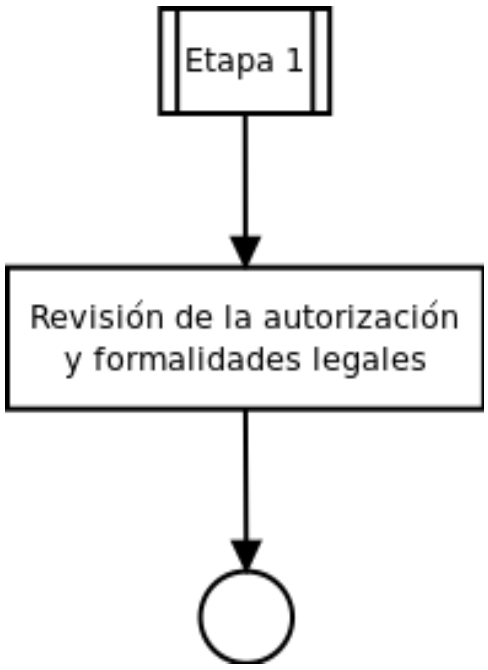

Figura 4.2: Etapa número uno

Al finalizar esta etapa, con la seguridad de que se cumplen todos los requisitos legales y procesales, mas la existencia de una clara definición del alcance de la pericia, se procede a documentar la situación guardando copia de la evidencia en cuestión.

El marco de trabajo no provee plantillas particulares para esta etapa, por lo que la evidencia y su formato de presentación se ajustará al criterio del perito, mas la documentación de origen externo que se tome como entrada para la etapa.

4.1.2. Etapa 2

Esta etapa cubre los aspectos vinculados a la identificación del hardware y software abarcado por el alcance del peritaje, en conjunto con las acciones requeridas para una correcta adquisición de datos.

La ejecución de esta etapa seguirá las acciones del siguiente diagrama de flujo, con el fin de ajustarse a las diversas condiciones que plantee cada escenario

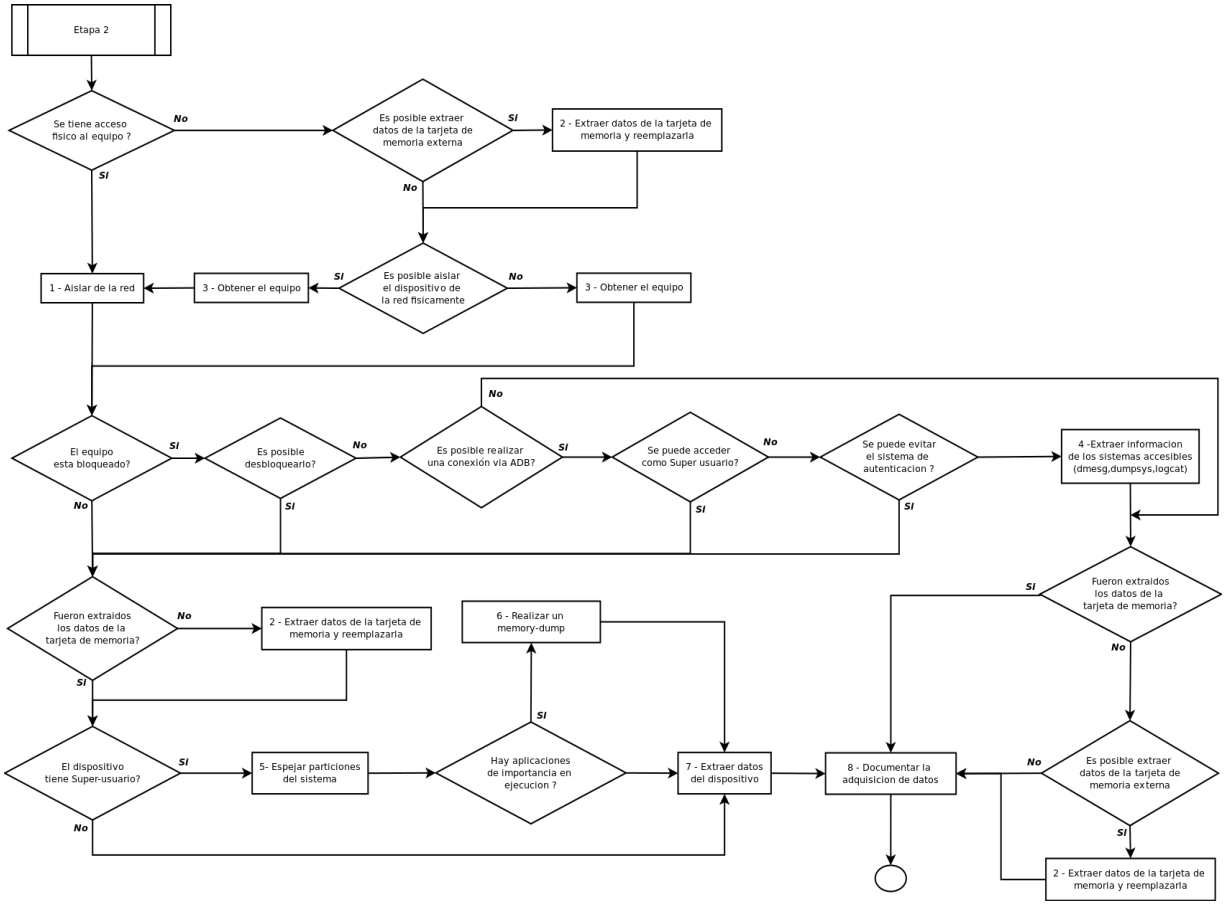

Figura 4.3: Etapa número dos

A continuación se proveen los detalles de cada acción prevista en el diagrama de

flujo, las mismas estarán acompañadas de la sugerencia técnica para completar la tarea en cuestión.

4.1.2.1. Aislar la red

Esta acción debe llevarse a cabo con el fin de garantizar que el equipo no dispone de comunicación que de lugar a acciones no controladas sobre el mismo, como actividad de mensajería, llamadas, control remoto del sistema, ejecución programada de aplicaciones, modificaciones de datos almacenados, etc.

La modalidad y efectividad del método de aislación del dispositivo dependerá de las condiciones de acceso y manipulación de éste. A continuación se listan los diferentes métodos sugeridos:

- Introducir el dispositivo dentro de una jaula de Faraday[1]
- Envolver el dispositivo en papel de aluminio, utilizando un mínimo de tres capas envolventes.
- Colocar el dispositivo en modo avión
- Utilizar un bloqueador de señal o jammer[2] cerca del dispositivo
- Remover la batería del dispositivo

4.1.2.2. Extraer datos de la tarjeta de memoria y reemplazarla

En este punto se debe extraer la tarjeta de datos removible con el fin de resguardar la misma y generar la extracción de datos que dará lugar a las copias y su código de integridad. Sobre estos elementos se trabajará en las etapas posteriores a fin de evitar el uso de la pieza original y permitir una rápida restauración y verificación de integridad de los datos de la evidencia.

Para completar esta tarea se podrá hacer uso de la herramienta *dc3dd*, mediante la siguiente sentencia:

[1] Una jaula de Faraday es una caja metálica que protege de los campos eléctricos estáticos
[2] Es un dispositivo que bloquea o interfiere señales inalámbricas

```
dc3dd if=/dev/sdb1 of=./sdcard.dd  hash=sha1 hlog=./sdcard.sha1
```

Los parámetros de esta sentencia configuran el comportamiento en función de las siguientes funciones:

Parámetro	Función
if	Origen de los datos. Ubicación del dispositivo asociado al lector de memoria SD donde se encuentra la tarjeta de memoria a copiar
of	Archivo de destino para la extracción de datos
hash	Algoritmo de hashing a utilizar
log	Archivo donde se depositara la información de auditoría del proceso

Cuadro 4.1: Tabla de parámetros de dc3dd

Al finalizar esta etapa se dispondrá de los siguientes elementos por cada tarjeta de memoria:

- Tarjeta de memoria SD[3] lista para ser rotulada y depositada como evidencia.
- Archivo de imagen o copia fiel de la tarjeta SD. El mismo se utilizará para el trabajo de peritaje, evitando la manipulación de la tarjeta SD, siendo el punto de referencia para la verificación de integridad de los datos y la generación de copias de trabajo.
- Archivo con la información de hash[4] de la imagen o copia, este se utilizará para verificar la integridad de las copias de trabajo.

4.1.2.3. Obtener el equipo

Esta es la acción de disponer personalmente del equipo para realizar la extracción de datos correspondiente que dará lugar a la recolección de muestras para el trabajo de análisis pericial.

[3]SD: Secure Digital es un formato de tarjeta de memoria portátil
[4]hash:Valor de representación casi unívoca para un documento o conjunto de datos.

4.1.2.4. Extraer información de los sistemas accesibles

Esta acción se vincula al escenario donde se logra acceder al dispositivo pero no se dispone de acceso como superusuario o root[5]. En consecuencia se estará limitado para ejecutar diversas acciones sobre el sistema como por ejemplo el espejado de las particiones.

A pesar de estas circunstancias desfavorables para el proceso de adquisición de datos se debe capturar toda la información disponible para el usuario en sesión, citando como ejemplo:

- Información del log del núcleo o kernel, la misma se obtiene con el comando "dmesg" y deberá redirigirse a un archivo en la memoria SD para poder ser retirada del dispositivo y almacenada con el recaudo para el caso. Un ejemplo para el llamado de ejecución es: **adb shell dmesg > /mnt/sdcard/dmesg.text**

- Android facilita la información del sistema para el dispositivo mediante el comando "dumpsys". Este comando puede proveer información específica mediante los siguientes parámetros (meminfo, cpuinfo, account, activity,window, wifi) o proveer toda la información disponible al ser invocado sin ningún parámetro adicional, un ejemplo para este llamado de ejecución es el siguiente: **adb shell dumpsys >/mnt/sdcard/dumpsys.text**

- El sistema Android permite visualizar sus mensajes de log mediante el comando "logcat", la salida del mismo también deberá ser direccionada a la memoria SD para su posterior tratamiento. Un ejemplo para la invocación de este comando es: **adb logcat -d -v time >/mnt/sdcard/logcat.text**

4.1.2.5. Espejar particiones del sistema

En esta etapa y con acceso de super-usuario o root se podrán espejar las particiones del dispositivo móvil llevando la información de cada una de ellas a un archivo que

[5]root: Usuario administrador o de máximo acceso en sistemas UNIX y derivados.

posteriormente se extraerá del dispositivo y se utilizará para el análisis de sus datos en el proceso de peritaje.

Para concretar esta acción se puede utilizar una técnica basada en los siguientes pasos:

- Identificar las particiones disponibles en el dispositivo. Para ello se puede listar las particiones montadas con el siguiente comando: **mount | grep mtd**

- Seleccionar aquellas particiones correspondientes al almacenamiento interno y con relevancia para el análisis. Se tomará como entrada el listado provisto por el punto anterior y se procederá con el criterio asociado a la estructura de archivos del sistema operativo, la misma ha sido descripta en el marco teórico de este documento. Se citan como ejemplos de particiones relevantes o que pueden contener información de interés a aquellas vinculadas a los siguientes puntos de montaje:

  - /data
  - /system
  - /cache

- Espejar cada partición en un archivo, esta tarea podrá realizarse utilizando una herramienta de copia directa como *dd*. Por ejemplo, se podría espejar la partición **/dev/mtd/mtd6ro** con la siguiente instrucción:

  - **dd if=/dev/mtd/mtd6ro of=/mnt/sdcard/mdt6ro.dd bs=512**

- Copiar o mover el archivo fuera del dispositivo, para tal fin simplemente se extraerá el archivo del dispositivo. En aquellos escenarios donde el dispositivo cuenta con la posibilidad de manejar tarjetas de memoria removibles se procede a generar la imagen del espejado de partición en la tarjeta para luego extraerla y operar con la misma fuera del dispositivo en peritaje.

4.1.2.6. Realizar un memory dump

En esta etapa se busca obtener información de la memoria RAM del dispositivo que contendrá datos utilizados por los programas en ejecución. Existen diferentes métodos para realizar esta tarea, a modo de referencia cito el método de interrupción por su sencillez y bajo impacto en el ambiente de estudio.

El procedimiento en cuestión consta de los siguientes pasos:

- Acceder a la consola del dispositivo en modo de super-usuario
- Ubicarse un el directorio **/data/misc**
- Modificar los permisos del directorio a 777 (permiso de ejecución, escritura y lectura para todos los usuarios). Esto se realiza con el comando **chmod 777 /data/misc**
- Visualizar los procesos en ejecución con el comando **ps**
- Terminar de forma abrupta cada proceso, de esta forma se genera un archivo de dump con la información requerida en este punto para cada programa. Para realizar esta tarea se debe tomar nota del PID [6] del programa en ejecución y ejecutar el comando **kill -10 [PID]**
- Listar los archivos de dump generados con el comando **ls /data/misc | grep dump** , allí se observaran los archivos con la información de memoria capturada para cada proceso interrumpido anteriormente, cada archivo contiene el PID del proceso asociado a su información.

Los archivos extraídos deberán ser retirados del dispositivo, identificados por su código de hash y anexados a la evidencia a analizar.

[6] PID: número identificador del proceso.

4.1.2.7. Extraer datos del dispositivo

En este punto se buscará capturar la información específica de las aplicaciones afectadas para los casos donde no se pueda espejar las particiones o resulte de interés aislar esta información para facilitar la posterior etapa de análisis. Se trabaja con la información contenida en las particiones, accediendo a los sistemas de archivos YAFFS regulares, por esta razón se dispondrá de diferentes métodos para obtener la información dependiendo del alcance de la extracción deseada ya que cada aplicación define la manera en que sus datos son almacenados. Sin embargo esta plataforma incluye muchos programas de uso común, inclusive distribuidos con el sistema operativo, permitiendo conocer el manejo de datos de los mismos y dando lugar a que la extracción pueda realizarse manualmente o utilizando productos que automatizan la extracción, como por ejemplo Android "Forensic Logical Application" de la empresa viaForensics.

Citaré como ejemplo de referencia la extracción manual de los archivos que contienen las bases de datos relacionadas con la actividad de mensajería y telefonía del sistema, estos archivos se listan a continuación:

- /data/data/com.android.providers.telephony/databases/mmssms.db
- /data/data/com.android.providers.contacts/databases/contacts2.db

Dichos archivos deben ser extraídos del dispositivo, documentados y resguardados para su uso futuro junto a al código de hash correspondiente a cada uno.

4.1.2.8. Documentar la adquisición de datos

Al finalizar esta etapa se encontrará en condiciones de documentar la información obtenida en los puntos previos, para esto el proceso sugiere el uso de los siguientes documentos vinculados al anexo de este documento:

- Ficha de identificación de Hardware, este documento contendrá la información relativa al hardware del dispositivo, la misma podrá ser relevada manualmente leyendo las etiquetas y grabados del mismo, accediendo a sus módulos de almacenamiento para relevar sus grabados y/o acceder al menú de configuración

mediante la interfaz gráfica. No obstante, este estudio sugiere el uso de las siguientes sentencias para obtener la información desde la terminal de adb:

Campo	**Método sugerido**
Marca	adb shell getprop ro.product.manufacturer
Modelo	adb shell getprop ro.product.model
Nro. de serie	adb shell getprop gsm.serial adb shell getprop ro.serialno
Garantía	-
IMEI	adb shell dumpsys iphonesubinfo
Nro. de teléfono	-
Proveedor	adb shell getprop gsm.sim.operator.alpha adb shell getprop gsm.sim.operator.alpha.2 adb shell getprop gsm.sim.operator.alpha.3 adb shell getprop gsm.sim.operator.alpha.4
Otro	adb shell getprop
Información de almacenamiento	df La información de salida muestra el estado de diferentes puntos de almacenamiento, que en general responden a la siguiente nomenclatura: /data (Memoria interna) /mnt/sdcard (Memoria montada como externa) /mnt/sdcard2 (Memoria montada como externa, el numero final se incrementará en el caso que existieran mas memorias en el dispositivo)

Cuadro 4.2: Tabla de adquisición de datos del hardware con adb

- Ficha de identificación de Software, el documento contendrá la información descriptiva del software disponible en el dispositivo, dicha información se podrá relevar manualmente desde la interfaz gráfica del dispositivo. A continuación, se provee una lista de sugerencias para realizar esta tarea desde la consola de ADB:

Campo	Método sugerido
Tipo	Android
Versión	adb shell getprop ro.build.version.release adb shell getprop ro.build.version.sdk adb shell getprop ro.build.display.id adb shell getprop ro.build.date
Detalles	adb shell getprop
Aplicaciones	adb shell pm list packages -f
Observaciones	Especificar las condiciones de configuración o características del software que afecten el proceso, por ejemplo: - Código, patrón u otro sistema de control de acceso a la interfaz gráfica. - Dispositivo en modo de usuario o root. Si se dispone de nivel root o administrador debe aclararse si existía previamente o si es resultado de una acción generada en la recolección, detallando el procedimiento utilizado y su impacto.

Cuadro 4.3: Tabla de adquisición de datos del sistema con adb

- Ficha de datos adquiridos, este documento listara todos los elementos contenedores de información obtenidos durante esta etapa dejando registro de su medio o tipo, punto de almacenamiento, código de hash y comentarios. Para registrar esta información se sugieren los siguientes métodos

Campo	Método sugerido
Tipo	En referencia al medio, por ejemplo: Tarjeta de memoria MicroSD, archivo de datos, archivo espejo de partición, etc.
Almacenamiento	Ubicación y nombre del medio contenedor
Hash	Código de hash (o integridad correspondiente). Se debe utilizar el mismo algoritmo para todos los registros del documento. Se sugiere identificarlo en la misma entrada, por ejemplo: SHA1: 4e1243bd22c66e76c2ba9eddc1f91394e57f9f83
Comentarios	Descripción general del origen y propósito de análisis de la información capturada.

Cuadro 4.4: Tabla de registro para datos adquiridos

El anexo C de este documento contiene un script de python que implementa

estas sugerencias con el fin de facilitar la tarea. Es importante destacar que solo automatiza los pasos sugeridos, sobre esta información el perito debe continuar completando los formularios manualmente con toda la información faltante o de interés para la pericia.

4.1.3. Etapa 3

Esta etapa abarca las acciones necesarias para documentar la cadena de custodia de la evidencia disponible y la conservación de datos para su uso a lo largo de las diferentes pruebas previstas y/o la necesidad de restauración o validación de los mismos.

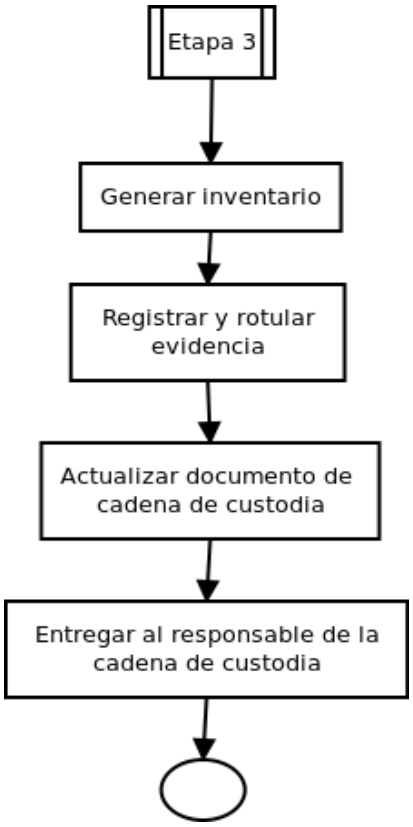

Figura 4.4: Etapa número tres

Las actividades de esta etapa podrán documentarse con las plantillas “Rotulo de evidencias”, “Recibo de efectos”, “Formulario para la cadena de custodia” e “Inventario”.

- Rótulo de evidencias, deberá generarse una copia de este documento para cada elemento constituido en evidencia, el mismo permitirá identificar de forma unívoca la pieza para que pueda referenciarse a lo largo de toda la documentación del proceso.

- Recibo de efectos, este documento dejara constancia de la entrega de evidencia para traslado y manipulación.

- Formulario para la cadena de custodia, el documento mantendrá registro para el seguimiento de la evidencia, teniendo constancia de los traslados de cada elemento y los responsables por el mismo.

- Inventario, este documento detalla y enumera los elementos que componen la evidencia obtenida en las etapas previas.

4.1.4. Etapa 4

La etapa en cuestión se ocupará de la realización del análisis pericial requerido y las acciones tendientes a la reconstrucción de los sucesos asociados a la prueba analizada. Es de suma importancia recordar que las tareas de análisis deberán ser coherentes con el alcance de la orden judicial o pedido particular que da lugar a la pericia, dicho material fue revisado y documentado en la primer etapa del marco de trabajo.

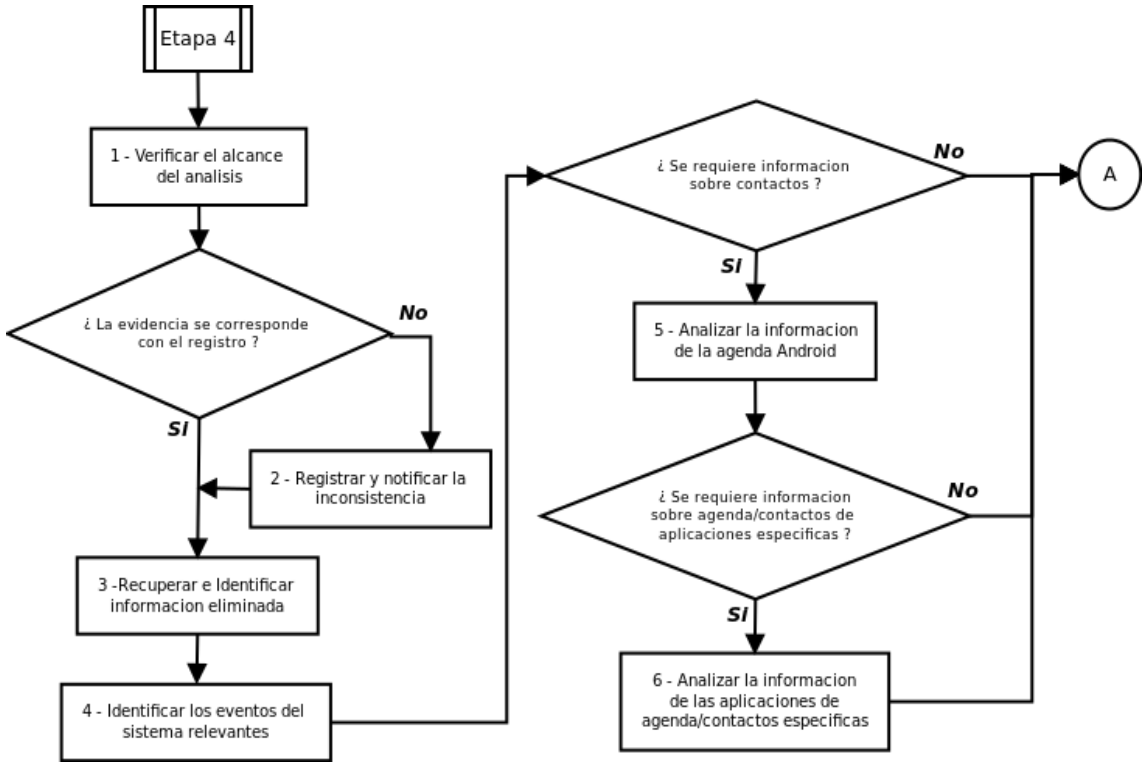

Figura 4.5: Etapa número cuatro - Parte 1

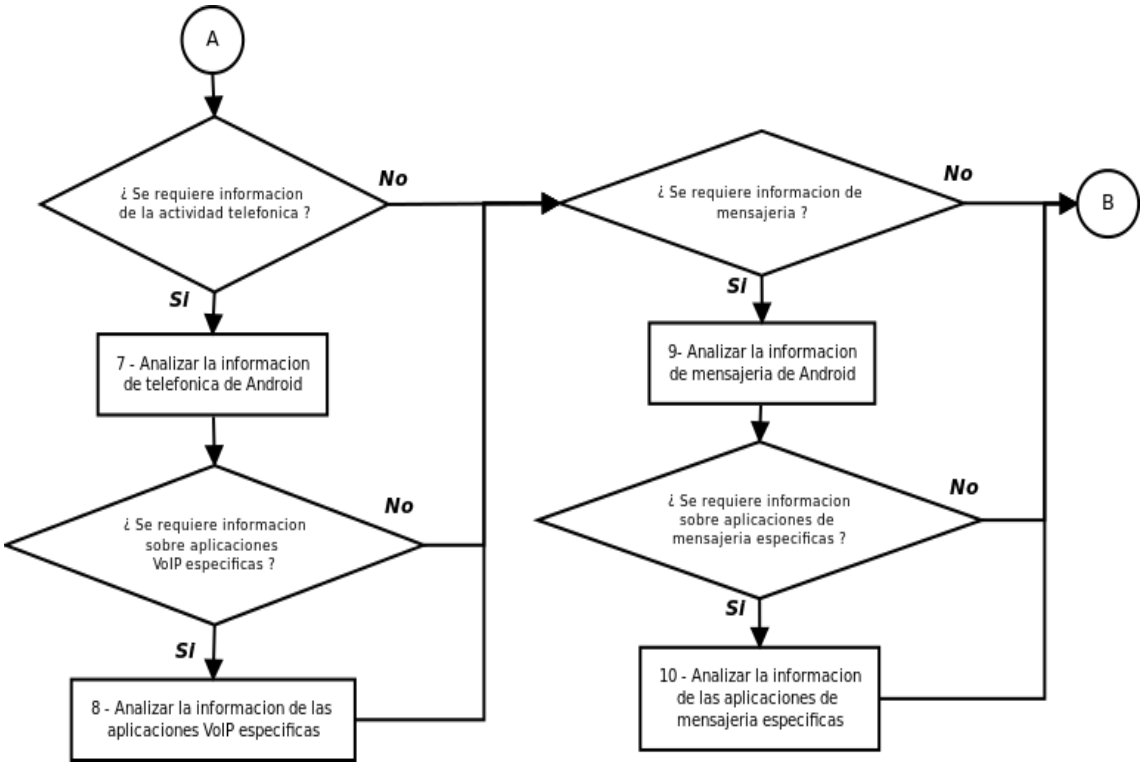

Figura 4.6: Etapa número cuatro - Parte 2

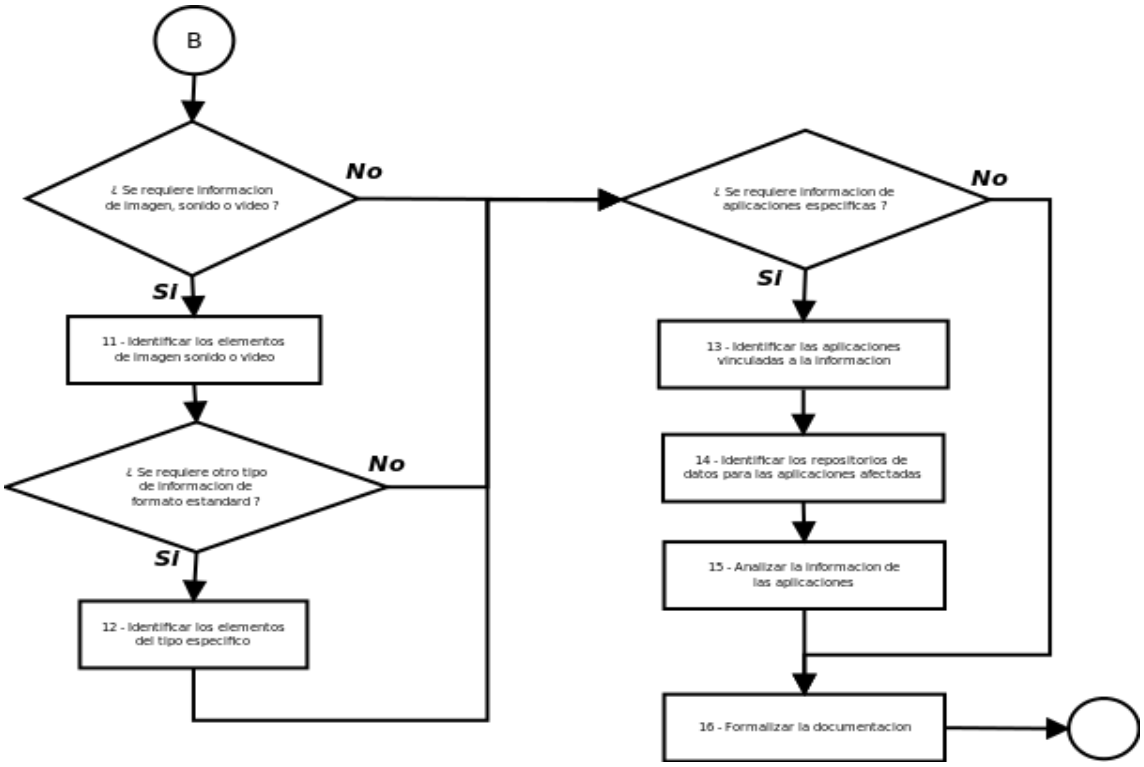

Figura 4.7: Etapa número cuatro - Parte 3

A continuación se detallan las actividades contempladas en cada acción del proceso.

4.1.4.1. Verificar el alcance del análisis

En este punto el perito deberá verificar el alcance de la pericia solicitada utilizando la información disponible como evidencia de la etapa uno, mas aquella información que pueda ser provista de manera formal por los diferentes actores del proceso.

La finalidad de esta tarea es disponer de un alcance claro y verificado para no excederse en las acciones técnicas del peritaje u omitir el análisis de información relevante para los solicitantes.

Cabe destacar que es de suma importancia realizar esta tarea dado que un alcance mal definido o interpretado podría dar lugar a la anulación del aporte de la pericia en el marco de un proceso judicial.

4.1.4.2. Registrar y notificar la inconsistencia

Como se detalló en la sección de documentación para la etapa numero dos, la evidencia recolectada se registró en los entregables mediante la ficha de datos adquiridos junto con la información de integridad de cada elemento. Por lo que la primer acción del perito deberá ser la revisión de los elementos de evidencia recibidos. A tal fin estará obligado a verificar la existencia y disponibilidad de los mismos, además de calcular el código de integridad o hash correspondiente a cada elemento y compararlo con el valor indicado para cada elemento en el entregable referenciado previamente.

En aquellos casos donde se encuentren inconsistencias como el faltante de evidencia, o una alteración de su estado (ya sea notable en el medio físico o de integridad de datos) deberá registrarse, detallarse y notificar la misma a todos los actores involucrados en el proceso que origina la pericia.

4.1.4.3. Recuperar e Identificar información eliminada

En esta etapa se analizarán las imágenes de particiones correspondientes a la memoria de almacenamiento del dispositivo y de unidades externas, como las obtenidas de memorias SD, con la finalidad de recuperar información residual de los archivos eliminados previamente.

Cabe destacar que se encontrarán dos escenarios para este análisis en función del la metodología de almacenamiento sujeta a los sistemas de partición utilizados, estas serán:

1. YAFFS – Para las imágenes de partición del sistema

2. FAT – Para los medios externos como las memorias SD. En este punto se debe considerar que hay dispositivos que contienen memorias de almacenamiento análogas a las externas pero embebidas en el mismo.

La información resultante será considerada para todas las siguientes tareas de análisis establecidas en esta etapa del marco de trabajo.

Esta tarea puede realizarse con diferentes herramientas, a continuación detallare un ejemplo mediante el uso de The Sleuth Kit, una herramienta open source de libre distribución que cuenta con las capacidades requeridas.

El primer paso es instalar la herramienta y verificar que la versión de la misma incluye el soporte para los sistemas de partición a utilizar, esto lo se podrá realizar con la siguiente instrucción:

```
# fls -f list

Supported file system types:
  ntfs (NTFS)
  fat (FAT (Auto Detection))
  ext (ExtX (Auto Detection))
  iso9660 (ISO9660 CD)
  hfs (HFS+)
  ufs (UFS (Auto Detection))
  raw (Raw Data)
  swap (Swap Space)
  fat12 (FAT12)
  fat16 (FAT16)
  fat32 (FAT32)
  ext2 (Ext2)
  ext3 (Ext3)
  ext4 (Ext4)
  ufs1 (UFS1)
  ufs2 (UFS2)
  yaffs2 (YAFFS2)
```

Una vez verificado este punto se puede proceder con el análisis de cada imagen de partición, para esto realizare tres pasos por cada archivo con los siguientes objetivos:

1. Obtener un listado del contenido para el sistema de archivos

```
# fls -f yaffs2 -m / /caso/imagen.dd > fs-data
```

2. Obtener el listado de información de inodos[7] para el sistema de archivos, esta información es fundamental para acceder a los datos que permiten reconstruir cada archivo.

```
# ils -f yaffs2 -m /caso/imagen.dd >> fs-data-inodes
```

3. Generar un reporte de actividad o linea de tiempo en formato CSV[8] para el sistema de archivos evaluando el periodo a peritar

```
# mactime -d -b fs-data-inodes 01/01/2013-12/31/2013 > reporte-
  actividad-fs-2013.csv
```

Como último punto cabe destacar que en algunas ocasiones la pericia requerirá la recuperación del contenido de uno o mas archivos del sistema de archivos, esta tarea puede realizarse con la herramienta de nombre *icat* del mismo software, indicando el numero de inodo correspondiente. Permitiendo de esta forma acceder al contenido tanto para archivos regulares como eliminados(solo cuando las condiciones del sistema de archivos lo permitan). La siguiente instrucción es un ejemplo de su uso:

```
# icat -s -f yaffs2 /caso/imagen.dd 47369
```

Los comandos anteriores se han citado a modo de ejemplo, siendo el objetivo de los mismos el análisis de una imagen correspondiente a una partición con sistema de archivos tipo YAFFS2. Cabe destacar que para el manejo de imágenes asociadas a memorias externas, como MicroSD y otras variantes, suelen utilizarse configuraciones correspondientes a derivados de sistemas de archivos FAT[9].

4.1.4.4. Identificar los eventos del sistema relevantes

La etapa de recolección de este marco de trabajo establece puntos específicos para obtener los registros de actividad del dispositivo. En base a esto se dispondrá como

[7]inodo: Es una estructura de datos propia de los sistemas de archivos tradicionalmente empleados en los sistemas operativos tipo UNIX.
[8]CSV: Comma Separated Values, o Valores Separados por Comas
[9]FAT: File Allocation Table, o Tabla de Ubicación de archivos

mínimo de los siguientes archivos de registro:

- dmesg.text
- logcat.text
- dumpsys.text

Para este punto de trabajo se deberá verificar su existencia en la evidencia y validar su integridad con los registros del inventario, en caso de encontrar alguna inconsistencia se procederá a documentar la misma y dar la notificación pertinente a las partes involucradas.

Cuando la evidencia sea confiable deberá evaluarse si el alcance de la pericia requiere que se analice el contenido de estos archivos, lógicamente y según la necesidad se revisara el archivo pertinente.

A modo de referencia recordaré que el archivo *dmesg.text* contiene la información originada por el núcleo del sistema que será de suma utilidad para comprender los procesos centrales iniciados, los controladores en ejecución, e información vinculada al sistema como errores en la ejecución de los módulos del núcleo del sistema y hardware asociado a estos. El contenido de *logcat.text* mostrará la información de la bitácora o registro de las aplicaciones en ejecución, la lectura de este archivo permite determinar gran cantidad de operaciones realizadas con el dispositiv. A continuación se citan algunos ejemplos:

- Primer acceso al "Escritorio" del dispositivo

```
1 I/ActivityManager(  51): Displayed activity com.android.
    launcher/.Launcher: 1973987 ms (total 1973987 ms)
```

- Acceso a la aplicación de "Contactos"

```
1 I/ActivityManager(  51): Starting activity: Intent { act=
    android.intent.action.MAIN cat=[android.intent.category.
    LAUNCHER] flg=0x10200000 cmp=com.android.contacts/.
    DialtactsContactsEntryActivity bnds=[62,215][118,274] }
```

- Por último el archivo *dumpsys.text* contiene la información de diferentes áreas o servicios del sistema, entre ellos fondos de escritorio, teléfono, WiFi, ubicación, alarmas, etc. Una manera practica de obtener la posición o linea de inicio para cada sección en el archivo es con la siguiente instrucción:

```
# cat dumpsys.text | grep -n DUMP
```

4.1.4.5. Analizar la información de la agenda Android

Durante esta instancia se buscará la información asociada a los contactos del repositorio del sistema operativo Android. Con tal fin se extrae de la evidencia el archivo *data/data/com.android.providers.contacts/databases/contacts2.db* que será manejado mediante el cliente de SQL Lite versión 3, dado que su información corresponde a una base de datos con el formato utilizado por este producto y que podrá consultarse con el lenguaje SQL estándar.

A modo de referencia se pueden observar las tablas que componen el modelo de esta base.

```
# sqlite3 contacts2.db
sqlite> .table
_sync_state                       status_updates
_sync_state_metadata              v1_settings
activities                        view_contacts
agg_exceptions                    view_contacts_restricted
android_metadata                  view_data
calls                             view_data_restricted
contact_entities_view             view_groups
contact_entities_view_restricted  view_raw_contacts
contacts                          view_raw_contacts_restricted
data                              view_v1_contact_methods
groups                            view_v1_extensions
mimetypes                         view_v1_group_membership
name_lookup                       view_v1_groups
nickname_lookup                   view_v1_organizations
```

```
17 packages                              view_v1_people
18 phone_lookup                          view_v1_phones
19 raw_contacts                          view_v1_photos
20 settings
```

Con fines prácticos, se podrá observar un ejemplo que nos muestra como en el siguiente cuadro se obtiene la información sobre los contactos registrados detallando sus datos particulares, entre ellos el número telefónico y la cantidad de veces que han sido utilizados

```
1 # sqlite3 contacts2.db
2 sqlite> .header on
3 sqlite> SELECT raw_contacts.account_name, raw_contacts.display_name,
      phone_lookup.normalized_number, raw_contacts.times_contacted
    FROM raw_contacts, phone_lookup WHERE raw_contacts._id =
    phone_lookup.raw_contact_id;
```

4.1.4.6. Analizar la información de las aplicaciones de agenda/contactos específicas

Cuando la pericia solicite extender el trabajo de análisis de la agenda de contactos a otras aplicaciones específicas se deberá proceder de la siguiente manera:

- Identificar las aplicaciones que puedan contener información de esta índole.
- Si el alcance no esta acotado se deberán repetir los siguientes casos para cada aplicación, en caso de estar acotada el perito se limitara a aquellas aplicaciones indicadas en la solicitud que existen en el dispositivo (en referencia a la información del punto previo).
- Identificar él o los archivos de almacenamiento de datos de la aplicación.
- Extraer él o los archivos de la imagen de partición en uso.
- Analizar el contenido para determinar el formato de almacenamiento y extraer los datos de relevancia para el proceso.

4.1.4.7. Analizar la información de telefónica de Android

En este punto se analizará la información de las comunicaciones telefónicas realizadas con el dispositivo, dicha información reside en el archivo *data/data/-com.android.providers.contacts/databases/contacts2.db*, por lo que deberá ser extraído de la evidencia para ser utilizado con la herramienta *SQLite*.

El siguiente cuadro muestra, a modo de ejemplo, una extracción de la información de llamados.

```
# sqlite3 contacts2.db
sqlite> .header on
sqlite> select _id,number,strftime("%Y-%m-%d %H:%M:%S", date/1000, '
   unixepoch','localtime'),duration,type,new,name,numbertype,
   numberlabel from CALLS;
```

4.1.4.8. Analizar la información de las aplicaciones VoIP especificas

Debido a la masificación de la tecnología de comunicación de VoIP[10] es probable que muchas pericias deban incluir el análisis de aplicaciones que implementan esta solución para realizar llamadas de voz con dispositivos móviles Android. En este contexto se deberá proceder de la siguiente manera:

- Identificar las aplicaciones que puedan contener información de esta índole.
- Si el alcance no esta acotado se deberán repetir los siguientes casos para cada aplicación, en caso de estar acotada el perito se limitara a aquellas aplicaciones indicadas en la solicitud que existen en el dispositivo (en referencia a la información del punto previo).
- Identificar el o los archivos de almacenamiento de datos de la aplicación.
- Extraer el o los archivos de la imagen de partición en uso.

[10]VoIP: Voice over Internet Protocol, o Voz sobre IP

- Analizar el contenido para determinar el formato de almacenamiento y extraer los datos de relevancia para el proceso.

Un ejemplo de estas aplicaciones es el producto *Skype*, dicha aplicación almacena su información en el archivo */data/data/com.skype.raider/files/<user>/main.db*, que como indica su extensión es de tipo base de datos y análogamente con el resto de las aplicaciones de la plataforma puede accederse con la herramienta SQLite para consultar sus tablas mediante lenguaje SQL.

4.1.4.9. Analizar la información de mensajería de Android

En este paso se analizará la información relacionada con la mensajería sms del sistema Android, la información sobre la misma reside en el archivo */data/data/-com.android.providers.telephony/databases/mmssms.db*, y por esta razón deberá ser extraído de la evidencia para su análisis con la herramienta SQLite mediante el uso de consultas SQL.

El siguiente cuadro muestra un ejemplo practico de conexión a dicha base y el listado de tablas disponibles en su esquema de datos:

```
# sqlite3 contacts2.db
sqlite> .table
addr                  part                  sms
android_metadata      pdu                   sr_pending
attachments           pending_msgs          threads
canonical_addresses   rate
drm                   raw
```

El modelo de datos de esta aplicación esta basado en el seguimiento de las conversaciones entre este dispositivos y cada contacto externo, por lo que en primera instancia se buscarán los códigos de identificación de cada hilo de mensajes que representa una sucesión de mensajes entre estos dos actores. Esto puede realizarse con la siguiente instrucción:

```
# sqlite3 mmssms.db
```

```
2 sqlite> .header on
3 sqlite> SELECT _id, snippet FROM threads;
```

Identificado él o los identificadores de hilos de conversación a relevar se puede utilizar la siguiente instrucción consultar para obtener la información de los mensajes pertenecientes a dicho hilo en orden cronológico (Esta instrucción muestra un ejemplo para un hilo de conversión con identificador numero 3).

```
1 # sqlite3 contacts2.db
2 sqlite> .header on
3 sqlite> SELECT datetime(date/1000, 'unixepoch','localtime'), person,
      body FROM sms WHERE thread_id = 3 ORDER BY date;
```

O de forma genérica obtener todo el registro de actividad mediante la siguiente instrucción.

```
1 # sqlite3 contacts2.db
2 sqlite> .header on
3 sqlite> Ssqlite> select _id, thread_id, type, address, strftime("%Y
    -%m-%d %H:%M:%S", date/1000, 'unixepoch','localtime') as date,
    read, subject, body from sms;
```

4.1.4.10. Analizar la información de las aplicaciones de mensajería específicas

En este rubro de aplicaciones han aparecido numerosos productos que proveen funcionalidades similares para el uso de mensajería. Cada uno de ellos dispone de su propio criterio para definir su modelo de datos, formatos de almacenamiento y cifrado de datos. Por esta razón, cada caso será particular y estará sujeto al criterio del perito, quien deberá detallar y documentar la metodología y procedimientos a utilizar.

En este contexto se deberá proceder de la siguiente manera:

- Identificar las aplicaciones que puedan contener información de esta índole.
- Si el alcance no esta acotado se deberán repetir los siguientes casos para cada

aplicación, en caso de estar acotada el perito se limitara a aquellas aplicaciones indicadas en la solicitud que existen en el dispositivo (en referencia a la información del punto previo).

- Identificar él o los archivos de almacenamiento de datos de la aplicación.

- Extraer él o los archivos de la imagen de partición en uso.

- Analizar el contenido para determinar el formato de almacenamiento y extraer los datos de relevancia para el proceso.

A continuación detallaré un caso de referencia que muestra como se debe acceder a la información de la reconocida aplicación de mensajería *WhatsApp* y como la misma ha variado su metodología de almacenamiento con sus diferentes versiones. Cabe destacar que la información a desarrollar en los siguientes párrafos esta sujeta a las variaciones de cada versión de la aplicación, pero su objetivo se limita a brindar una referencia practica para este tipo de casos.

En concreto, la aplicación *WhatsApp* utiliza dos puntos de almacenamiento para la información del usuario, estos son

- /data/data/com.whatsapp/databases/wa.db

- /data/data/com.whatsapp/databases/msgstore.db

El primero contiene la información referente a los contactos mientras que el segundo almacena los datos propios de la mensajería como los mensajes y archivos adjuntos. A continuación se muestra un ejemplo de la estructura de datos para cada archivo

wa.db	**msgstore.db**
android_metadata	chat_list
locale	_id
wa_contacts	key_remote_jid
id	message_table_id
jid	messages
is_whatsapp_user	_id
is_iphone	key_remote_jid
status	key_from_me
number	key_id
raw_contract_id	status
display_name	needs_push
phone_type	data
phone_label	timestamp
unseen_msg_count	media_url
photo_ts	media_mime_type
sqlite_sequence	media_wa_type
name	media_size
seq	media_name
	latitude
	longitude
	thumb_image
	remote_resource
	received_timestamp
	send_timestamp
	receipt_server_timestamp
	receipt_device_timestamp
	sqlite_sequence
	name
	seq

Cuadro 4.5: Whatsapp - Estructura de bases de datos

Con esta información del modelo, que es bastante descriptiva y posee un solo nivel, se podrá fácilmente obtener la información deseada mediante el uso de SQL en sqlite3, al igual que con el resto de las bases datos. Por esta razón centraré la atención de los próximos párrafos en la criptografía que protege esta información.

La evolución de este producto ha implementado diferentes metodologías para proteger esta información, se podrá identificar su implementación a través del cambio e extensión, por ejemplo del clásico *.db* a *.db.crypt5*, donde el último dígito identifica el método de cifrado.

Como primer caso con almacenamiento cifrado tomaré el formato mas antiguo y simple siendo el objeto de trabajo el archivo *msgstore.db.crypt*. En este caso la implementación para el cifrado es muy básica utilizando el algoritmo AES[11] en 192 bits con modo ECB[12] para cifrar la base de sqlite, y tomando como contraseña un valor fijo para todos los clientes; este valor corresponde a *346a23652a46392b4d73257c67317e352e3372482177652c*. En este escenario se podrá utilizar cualquier herramienta de cifrado que soporte el algoritmo para descifrar el archivo obteniendo como resultado la base de sqlite para ser manejada normalmente. A continuación se muestra como realizar esta operación median el uso de OpenSSL[13]

```
1 openssl enc -d -aes-192-ecb -in msgstore.db.crypt -out msgstore.db -
    K 346a23652a46392b4d73257c67317e352e3372482177652c
```

El segundo caso a analizar es el correspondiente al archivo *msgstore.db.crypt5*, este formato es una mejora sobre el anterior incrementando la complejidad de la implementación al cambiar el modo de cifrado de ECB a CBC[14] y utilizando una clave derivada del nombre de la cuenta; estos cambios eliminan el uso de la contraseña fija y cambian el algoritmo de cifrado a AES-192-CBC. En base a estos cambios se incorpora un vector de inicialización fijo y una clave base fija que se opera con XOR[15] sobre el código de

[11] AES: Advanced Encryption Standard
[12] ECB: Electronic Code Book, corresponde a un modo básico para el cifrado de bloques.
[13] OpenSSL:Es un paquete Open Source de herramientas de administración y bibliotecas relacionadas con la criptografía
[14] CBC: Cipher Block Chaining, modo de cifrado de bloque con distorsión generada en base a un vector de inicializacion.
[15] XOR: Operación binaria, OR excluyente.

hash MD5[16] resultante para el nombre de la cuenta, estos valores son:

Clave base	[0x8d, 0x4b, 0x15, 0x5c, 0xc9, 0xff, 0x81, 0xe5, 0xcb, 0xf6, 0xfa, 0x78, 0x19, 0x36, 0x6a, 0x3e, 0xc6, 0x21, 0xa6, 0x56, 0x41, 0x6c, 0xd7, 0x93]
Vector de inicialización	[0x1E, 0x39, 0xF3, 0x69, 0xE9, 0xD, 0xB3, 0x3A, 0xA7, 0x3B, 0x44, 0x2B, 0xBB, 0xB6, 0xB0, 0xB9]

Cuadro 4.6: Información de la implementación criptográfica para db.crypt5

Debido a los cambios descriptos el proceso de descifrado requiere mas pasos, el siguiente script de python ha sido desarrollado para automatizarlos:

```
1  #!/usr/bin/env python
2  """
3  48bits presents:
4  8================================================D~~~
5  WhatsApp msgstore crypt5 decryptor by grbnz0 and nullsub
6  8================================================D~~~
7  """
8  import sys
9  import hashlib
10 import StringIO
11 from M2Crypto import EVP
12
13 key = bytearray([141, 75, 21, 92, 201, 255, 129, 229, 203, 246, 250,
       120, 25, 54, 106, 62, 198, 33, 166, 86, 65, 108, 215, 147])
14 iv = bytearray([0x1E,0x39,0xF3,0x69,0xE9,0xD,0xB3,0x3A,0xA7,0x3B,0
      x44,0x2B,0xBB,0xB6,0xB0,0xB9])
15
16 def decrypt(db,acc):
17   fh = file(db,'rb')
18   edb = fh.read()
19   fh.close()
20   m = hashlib.md5()
21   m.update(acc)
```

[16]MD5: Algoritmo de hash

```
22   md5 = bytearray(m.digest())
23   for i in xrange(24): key[i] ^= md5[i&0xF]
24   cipher = EVP.Cipher('aes_192_cbc', key=key, iv=iv, op=0)
25   sys.stdout.write(cipher.update(edb))
26   sys.stdout.write(cipher.final())
27
28 if __name__ == '__main__':
29   if len(sys.argv) != 3:
30     print 'usage %s   > decrypted.db' % sys.argv[0]
31   else:
32     decrypt(sys.argv[1],sys.argv[2])
```

Citando el ejemplo de sus autores, puede ser ejecutado de la siguiente forma para descifrar la base de SQLite

```
1 $ python pwncrypt5.py msgstore.db.crypt5 grbnz0@gmail.com > msgstore
    .db
```

Como último ejemplo desarrollaré el caso para el archivo **msgstore.db.crypt7**, como es de esperar corresponde a una evolución del previo y el proceso es mas complejo. Los cambios en el formato han sido los siguientes:

- El algoritmo de cifrado elegido es AES de 256 bits operado en modo CBC.
- Se reemplazo el modelo de gestión para clave-vector de inicialización anterior, ahora ambos valores se almacenan en el archivo */data/data/com.whatsapp/files/key*, que solo puede ser accedido con nivel root, por lo que permanece almacenado en esta ubicación considerada segura.
- El archivo contiene una cabecera adicional en su formato cifrado.

El proceso se iniciará obteniendo el archivo */data/data/com.whatsapp/files/key*, a partir de este punto se procederá a extraer los valores correspondientes a la clave y el vector de inicialización. Para la contraseña se puede utilizar la siguiente instrucción que entregara el valor buscado como una cadena hexadecimal de 64 caracteres, a fin de cumplir con los 256 bits esperados; esta instrucción lee desde el offset 0x7E hasta el

0x9D, el formato de este archivo establece que este el espacio para el almacenamiento de la contraseña.

```
$ hexdump -e '2/1 "%02x"' key | cut -b 253-316
```

Luego se procederá a buscar el valor del vector de inicialización de 128 bits o 32 dígitos hexa-decimales, el mismo se encuentra en el espacio inmediatamente anterior a la contraseña.

```
$ hexdump -e '2/1 "%02x"' key | cut -b 221-252
```

El siguiente paso es preparar el archivo *msgstore.db.crypt7* para su descifrado, con tal fin se deberán remover los primeros 67 bytes que corresponden al *header* o cabecera de datos adicionado en el cifrado, que entre otras cosas incluye el vector de inicialización en el offset 0x34 a 0x42. Realizaré esta operación con la siguiente instrucción:

```
$ dd if=msgstore.db.crypt7 of=msgstore.db.crypt7.nohdr ibs=67 skip=1
```

Por ultimo se utilizara OpenSSL para descifrar el archivo mediante la siguiente instrucción donde $k es la contraseña y $iv el valor del vector de inicialización.

```
$ openssl enc -aes-256-cbc -d -nosalt -nopad  -bufsize 16384 -in
   msgstore.db.crypt7.nohdr -K $k -iv $iv > msgstore.db
```

4.1.4.11. Identificar los elementos de imagen sonido o vídeo

En este punto se buscará identificar la información de sonido y vídeo almacenada y/o capturada por el dispositivo. El origen de datos de la misma serán las imágenes de partición disponibles en la evidencia.

La realización de esta búsqueda puede completarse montando las imágenes de partición y realizando búsquedas directas sobre el mismo para los formatos de imágenes, sonidos y vídeos reconocidos, como por ejemplo jpeg, avi, mpeg, png, wav, mp3.... etc. Cabe destacar que el conjunto de formatos seleccionados debe ser enumerado y documentado, además de considerar que puede estar acotado por el alcance de la pericia.

4.1.4.12. Identificar los elementos del tipo especifico

Cuando la pericia solicite la identificación y análisis de formatos particulares o específicos se deberá proceder a listar los mismos y aplicar la misma metodología utilizada para los tipos comunes (imagen, sonido y vídeo). Lógicamente el análisis del contenido estará sujeto a las particularidades de cada formato y no puede ser descripto de manera genérica, la metodología y alcance quedara sujeta al criterio del perito con el fin de alcanzar u obtener la solicitud formalizada en la solicitud de la pericia.

4.1.4.13. Identificar las aplicaciones vinculadas a la información

Cuando la pericia requiera información sobre aplicaciones particulares que no han sido contempladas en los pasos previos se deberá proceder a identificar la existencia de las mismas en los registros de software de la evidencia. Dicha tarea se realiza con el fin de verificar su disponibilidad en el resto de los elementos que componen la evidencia y proceder a definir la metodología de análisis a utilizar para cada caso en particular.

4.1.4.14. Identificar los repositorios de datos para las aplicaciones afectadas

Para cada aplicación particular a analizar se deberá identificar los puntos de almacenamiento de información utilizados, y el formato de los mismos. De esta forma, quedaran documentados para su posterior análisis.

Cabe destacar que por la naturaleza de la tarea y la gran diversidad de aplicaciones no es posible estandarizar la tarea en cuestión.

4.1.4.15. Analizar la información de las aplicaciones

Al igual que en secciones previas que se enfocan al análisis de información para aplicaciones particulares, muy comunes en el entorno de Android, no es viable definir un único procedimiento por lo que en este contexto se deberá proceder de la siguiente manera:

- Identificar las aplicaciones que puedan contener información de esta índole.

- Si el alcance no esta acotado se deberán repetir los siguientes casos para cada aplicación, en caso de estar acotada el perito se limitara a aquellas aplicaciones indicadas en la solicitud que existen en el dispositivo (en referencia a la información del punto previo).

- Identificar el o los archivos de almacenamiento de datos de la aplicación.

- Extraer el o los archivos de la imagen de partición en uso.

- Analizar el contenido para determinar el formato de almacenamiento y extraer los datos de relevancia para el proceso.

4.1.4.16. Formalizar la documentación

Esta etapa documentará su desarrollo en dos documentos:

- Ficha de análisis pericial, este documento dispone de una sección principal para detallar el "Análisis Pericial" realizado, en este documento se registraran las diferentes tareas técnicas realizadas. El objetivo de este documento es tener un registro sobre la manera en que se han obtenido datos para los diferentes puntos de análisis de la pericia.

- Ficha de linea de tiempo, en este documento se podrá registrar la información resultante del análisis, el formato del documento tiene por finalidad facilitar su lectura e interpretación mediante su ocurrencia temporal, característica y origen; cabe destacar que el orden sugerido es descendente en función del campo "Fecha-Hora", no obstante el mismo no es mandatorio ya que se espera que esta información pueda ser extraída y reutilizada por otras herramientas si el volumen y complejidad de los datos lo requieren.

Campo	Detalle
Fecha-Hora	Fecha y hora del evento registrado. Para datos de importancia para la pericia que no puedan estar asociados a su evento de creación este campo podrá quedar vació.
Tipo	Tipo de dato y/o evento.
Aplicación	Aplicación responsable del evento y/o almacenamiento de los datos
Detalle	Explicación o detalle sobre la información o situación analizada.

Cuadro 4.7: Tabla con referencias para la documentacion

4.1.5. Etapa 5

Esta última etapa es la encargada de preparar la presentación de las conclusiones y el reporte final del trabajo pericial realizado en las etapas previas.

Figura 4.8: Etapa número cinco

4.1.5.1. Generación del reporte Final

En este punto se tomará como entrada a los documentos disponibles que han sido generados en la etapa cuatro mas el soporte de la etapa uno, relacionado con las formas y limites del alcance de la pericia solicitada.

En base a esta información el perito deberá redactar el entregable de esta etapa, que podrá basarse en la plantilla de "Reporte Final" del marco de trabajo, disponible en el Anexo B de este documento. En él constarán los detalles de interés para la pericia mas los hechos que respaldan las declaraciones expresadas por el perito basado en la evidencia que fue objeto del proceso.

4.1.5.2. Entrega del Resultado pericial

El marco de trabajo sugiere como entregable final al documento titulado como "Reporte Final" basado en las plantillas de este documento, esperando que el mismo contenga la información requerida en la pericia. No obstante existirán situaciones donde las formalidades requieran cumplir con otros formatos o inclusive soliciten anexar información particular que podrá ser referida al resto de la información recopilada y documentada en la pericia. Es por esta razón que se contempla esta etapa de entrega del resultado pericial donde deben realizarse las acciones necesarias para cumplir con las formalidades de entrega de la pericia ya sea en el ámbito judicial o privado.

Capítulo 5

Validación

5.1. Pruebas

5.1.1. Descripción y tamaño de las muestras; limitaciones que esto impone al estudio

Las muestras consideradas para este estudio se encuentran contempladas dentro del siguiente conjunto, el mismo se divide en dos grupos primarios descriptos a continuación:

5.1.1.1. Dispositivos virtuales o emulados :

El marco de referencia sera aplicable a los estudios descriptos en este documento con el fin de proveer cobertura sobre diversas versiones del sistema operativo Android contempladas en el alcance del mismo. Sin embargo estas plantean limitaciones asociadas a personalizaciones o particularidades del entorno (como son los componentes y controladores del hardware de un dispositivo real), al mismo tiempo que no serán representativas de entornos con protección de acceso como root o administrador.

Se puede citar como referencia del alcance al conjunto de muestras de esta categoría que estará comprendido por los siguientes elementos

- Entorno virtual con Android 2.1 (API 7)

- Entorno virtual con Android 2.2 (API 8)
- Entorno virtual con Android 2.3.3 (API 10)
- Entorno virtual con Android 3.0 (API 11)

Los entornos virtuales serán configurados con el sistema operativo correspondiente a la versión de cada muestra prevista según se listó previamente. Al mismo tiempo se dispondrá de las siguientes características de configuración en el AVD[1]:

- 512 Mega-bytes de memoria RAM.
- Sin teclado de hardware presente.
- 64 Mega-bytes de VM heap.
- Pantalla de 7 pulgadas.
- Sin cámaras para captura de imágenes.
- Tarjeta SD de 1 Giga-byte de capacidad.

5.1.1.2. Dispositivos físicos:

Los dispositivos utilizados para estas muestras se verán sujetos a las limitaciones propias de su hardware y la personalización que el sistema sufre por parte del fabricante para implementar su uso en cada dispositivo. Esta situación condiciona el libre acceso administrativo y en consecuencia la capacidad de efectuar determinadas operaciones sobre la muestra.

5.1.2. Definición de las variables

Las variables a contemplar en este estudio estarán dadas por los siguientes elementos de salida:

[1] AVD:Android Virtual Device, o Dispositivo Virtual Android

- Cantidad de mensajes texto entrantes o salientes recuperados.
- Cantidad de información de llamados entrantes o salientes recuperados.
- Cantidad de contactos recuperados.
- Cantidad de archivos existentes recuperados de la memoria de almacenamiento.
- Cantidad de archivos eliminados recuperados de la memoria de almacenamiento.

Las variables de entrada se dadas por los registros de contactos, mensajes y llamados se ajustaran al siguiente conjunto de datos generados por el software del anexo A.

5.1.2.1. Registros de contactos

La variable de entrada de registros de contacto estará compuesta por diez entradas enumeradas en el siguiente cuadro:

Nombre	Número telefónico
Luminosa Perales Saldivar	00000001
Elias Mota Ozuna	11111111
Saul Aguirre Lujan	22222222
Macra Veliz Pineda	33333333
Ursy Marín Sierra	44444444
Betty Guevara Arreola	55555555
Ulpiano Suarez Anguiano	66666666
Isaias Montés Colón	77777777
Crispina Narvaez Melendez	88888888
Publia Muro Villalpando	99999999

Cuadro 5.1: Tabla de registro de contactos

5.1.2.2. SMS Recibidos

La variable de entrada de SMS[2] recibidos se compondrá de nueve entradas correspondientes a mensajes enviados desde diversos orígenes hacia el dispositivo de la muestra. El conjunto de datos a aplicar se encuentra detallado en la siguiente tabla:

[2]SMS: Short Message Systems, o Sistema de Mensajes Cortos

Número del emisor	Texto del mensaje
44444444	La fortuna juega en favor de una mente preparada
22222222	En teoria no existe diferencia entre teoria y practica en la practica si la hay
77777777	Ninguna ciencia en cuanto a ciencia engana el engano esta en quien no sabe
00000001	La ciencia mas peligrosa es aquella que esta restringuida al dominio de los expertos
66666666	El conocimiento es la region inexplorada del manana
33333333	La tecnologia no nos ahorra tiempo pero su lo reparte de otra manera
44444444	El conocimiento es la region inexplorada del manana
55555555	La ciencia mas util es aquella cuyo fruto es el mas comunicable
00000000	En que consiste la ciencia? En conocer a los hombres

Cuadro 5.2: Tabla de SMS recibidos

5.1.2.3. SMS Enviados

La variable de entrada para emisión de mensajes contiene cuatro entradas correspondientes a mensajes emitidos desde el dispositivo de la muestra, a continuación se detallan dichas entradas.

Número del destinatario	Texto del mensaje
55555555	La verdadera ciencia ensena sobre todo a dudar y a ser ignorante
77777777	La felicidad no esta en la ciencia sino en la adquisicion de la ciencia
99999999	La ciencia es el alma de la prosperidad de las naciones y la fuente de todo progreso
22222222	El fin de la ciencia especulativa es la verdad y el fin de la ciencia practica es la accion

Cuadro 5.3: Tabla de SMS enviados

5.1.2.4. Llamadas telefónicas recibidas

La variable de entrada de llamadas telefónicas sera provista por diez entradas detalladas en la siguiente tabla:

Número de origen de la llamada	Situación
44444444	Aceptada
77777777	Rechazada
44444444	Aceptada
88888888	Rechazada
33333333	Aceptada
77777777	Rechazada
88888888	Aceptada
55555555	Rechazada
22222222	Aceptada
33333333	Rechazada

Cuadro 5.4: Tabla de llamadas recibidas

La medición de los resultados para este trabajo se verá sujeta a la metodología propuesta por el marco de trabajo y será aplicada de manera independiente a cada una de las muestras evaluadas. Dicha medición basada en la información de los registros documentales establecidos por el marco de trabajo (asociados a las plantillas del anexo B) y acotada a las variables del alcance de la investigación se registrará y evaluará con fines de comparación para determinar la confiabilidad del marco de trabajo.

5.2. Resultados obtenidos

Se procedió a la aplicación del marco de trabajo propuesto en el capitulo cuatro sobre un entorno virtual con Android 2.1, ejecutándose la prueba empírica correspondiente a una pericia de índole genérico y sin requisitos de información especifica o aplicaciones adicionales.

Las acciones y documentos entregables generados durante dicho procedimiento se han documentado en el Anexo E - “Pericia de referencia” de este mismo documento; cabe destacar que el objetivo de dicha pericia ha sido utilizar el marco de trabajo definido en este trabajo en conjunto con las herramientas y métodos técnicos sugeridos y

de libre acceso, para cumplir con esta tarea se procedió tanto con ejecuciones manuales como con la utilización de programas que faciliten las tareas repetitivas o de gran carga humana que conllevan un riesgo de falla mayor, el caso concreto corresponde al programa documentado en el Anexo D - "Programa para extracción de datos de bases sqlite y linea de tiempo", utilizado para facilitar la extracción de información de las bases de datos, manejo de la información de linea de tiempo y organización de los mismos.

El trabajo de aplicación del marco de trabajo encontró los siguientes puntos de atención en el entorno objetivo

- Se han encontrado inconvenientes para espejar las particiones internas del sistema de archivos principal del emulador. El proceso de acceso a las posiciones de memoria correspondientes al mismo retornan un error de lectura en las herramientas utilizadas.

- La automatización de eventos para componer el entorno de pruebas en esta versión del sistema emulado ha presentado anomalías, presentando demoras en su ejecución y dando como consecuencia la omisión o ejecución duplicada de algunos eventos. Ejemplos: se ha perdido la recepción de un SMS por lo que el conjunto de mensajes recibidos en el entorno de pruebas al terminar el proceso de preparación fue de siete entradas en lugar de las ocho previstas; para el caso de los envíos de SMS se han duplicado todos los eventos de este tipo generando ocho mensajes salientes en lugar de los cuatro previstos.

Estos puntos corresponden a anomalías circunstanciales relacionadas al entorno de pruebas emulado, si bien la muestra de entrada se ve afectada, esta situación no genera impacto en la aplicación del procedimiento o distorsión de los resultados obtenidos sobre los valores observados al iniciar en el entorno de pruebas al iniciar el procedimiento.

Salvando los inconvenientes detallados previamente se procedió a la ejecución de las etapas del marco de trabajo, siendo la etapa numero uno omitida por su naturaleza, ya que en este caso de estudio no hay documentación judicial o privada que de origen

a la solicitud de la pericia, limitaciones de su alcance o adicione requisitos específicos a la misma.

Como resultado de la ultima etapa se ha elaborado un reporte general a modo de sumario o síntesis de los resultados obtenidos por el marco de trabajo aplicado; su contenido es el siguiente:

La pericia, de índole genérico y sin solicitud de datos particulares, evidencia el registro de los siguientes contactos telefónicos en la agenda del dispositivo:

```
Nombre en la agenda, Numero telefónico, Cantidad de comunicaciones
Luminosa Perales Saldivar,10000000,0
Elias Mota Ozuna, 11111111, 0
Saul Aguirre Lujan, 22222222, 1
Macra Veliz Pineda, 33333333, 2
Ursy Marin Sierra, 44444444, 2
Betty Guevara Arreola, 55555555, 1
Ulpiano Suarez Anguiano, 66666666, 0
Isaias Montes Colon, 77777777, 2
Crispina Narvaez Melendez, 88888888, 2
Publia Muro Villalpando, 99999999, 0
```

Así mismo se registra actividad telefónica y de mensajería asociada a un subconjunto de números registrados en la agenda de contactos del dispositivo; se referencia a la documentación adjunta para los detalles y orden cronológico de los mismos.

Se ha identificado la existencia de archivos de imágenes en el espacio de almacenamiento del dispositivo, como también actividad vinculada a la eliminación de archivos. Los archivos de tipo especifico y aquellos eliminados que se han recuperado se encuentran en la documentación adjunta. Ellos son:

```
Archivos de tipo especifico, con codigo SHA-1:
016e60e49b8c22b5dd98b4df42ff9b45d5785fe5  android\_nombre.png
d197d660b45f19e0887becf8dae061545e368771  android\_paquete.jpg
Archivos eliminados, con codigo SHA-1:
af71221b724100af98280e0033f5e83948e77d11  pensamiento\_imagen.jpg
025ac2b6e2f3c30ffdc379996c7df5bcc025f507  legado.text
```

Se adjunta a este reporte la documentación correspondiente al relevamiento de Hardware y Software, Extracción de datos, Inventario y Ficha de Análisis realizado en este peritaje

Con esto ha finalizado de la aplicación del marco de trabajo propuesto y procedimientos sugeridos sobre un entorno emulado con las características y preparación detallada en este documento. Durante el proceso se han documentado todos los pasos y generado los documentos sugeridos mediante las plantillas disponibles en el Anexo B –"Material de soporte para el procedimiento" de este documento.

5.3. Calidad de la solución

La confiabilidad de la medición quedara sujeta a las condiciones de la prueba, dado que los objetos de evaluación corresponden a dispositivos utilizados solamente para este estudio podrá ser considerada alta sobre el software estándar de los mismos.

5.4. Dificultades encontradas

La validación de la solución aplicada encontró solamente dificultades técnicas asociadas a las limitaciones propias del entorno emulado sobre el cual se realizo la ejecución del trabajo.

5.5. Contribución

La contribución especifica que se ha realizado corresponde a la definición del marco de trabajo, incluyendo no solo las etapas con su orden y finalidad, sino también especificando la información a relevar junto con las plantillas para documentar cada tarea.

Capítulo 6

Conclusiones y futuras líneas de investigación

La experiencia de aplicar el marco de trabajo propuesto sobre un entorno emulado presenta diversas particularidades que dificultan su uso, sin embargo se ha demostrado que es posible realizar una pericia a un dispositivo Android de las versiones abarcadas utilizando la definición que provee este trabajo.

Los resultados obtenidos permiten observar que el marco definido provee como resultado una documentación consistente y trazable, cubriendo los diferentes aspectos técnicos y procesales que pueden afectar al proceso pericial, al mismo tiempo que logra con efectividad proveer la información de mayor relevancia en un formato simple, descriptivo y fácil de interpretar por los diferentes actores interesados en la información involucrada.

Conforme a la afirmación previa se ha demostrado que los procesos se han definido en base a una cobertura general sin excluir la posibilidad de adicionar acciones para alcances particulares, como aplicaciones o tipos de datos específicos. También es de interés destacar otro punto de valor agregado, que es el hecho de que las propuestas de índole técnico disponibles en cada etapa del marco de trabajo definido se han basado en herramientas de tipo Open-Source, de fácil disponibilidad y aplicación, generando así propuestas con efectividad demostrada que a la vez reducen las limitaciones técnicas

presentadas para validar resultados entre diferentes peritos o especialistas técnicos.

En términos generales la información provista en este documento, que incluye la definición del marco de trabajo es acorde a un modelo pericial actual, provee soporte a buenas practicas tanto para los procedimientos propios del área pericial como para los aspectos técnicos de los dispositivos móviles Android contando con la flexibilidad necesaria para utilizarse en el ámbito civil y judicial de la República Argentina.

Durante el desarrollo del presente documento se han identificado diversas lineas de investigación que dan lugar a continuar el trabajo realizado, algunas de ellas son:

- **Aplicación del marco de trabajo definido en nuevas versiones del sistema operativo Android**: Este trabajo ha sido acotado a un conjunto de versiones del sistema operativo Android, sin embargo el desarrollo esta plataforma es constante. Por esta razón y el hecho de que el marco de trabajo ha sido definido en forma genérica e independientemente de cualquier versión del sistema operativo, se considera factible investigar la aplicación del mismo en estas versiones no alcanzadas por este documento.

- **Extensión del trabajo de campo para un análisis cuantitativo de la efectividad del marco de trabajo en diferentes dispositivos**: Dado que el objeto de estudio corresponde a dispositivos móviles, existe una gran variedad de marcas y modelos sobre los cuales se puede aplicar el marco de trabajo y es por esta razón que se sugiere como una futura linea de investigación, la ampliación del conjunto de pruebas utilizando mas dispositivos reales.

Bibliografía

[pyr, 2013] (2013). The hottest mobile markets in latam.

[lat, 2013] (2013). Latam mobile market to grow by over 7 % in 2013. http://www.telecompaper.com/news/latam-mobile-market-to-grow-by-over-7-in-2013–923117.

[pyr, 2015] (2015). Lte on track to account for 4.2 % of latin america's total mobile subscriptions at year-end 2015.

[mob, 2015] (2015). Mobile phones the favorite device in argentina.

[hor, 2015] (2015). What's on the horizon for mobile.

[André Morum de L. Simao, 2011] André Morum de L. Simao, Fábio Caús Sícoli, L. P. d. M. F. E. d. D. R. T. d. S. J. (2011). Acquisition of digital evidence in android smarthphones.

[Cabrera, 2011] Cabrera, G. E. J. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles.

[Carrier and Spafford, 2003] Carrier, B. and Spafford, E. (2003). Getting physical with the digital investigation process. *IJDE - International Journal of Digital Evidence Fall*, 2.

[Casey, 2004] Casey, E. (2004). *Digital Evidence and Computer Crime*. Elsevier, second edition edition.

[Chiovenda, 1940] Chiovenda, G. (1940). *Instituciones de Derecho Procesal Civil*. Revista de Derecho Privado, Madrid.

[D. Brezinski, 2002] D. Brezinski, T. K. (2002). Guidelines for evidence collection and archiving. Technical report. RFC-3227.

[Darahuge, 2011] Darahuge, María Elena/Arellano González, L. E. (2011). *Manual de Informática Forense*. Errepar.

[Darahuge, 2012] Darahuge, María Elena/Arellano González, L. E. (2012). *Manual de Informática Forense II*. Errepar.

[Echandia, 1969] Echandia, H. D. (1969). Concepto, naturaleza y funciones jurídicas del documento en el ámbito procesal. *Revista Argentina de Derecho Procesal*, (3).

[Jansen and Ayers, 2007] Jansen, W. and Ayers, R. P. (2007). Sp 800-101. guidelines on cell phone forensics. Technical report, Gaithersburg, MD, United States.

[Jeff Lessard, 2010] Jeff Lessard, G. K. (2010). Android forensics: Simplifying cell phone examinations. *Small Scale Digital Device Forensics Journal*, 4(1).

[Kielmanovich, 2001] Kielmanovich, J. (2001). *Teoría de la Prueba y Medios Probatorios*. Rubinzal-Culzoni Editores, Argentina, 2ª edición edition.

[Trabajo colectivo de participantes del DFRWS por,] Trabajo colectivo de participantes del DFRWS por, Gary Palmer, C. M. A road map for digital forensic research.

[V. and Tushabe, 2004] V., B. and Tushabe, F. (2004). The enhanced digital investigation process model.

Apéndice A

Software para la preparación del objeto de análisis

El siguiente script fue desarrollado en Python con soporte de la librería pyadb, su finalidad es ingresar un conjunto predefinido de datos en un dispositivo Android.

```
1 #!/usr/bin/env python
2 # -*- coding: cp1252 -*-
3 #
4 #  preparar_android.py
5 #
6 #  Copyright 2014 Walter R. Ureta <wureta@gmail.com>
7 #
8 #
9 from pyadb import ADB
10 import time
11
12 adb_tool='/home/dagger/Downloads/android-sdk-linux/platform-tools/
      adb'
13
14 class DispositivoAndroid():
15     __adb = ADB(adb_tool)
16
17     def __init__(self):
```

```
18          #print self.__adb.pyadb_version()
19          self.__adb.wait_for_device()
20          None
21
22      def crearContacto(self, nombre, telefono):
23          print time.ctime() + "-> %s (%s)" % (nombre, telefono)
24          self.__adb.run_cmd("shell am start -a android.intent.action.
                INSERT -t vnd.android.cursor.dir/contact -e name \"%s\" -
                e phone %s" % (nombre, telefono) )
25          self.__adb.run_cmd("shell input keyevent 4")
26          self.__adb.run_cmd("shell input keyevent 4")
27          self.__adb.run_cmd("shell input keyevent 4")
28          time.sleep(3)
29          self.__adb.wait_for_device()
30
31      def recibirSMS(self, numero, texto):
32          print "-> " + texto
33          # Recibir[EMU]: sms send numero_de_telefono mensaje
34          self.__adb.run_emulator("sms send %s \"%s\"" % (numero,
                texto) )
35          time.sleep(4)
36          self.__adb.wait_for_device()
37
38      def enviarSMS(self, numero, texto):
39          print "-> " + texto
40          # Enviar[adb]: shell am start -a android.intent.action.
                SENDTO -d sms:CCXXXXXXXXXX --es sms_body "SMS BODY GOES
                HERE" --ez exit_on_sent true
41          time.sleep(3)
42          self.__adb.wait_for_device()
43          print self.__adb.shell_command("am start -a android.intent.
                action.SENDTO -d \"smsto:%s\" --es sms_body \"%s\" --ez
                exit_on_sent true" % (numero, texto))
44          time.sleep(3)
45          self.__adb.wait_for_device()
```

```
46          self.__adb.shell_command("input keyevent 66")
47          time.sleep(3)
48          self.__adb.wait_for_device()
49
50      def rechazarLlamada(self, numero):
51          print "-> " + str(numero)
52          # Llamar[EMU]: gsm call numero_de_telefono
53          print "gsm call %s" % numero
54          self.__adb.run_emulator("gsm call %s" % numero)
55          time.sleep(2)
56          self.__adb.wait_for_device()
57          # Cortar[EMU]
58          print "gsm cancel %s" % numero
59          self.__adb.run_emulator("gsm cancel %s" % numero)
60          self.__adb.wait_for_device()
61
62      def aceptarLlamada(self, numero):
63          print "-> " + str(numero)
64          # Llamar[EMU]
65          print "gsm call %s" % numero
66          self.__adb.run_emulator("gsm call %s" % numero)
67          self.__adb.wait_for_device()
68          time.sleep(2)
69          # Aceptar[EMU]
70          print "gsm accept %s" % numero
71          self.__adb.run_emulator("gsm accept %s" % numero)
72          time.sleep(5)
73          self.__adb.wait_for_device()
74          # Cortar[EMU]
75          print "gsm cancel %s" % numero
76          self.__adb.run_emulator("gsm cancel %s" % numero)
77          self.__adb.wait_for_device()
78
79      def navegar(self, url):
80          # Navegar[adb] shell am start -a android.intent.action.VIEW
```

```
            -d http://google.com
81          self.__adb.run_cmd("shell am start -a android.intent.action.
               VIEW -d %s" % url)
82          self.__adb.run_cmd("shell input keyevent 4")
83          time.sleep(3)
84
85      def posicionGeografica(self, lat, lon):
86          self.__adb.run_emulator("geo fix %s %s" % (lat, lon) )
87          time.sleep(3)
88
89      def info(self):
90          return "Serial  : " + str(self.__adb.get_serialno()).strip()
                + "\n" + \
91              "Target  : " + str(self.__adb.get_target_device()).strip
                   () + "\n" + \
92              "State   : " + str(self.__adb.get_state()).strip() + "\n
                   " + \
93              "Version : " + str(self.__adb.get_version()).strip()
94
95  def main():
96      print "Iniciando el proceso de carga de datos"
97      android = DispositivoAndroid()
98      print "Informacion general"
99      print android.info() + "\n"
100
101     # AGENDA
102     print "Creando contactos...."
103     android.crearContacto("Luminosa Perales Saldivar",'00000001')
104     android.crearContacto("Elias Mota Ozuna",'11111111')
105     android.crearContacto("Saul Aguirre Lujan",'22222222')
106     android.crearContacto("Macra Veliz Pineda",'33333333')
107     android.crearContacto("Ursy Marin Sierra",'44444444')
108     android.crearContacto("Betty Guevara Arreola",'55555555')
109     android.crearContacto("Ulpiano Suarez Anguiano",'66666666')
110     android.crearContacto("Isaias Montes Colon",'77777777')
```

```
111     android.crearContacto("Crispina Narvaez Melendez",'88888888')
112     android.crearContacto("Publia Muro Villalpando",'99999999')
113
114     # SMS
115     print "Recibiendo SMSs...."
116     android.recibirSMS('44444444',"La fortuna juega en favor de una
            mente preparada")
117     android.recibirSMS('22222222',"En teoria no existe diferencia
            entre teoria y practica en la practica si la hay")
118     android.recibirSMS('77777777',"Ninguna ciencia en cuanto a
            ciencia engana el engano esta en quien no sabe")
119     android.recibirSMS('00000001',"La ciencia mas peligrosa es
            aquella que esta restringuida al dominio de los expertos")
120     android.recibirSMS('66666666',"El conocimiento es la region
            inexplorada del manana")
121     android.recibirSMS('33333333',"La tecnologia no nos ahorra
            tiempo pero su lo reparte de otra manera")
122     android.recibirSMS('44444444',"El conocimiento es la region
            inexplorada del manana")
123     android.recibirSMS('55555555',"La ciencia mas util es aquella
            cuyo fruto es el mas comunicable")
124     android.recibirSMS('00000001',"En que consiste la ciencia? En
            conocer a los hombres")
125     print "Enviandondo SMSs...."
126     android.enviarSMS('55555555',"La verdadera ciencia ensena sobre
            todo a dudar y a ser ignorante")
127     android.enviarSMS('77777777',"La felicidad no esta en la ciencia
             sino en la adquisicion de la ciencia")
128     android.enviarSMS('99999999',"La ciencia es el alma de la
            prosperidad de las naciones y la fuente de todo progreso")
129     android.enviarSMS('22222222',"El fin de la ciencia especulativa
            es la verdad y el fin de la ciencia practica es la accion")
130
131     # LLAMADAS
132     print "Simulando llamadas...."
```

```
133     android.aceptarLlamada('44444444')
134     android.rechazarLlamada('77777777')
135     android.aceptarLlamada('44444444')
136     android.rechazarLlamada('88888888')
137     android.aceptarLlamada('33333333')
138     android.rechazarLlamada('77777777')
139     android.aceptarLlamada('88888888')
140     android.rechazarLlamada('55555555')
141     android.aceptarLlamada('22222222')
142     android.rechazarLlamada('33333333')
143
144     print "Fin del proceso de carga de datos"
145     return 0
146
147 if __name__ == '__main__':
148     main()
```

Apéndice B

Material de soporte para el procedimiento

Este apéndice mostrará las diferentes plantillas diseñadas con el fin de documentar las diferentes etapas del marco de trabajo propuesto.

B.1. Ficha de identificación de Hardware

Nro de Caso	**Juzgado**		**Lugar y fecha**	
Especificaciones del celular				
Marca				
Modelo				
Nro. de serie				
Garantía				
IMEI				
Nro. de teléfono				
Proveedor				
Otro				
Almacenamiento				
Cantidad	Tipo de memoria	Marca / Modelo	Velocidad / Capacidad	Numero de Serie
Accesorios y periféricos				
Observaciones generales:				
Perito informático forense			**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:				
			Firma: Aclaración:	

B.2. Ficha de identificación de Software

Nro de Caso	**Juzgado**		**Lugar y fecha**
Especificaciones del Sistema Operativo			
Tipo			
Versión			
Detalles			
Aplicaciones			
Nombre	Versión	Tipo	Comentarios
Observaciones generales:			
Perito informático forense		**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:			
		Firma: Aclaración:	

B.3. Ficha de datos adquiridos

Nro de Caso	**Juzgado**		**Lugar y fecha**
Datos Obtenidos			
Tipo	Almacenamiento	Hash	Comentarios
Observaciones generales:			
Perito informático forense		**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:			
		Firma: Aclaración:	

B.4. Fichas de conservación y cadena de custodia

A continuación se detallan las diferentes plantillas de documentos vinculadas a la cadena de custodia y el manejo de evidencias.

B.4.1. Inventario

Nro de Caso	**Juzgado**	**Lugar y fecha**
Inventario		
Numero	Tipo	Comentarios
Observaciones generales:		
Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

B.4.2. Rotulo de evidencias

Número	
Caso	
Fecha	
Tipo	
Observaciones	
Firma	

B.4.3. Recibo de efectos

Fecha	**Organismo**	**Numero de Caso**
Dirección	Ciudad/Provincia	Teléfono
Requiere consentimiento Si/No	Firma del Responsable del consentimiento	Rotulo
Descripción del elemento		
Numero de identificación		
Modelo		
P/N		
S/N		
Entrega Conforme		Firma
Recibe Conforme		Firma

B.4.4. Formulario para la cadena de custodia

Cadena de custodia de la evidencia					
Numero de Caso					
Numero de Identi-ficación	**Ubicación Actual**	**Fecha**	**Razón del traslado**	**Sitio adonde se traslada**	**Observa-ciones**
Entregado por:				**Firma y Aclaración**	
Recibido por:				**Firma y Aclaración**	
Lugar del deposito final de la evidencia:				**Fecha**	

B.5. Ficha de análisis pericial

Nro de Caso	**Juzgado**	**Lugar y fecha**
Análisis pericial		
Observaciones generales:		
Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

B.6. Ficha de linea de tiempo

Nro de Caso	**Juzgado**		**Lugar y fecha**
Linea de tiempo			
Fecha-Hora	Tipo	Aplicación	Detalle
Observaciones generales:			
Perito informático forense		**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:			
		Firma: Aclaración:	

B.7. Reporte Final

Nro de Caso	**Juzgado**	**Lugar y fecha**	
Reporte del perito			
.			
Perito informático forense		**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:			
		Firma: Aclaración:	

Apéndice C

Software para la obtención de información básica sobre Hardware y Software

El siguiente script fue desarrollado en Python con soporte de la librería pyadb, su finalidad es automatizar el acceso a la información básica que describe el hardware y software del dispositivo.

```
1 #!/usr/bin/env python
2 # -*- coding: utf-8 -*-
3 #
4 #  informacion_hard_soft.py
5 #
6 #  Copyright 2014 Walter R. Ureta <wureta@gmail.com>
7 #
8 from pyadb import ADB
9 import time
10
11 adb_tool='/home/dagger/Downloads/android-sdk-linux/platform-tools/
      adb'
12
13 class DispositivoAndroid():
```

```
14      __adb = ADB(adb_tool)
15      __lineas = 20
16
17      def __init__(self):
18          #print self.__adb.pyadb_version()
19          None
20
21      def info(self):
22          return "Serial  : " + str(self.__adb.get_serialno()).strip()
                + "\n" + \
23              "Target  : " + str(self.__adb.get_target_device()).strip
                   () + "\n" + \
24              "State   : " + str(self.__adb.get_state()).strip() + "\n
                   " + \
25              "Version : " + str(self.__adb.get_version()).strip()
26
27      def infoHardware(self):
28          message=""
29          message += "-"*self.__lineas + "Marca" + "-"*self.__lineas +
                "\n"
30          self.__adb.run_cmd("shell getprop ro.product.manufacturer")
31          message += self.__adb.get_output() + "\n"
32          message += "-"*self.__lineas + "Modelo" + "-"*self.__lineas
               + "\n"
33          self.__adb.run_cmd("shell getprop ro.product.model")
34          message += self.__adb.get_output() + "\n"
35          message += "-"*self.__lineas + "Nro. de serie" + "-"*self.
               __lineas + "\n"
36          self.__adb.run_cmd("shell getprop gsm.serial")
37          message +=  self.__adb.get_output() + "\n"
38          self.__adb.run_cmd("shell getprop ro.serialno")
39          message +=  self.__adb.get_output() + "\n"
40          message += "-"*self.__lineas + "Garantía" + "-"*self.
               __lineas + "\n"*3
41          message += "-"*self.__lineas + "IMEI" + "-"*self.__lineas +
```

```
            "\n"
42          self.__adb.run_cmd("shell dumpsys iphonesubinfo")
43          message += self.__adb.get_output() + "\n"
44          message += "-"*self.__lineas + "Nro. de teléfono" + "-"*self
                .__lineas + "\n"*3
45          message += "-"*self.__lineas + "Proveedor" + "-"*self.
                __lineas + "\n"
46          self.__adb.run_cmd("shell getprop gsm.sim.operator.alpha")
47          message += "\t" + self.__adb.get_output() + "\n"
48          self.__adb.run_cmd("shell getprop gsm.sim.operator.alpha.2")
49          message += "\t" + self.__adb.get_output() + "\n"
50          self.__adb.run_cmd("shell getprop gsm.sim.operator.alpha.3")
51          message += "\t" + self.__adb.get_output() + "\n"
52          self.__adb.run_cmd("shell getprop gsm.sim.operator.alpha.4")
53          message += "\t" + self.__adb.get_output() + "\n"
54          message += "-"*self.__lineas + "Otro" + "-"*self.__lineas +
                "\n"
55          self.__adb.run_cmd("shell getprop")
56          message += self.__adb.get_output() + "\n"
57          message += "-"*self.__lineas + "Información de
                almacenamiento" + "-"*self.__lineas + "\n"
58          self.__adb.run_cmd("shell df")
59          message += self.__adb.get_output() + "\n"
60          return message
61
62      def infoSoftware(self):
63          message = ""
64          message += "-"*self.__lineas + "Tipo" + "-"*self.__lineas +
                "\n"
65          message += "Android\n"
66          message += "-"*self.__lineas + "Versión" + "-"*self.__lineas
                 + "\n"
67          self.__adb.run_cmd("shell getprop ro.build.version.release")
68          message += self.__adb.get_output() + "\n"
69          self.__adb.run_cmd("shell getprop ro.build.version.sdk")
```

```
70          message += self.__adb.get_output() + "\n"
71          self.__adb.run_cmd("shell getprop ro.build.display.id")
72          message += self.__adb.get_output() + "\n"
73          self.__adb.run_cmd("shell getprop ro.build.date")
74          message += self.__adb.get_output() + "\n"
75          message += "-"*self.__lineas + "Detalles" + "-"*self.
               __lineas + "\n"
76          self.__adb.run_cmd("shell getprop")
77          message += self.__adb.get_output() + "\n"
78          message += "-"*self.__lineas + "Aplicaciones" + "-"*self.
               __lineas + "\n"
79          self.__adb.run_cmd("shell pm list packages -f")
80          message += self.__adb.get_output() + "\n"
81          return message
82
83  def main():
84      lineas = 20
85      print "Iniciando el proceso de extraccion de informacion sobre
           Hardware y Software"
86      android = DispositivoAndroid()
87      print "Informacion general"
88      print android.info() + "\n"
89
90      print "="*lineas + "Ficha de identificación de Hardware" + "="*
           lineas
91      print android.infoHardware()
92
93      print "="*lineas + "Ficha de identificación de Software" + "="*
           lineas
94      print android.infoSoftware()
95
96      print "Fin del proceso de carga de extraccion de informacion
           sobre Hardware y Software"
97      return 0
98
```

```
99 if __name__ == '__main__':
100     main()
```

Apéndice D

Software para la obtención de información sobre datos extraídos

El siguiente script fue desarrollado en Python con soporte de la librería para el manejo de bases de datos sqlite3, su finalidad es automatizar el análisis y presentación de la información correspondiente a las bases de información de contactos, telefonía, mensajería Android mas los datos de actividad en los sistemas de archivos

```
1  #!/usr/bin/env python
2  # -*- coding: utf-8 -*-
3  #
4  #  analizar_bases.py
5  #
6  #  Copyright 2014 Walter R. Ureta <wureta@gmail.com>
7  #
8  #
9  import sqlite3
10 import dateutil.parser
11 import datetime
12 import csv
13
14 def main():
15     output = []
```

```
16
17      # Procesa base de SMS/MMS Android
18      c = sqlite3.connect('mmssms.db')
19      c.row_factory = sqlite3.Row
20      for row in c.execute("select _id, thread_id, type, address,
            strftime('%Y-%m-%d %H:%M:%S', date/1000, 'unixepoch','
            localtime') as date, read, subject, body from sms"):
21          if row['type'] == 1:
22              detalle = "Mensaje entrante del numero %s." % row['
                    address']
23          elif row['type'] == 2:
24              detalle = "Mensaje saliente al numero %s." % row['
                    address']
25          else:
26              detalle = "Actividad de mensajeria desconocida, en
                    relacion al numero %s." % row['address']
27          output.append( "%s|Mensaje de texto|Mensajero Android|%s" %
                (row['date'], detalle) )
28      c.close()
29
30      # Procesa base de llamados Android
31      c = sqlite3.connect('contacts2.db')
32      c.row_factory = sqlite3.Row
33      for row in c.execute("select _id,number,strftime('%Y-%m-%d %H:%M
            :%S', date/1000, 'unixepoch','localtime') as date,duration,
            type,new,name,numbertype,numberlabel from CALLS"):
34          if row['type'] == 1:
35              detalle = "Llamada entrante del numero %s recibida de %s
                     segundos de duracion." % (row['number'],row['
                    duration'])
36          elif row['type'] == 3:
37              detalle = "Llamada entrante del numero %s rechazada o
                    invalida, %s segundos de duracion." % (row['number'],
                    row['duration'])
38          else:
```

```
39              detalle = "Actividad de telefonia desconocida, en
                    relacion al numero %s." % row['number']
40          output.append( "%s|Llamada telefonica|Telefono Android|%s" %
                (row['date'], detalle) )
41      c.close()
42
43      # Procesa el reporte de The Sleuth Kit
44      with open('reporte-actividad-fs.csv', 'rb') as f:
45          reader = csv.reader(f)
46          for row in reader:
47              try:
48                  tiempo = dateutil.parser.parse(row[0])
49                  tz = datetime.timedelta(hours = -3)
50                  tiempo = tiempo + tz
51                  comentario = ''
52                  if 'm' in row[2] or 'c' in row[2] :
53                      comentario += 'Archivo modificado, '
54                  if 'a' in row[2]:
55                      comentario += 'Archivo accedido, '
56                  if 'b' in row[2] :
57                      comentario += 'Archivo creado, '
58              output.append( "%s|Actividad de archivos|Sistema de
                    archivos|%s" % (tiempo.strftime("%Y-%m-%d %H:%M:%S"),
                    comentario + row[7]) )
59              except ValueError:
60                  None
61      #Orden la salida
62      output.sort()
63      for line in output:
64          print line
65      return 0
66
67  if __name__ == '__main__':
68      main()
```

Apéndice E

Evidencia del caso de prueba

Este anexo contiene la información correspondiente a la pericia realizada con la finalidad de demostrar la aplicación del marco de trabajo propuesto.

Entorno utilizado: Emulador Android 2.1

Limitaciones del entorno:

- Se han encontrado inconvenientes para espejar las particiones internas del sistema de archivos principal del emulador. El proceso de acceso a las posiciones de memoria correspondientes al mismo retornan un error de lectura en las herramientas utilizadas.

- La automatización de eventos para componer el entorno de pruebas en esta versión del sistema emulado ha presentado anomalías, presentando demoras en su ejecución y dando como consecuencia la omisión o ejecución duplicada de algunos eventos. Ejemplos: se ha perdido la recepción de un SMS por lo que el conjunto de mensajes recibidos en el entorno de pruebas al terminar el proceso de preparación fue de siete entradas en lugar de las ocho previstas. Para el caso de los envíos de SMS se han duplicado todos los eventos de este tipo generando ocho mensajes salientes en lugar de los cuatro previstos.

Las limitaciones enumeradas corresponden a anomalías circunstanciales relacionadas al entorno de pruebas emulado, si bien la muestra de entrada se ve afectada, esta

situación no genera impacto en la aplicación del procedimiento o distorsión de los resultados obtenidos sobre los valores observados al iniciar en el entorno de pruebas al iniciar el procedimiento.

E.1. Etapa 1

No aplica al caso dado que este trabajo se limita al alcance de la tesis en cuestión.

E.2. Etapa 2

Aislar la red:

No aplica el dispositivo en estudio corresponde a una unidad emulada en un entorno de software.

Extraer datos de la tarjeta de memoria y reemplazarla:

Se genero la imagen de la tarjeta utilizando el software *dc3dd*.

Obtener el equipo:

No aplica el dispositivo en estudio corresponde a una unidad emulada en un entorno de software.

Extraer información de los sistemas accesibles:

Se realizo la extracción de la información del sistema con las siguientes instrucciones

```
1 ./adb shell dmesg {\textgreater} ./dmesg.text
2 ./adb shell dumpsys {\textgreater} ./dumpsys.text
3 ./adb logcat -d -v time {\textgreater} ./logcat.text
```

Espejar particiones del sistema:

No se ha podido acceder al espacio de almacenamiento debido a errores de lectura generados en el entorno emulado.

Realizar un memory dump:

Se realizo la extracción de los procesos vinculados a aplicaciones con el procedimiento sugerido en la descripción del marco de trabajo.

Extraer datos del dispositivo:

Se han extraído los archivos con la información sugerida con los siguientes comandos

```
1 ./adb -e pull /data/data/com.android.providers.telephony/databases/
    mmssms.db /home/dagger/tesisLab/.
2 ./adb -e pull /data/data/com.android.providers.contacts/databases/
    contacts2.db /home/dagger/tesisLab/.
```

Documentar la adquisición de datos:

La información se documento utilizando las plantillas y programas *informacion_hard_soft.py* disponibles como anexos de este trabajo .

Nro de Caso	Juzgado	Lugar y fecha
1	Tesis de Maestría	Buenos Aires, 1 de Marzo 2014
Especificaciones del celular		
Marca	unknown	
Modelo	sdk	
Nro. de serie		
Garantía		
IMEI	DUMP OF SERVICE iphonesubinfo: Phone Subscriber Info: Phone Type = GSM Device ID = 000000000000000	
Nro. de teléfono		
Proveedor		
Otro	[ro.secure]: [0] [ro.allow.mock.location]: [1] [ro.debuggable]: [1] [persist.service.adb.enable]: [1] [ro.kernel.qemu.gles]: [0] [ro.kernel.qemu]: [1] [ro.kernel.console]: [ttyS0] [ro.kernel.android.qemud]: [ttyS1] [ro.kernel.android.checkjni]: [1] [ro.kernel.ndns]: [1] [ro.factorytest]: [0] [ro.serialno]: [] [ro.bootmode]: [unknown] [ro.baseband]: [unknown] [ro.carrier]: [unknown] [ro.bootloader]: [unknown] [ro.hardware]: [goldfish] [ro.revision]: [0] [ro.build.id]: [ECLAIR] [ro.build.display.id]: [sdk-eng 2.1-update1 ECLAIR 35983 test-keys] [ro.build.version.incremental]: [35983] [ro.build.version.sdk]: [7] [ro.build.version.codename]: [REL] [ro.build.version.release]: [2.1-update1] [ro.build.date]: [Thu May 6 09:06:12 PDT 2010] [ro.build.date.utc]: [1273161972] [ro.build.type]: [eng] [ro.build.user]: [android-build] [ro.build.host]: [android-test-13.mtv.corp.google.com]	

Otro	[ro.build.tags]: [test-keys] [ro.product.model]: [sdk] [ro.product.brand]: [generic] [ro.product.name]: [sdk] [ro.product.device]: [generic] [ro.product.board]: [] [ro.product.cpu.abi]: [armeabi] [ro.product.manufacturer]: [unknown] [ro.product.locale.language]: [ldpi] [ro.product.locale.region]: [] [ro.wifi.channels]: [] [ro.board.platform]: [] [ro.build.product]: [generic] [ro.build.description]: [sdk-eng 2.1-update1 ECLAIR 35983 test-keys] [ro.build.fingerprint]: [generic/sdk/generic/:2.1-update1/ECLAIR/35983:eng/test-keys] [rild.libpath]: [/system/lib/libreference-ril.so] [rild.libargs]: [-d /dev/ttyS0] [ro.config.notification_sound]: [OnTheHunt.ogg] [ro.config.alarm_alert]: [Alarm_Classic.ogg] [ro.setupwizard.mode]: [OPTIONAL] [xmpp.auto-presence]: [true] [ro.config.nocheckin]: [yes] [net.bt.name]: [Android] [net.change]: [net.dnschange] [ro.config.sync]: [yes] [dalvik.vm.stack-trace-file]: [/data/anr/traces.txt] [persist.sys.timezone]: [America/Buenos_Aires] [persist.sys.language]: [en] [persist.sys.country]: [US] [persist.sys.localevar]: [] [ro.FOREGROUND_APP_ADJ]: [0] [ro.VISIBLE_APP_ADJ]: [1] [ro.SECONDARY_SERVER_ADJ]: [2] [ro.BACKUP_APP_ADJ]: [2] [ro.HOME_APP_ADJ]: [4] [ro.HIDDEN_APP_MIN_ADJ]: [7] [ro.CONTENT_PROVIDER_ADJ]: [14] [ro.EMPTY_APP_ADJ]: [15] [ro.FOREGROUND_APP_MEM]: [1536] [ro.VISIBLE_APP_MEM]: [2048] [ro.SECONDARY_SERVER_MEM]: [4096]

Otro	[ro.BACKUP_APP_MEM]: [4096] [ro.HOME_APP_MEM]: [4096] [ro.HIDDEN_APP_MEM]: [5120] [ro.CONTENT_PROVIDER_MEM]: [5632] [ro.EMPTY_APP_MEM]: [6144] [net.tcp.buffersize.default]: [4096,87380,110208,4096, 16384,110208] [net.tcp.buffersize.wifi]: [4095,87380,110208,4096, 16384,110208] [net.tcp.buffersize.umts]: [4094,87380,110208,4096, 16384,110208] [net.tcp.buffersize.edge]: [4093,26280,35040,4096, 16384,35040] [net.tcp.buffersize.gprs]: [4092,8760,11680,4096, 8760,11680] [init.svc.console]: [running] [init.svc.servicemanager]: [running] [init.svc.vold]: [running] [init.svc.debuggerd]: [running] [init.svc.ril-daemon]: [running] [init.svc.zygote]: [running] [init.svc.media]: [running] [init.svc.installd]: [running] [init.svc.keystore]: [running] [init.svc.goldfish-setup]: [running] [init.svc.qemud]: [running] [init.svc.goldfish-logcat]: [stopped] [ARGH]: [ARGH] [net.eth0.dns1]: [10.0.2.3] [net.gprs.local-ip]: [10.0.2.15] [ro.radio.use-ppp]: [no] [status.battery.state]: [Slow] [status.battery.level]: [5] [status.battery.level_raw]: [50] [status.battery.level_scale]: [9] [ro.com.google.locationfeatures]: [1] [init.svc.adbd]: [running] [dalvik.vm.heapsize]: [64m] [ro.config.low_ram]: [true] [qemu.sf.lcd_density]: [160] [qemu.hw.mainkeys]: [0] [qemu.sf.fake_camera]: [back]

Otro	[init.svc.bootanim]: [stopped] [hw.keyboards.65536.devname]: [qwerty2] [sys.settings_secure_version]: [4] [dev.bootcomplete]: [1] [sys.settings_system_version]: [8] [gsm.version.ril-impl]: [android reference-ril 1.0] [gsm.sim.operator.numeric]: [] [gsm.sim.operator.alpha]: [] [gsm.sim.operator.iso-country]: [] [gsm.sim.state]: [UNKNOWN] [gsm.current.phone-type]: [1] [gsm.operator.alpha]: [] [gsm.operator.numeric]: [] [gsm.operator.iso-country]: [] [gsm.operator.isroaming]: [false] [gsm.nitz.time]: [1411175406751] [gsm.network.type]: [UMTS] [net.gprs.http-proxy]: [] [gsm.defaultpdpcontext.active]: [true] [net.dns1]: [10.0.2.3] [net.dnschange]: [2] [adb.connected]: [1]

Almacenamiento

Cantidad	Tipo de memoria	Marca / Modelo	Velocidad / Capacidad	Numero de Serie
1	MicroSD	No disponible / SD-C01G	No disponible/ 1 Gigabyte	0948RB16638

Accesorios y periféricos

Observaciones:
/dev: 258264K total, 0K used, 258264K available (block size 4096)
/sqlite_stmt_journals: 4096K total, 0K used, 4096K available (block size 4096)
/system: 198656K total, 74636K used, 124020K available (block size 4096)
/data: 198656K total, 41648K used, 157008K available (block size 4096)
/cache: 65536K total, 1156K used, 64380K available (block size 4096)

Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

Nro de Caso	**Juzgado**	**Lugar y fecha**
1	Tesis de Maestría	Buenos Aires, 1 de Marzo 2014
Especificaciones del Sistema Operativo		
Tipo	Android	
Versión	2.1-update1 7 sdk-eng 2.1-update1 ECLAIR 35983 test-keys Thu May 6 09:06:12 PDT 2010	
Detalles		
Aplicaciones		
Nombre	Versión	Tipo	Comentarios

Observaciones generales:
[[ro.secure]: [0]
[ro.allow.mock.location]: [1]
[ro.debuggable]: [1]
[persist.service.adb.enable]: [1]
[ro.kernel.qemu.gles]: [0]
[ro.kernel.qemu]: [1]
[ro.kernel.console]: [ttyS0]
[ro.kernel.android.qemud]: [ttyS1]
[ro.kernel.android.checkjni]: [1]
[ro.kernel.ndns]: [1]
[ro.factorytest]: [0]
[ro.serialno]: []
[ro.bootmode]: [unknown]
[ro.baseband]: [unknown]
[ro.carrier]: [unknown]
[ro.bootloader]: [unknown]
[ro.hardware]: [goldfish]
[ro.revision]: [0]
[ro.build.id]: [ECLAIR]
[ro.build.display.id]: [sdk-eng 2.1-update1 ECLAIR 35983 test-keys]
[ro.build.version.incremental]: [35983]
[ro.build.version.sdk]: [7]
[ro.build.version.codename]: [REL]
[ro.build.version.release]: [2.1-update1]

```
[ro.build.date]: [Thu May 6 09:06:12 PDT 2010]
[ro.build.date.utc]: [1273161972]
[ro.build.type]: [eng]
[ro.build.user]: [android-build]
[ro.build.host]: [android-test-13.mtv.corp.google.com]
[ro.build.tags]: [test-keys]
[ro.product.model]: [sdk]
[ro.product.brand]: [generic]
[ro.product.name]: [sdk]
[ro.product.device]: [generic]
[ro.product.board]: []
[ro.product.cpu.abi]: [armeabi]
[ro.product.manufacturer]: [unknown]
[ro.product.locale.language]: [ldpi]
[ro.product.locale.region]: []
[ro.wifi.channels]: []
[ro.board.platform]: []
[ro.build.product]: [generic]
[ro.build.description]: [sdk-eng 2.1-update1 ECLAIR 35983 test-keys]
[ro.build.fingerprint]: [generic/sdk/generic/:2.1-update1/ECLAIR/35983:eng/test-
keys]
[rild.libpath]: [/system/lib/libreference-ril.so]
[rild.libargs]: [-d /dev/ttyS0]
[ro.config.notification_sound]: [OnTheHunt.ogg]
[ro.config.alarm_alert]: [Alarm_Classic.ogg]
[ro.setupwizard.mode]: [OPTIONAL]
[xmpp.auto-presence]: [true]
[ro.config.nocheckin]: [yes]
[net.bt.name]: [Android]
[net.change]: [net.dnschange]
[ro.config.sync]: [yes]
[dalvik.vm.stack-trace-file]: [/data/anr/traces.txt]
[persist.sys.timezone]: [America/Buenos_Aires]
[persist.sys.language]: [en]
[persist.sys.country]: [US]
[persist.sys.localevar]: []
[ro.FOREGROUND_APP_ADJ]: [0]
[ro.VISIBLE_APP_ADJ]: [1]
[ro.SECONDARY_SERVER_ADJ]: [2]
[ro.BACKUP_APP_ADJ]: [2]
[ro.HOME_APP_ADJ]: [4]
[ro.HIDDEN_APP_MIN_ADJ]: [7]
[ro.CONTENT_PROVIDER_ADJ]: [14]
```

```
[ro.EMPTY_APP_ADJ]: [15]
[ro.FOREGROUND_APP_MEM]: [1536]
[ro.VISIBLE_APP_MEM]: [2048]
[ro.SECONDARY_SERVER_MEM]: [4096]
[ro.BACKUP_APP_MEM]: [4096]
[ro.HOME_APP_MEM]: [4096]
[ro.HIDDEN_APP_MEM]: [5120]
[ro.CONTENT_PROVIDER_MEM]: [5632]
[ro.EMPTY_APP_MEM]: [6144]
[net.tcp.buffersize.default]: [4096,87380,110208,4096,16384,110208]
[net.tcp.buffersize.wifi]: [4095,87380,110208,4096,16384,110208]
[net.tcp.buffersize.umts]: [4094,87380,110208,4096,16384,110208]
[net.tcp.buffersize.edge]: [4093,26280,35040,4096,16384,35040]
[net.tcp.buffersize.gprs]: [4092,8760,11680,4096,8760,11680]
[init.svc.console]: [running]
[init.svc.servicemanager]: [running]
[init.svc.vold]: [running]
[init.svc.debuggerd]: [running]
[init.svc.ril-daemon]: [running]
[init.svc.zygote]: [running]
[init.svc.media]: [running]
[init.svc.installd]: [running]
[init.svc.keystore]: [running]
[init.svc.goldfish-setup]: [running]
[init.svc.qemud]: [running]
[init.svc.goldfish-logcat]: [stopped]
[ARGH]: [ARGH]
[net.eth0.dns1]: [10.0.2.3]
[net.gprs.local-ip]: [10.0.2.15]
[ro.radio.use-ppp]: [no]
[status.battery.state]: [Slow]
[status.battery.level]: [5]
[status.battery.level_raw]: [50]
[status.battery.level_scale]: [9]
[ro.com.google.locationfeatures]: [1]
[init.svc.adbd]: [running]
[dalvik.vm.heapsize]: [64m]
[ro.config.low_ram]: [true]
[qemu.sf.lcd_density]: [160]
[qemu.hw.mainkeys]: [0]
[qemu.sf.fake_camera]: [back]
[init.svc.bootanim]: [stopped]
[hw.keyboards.65536.devname]: [qwerty2]
```

```
[sys.settings_secure_version]: [5]
[sys.settings_system_version]: [8]
[dev.bootcomplete]: [1]
[gsm.version.ril-impl]: [android reference-ril 1.0]
[gsm.sim.operator.numeric]: [310260]
[gsm.sim.operator.alpha]: [Android]
[gsm.sim.operator.iso-country]: [us]
[gsm.sim.state]: [READY]
[gsm.current.phone-type]: [1]
[gsm.operator.alpha]: [Android]
[gsm.operator.numeric]: [310260]
[gsm.operator.iso-country]: [us]
[gsm.operator.isroaming]: [false]
[gsm.nitz.time]: [1413942868726]
[gsm.network.type]: [UMTS]
[net.gprs.http-proxy]: []
[gsm.defaultpdpcontext.active]: [true]
[net.dns1]: [10.0.2.3]
[net.dnschange]: [3]
[adb.connected]: [1]

————————Aplicaciones————————
package:/system/app/Fallback.apk=com.android.fallback
package:/system/app/SoundRecorder.apk=com.android.soundrecorder
package:/data/app/GestureBuilder.apk=com.android.gesture.builder
package:/system/app/AlarmClock.apk=com.android.alarmclock
package:/system/app/SdkSetup.apk=com.android.sdksetup
package:/system/app/Gallery.apk=com.android.gallery
package:/system/app/Launcher.apk=com.android.launcher
package:/system/framework/framework-res.apk=android
package:/system/app/EnhancedGoogleSearchProvider.apk=
com.google.android.providers.enhancedgooglesearch
package:/system/app/Settings.apk=com.android.settings
package:/system/app/ContactsProvider.apk= com.android.providers.contacts
package:/system/app/ApplicationsProvider.apk=
com.android.providers.applications
package:/system/app/Contacts.apk=com.android.contacts
package:/system/app/LatinIME.apk=com.android.inputmethod.latin
package:/system/app/Phone.apk=com.android.phone
package:/system/app/Calculator.apk=com.android.calculator2
package:/system/app/DrmProvider.apk=com.android.providers.drm
package:/system/app/HTMLViewer.apk=com.android.htmlviewer
package:/data/app/SoftKeyboard.apk=com.example.android.softkeyboard
```

package:/system/app/Term.apk=com.android.term
package:/system/app/LiveWallpapersPicker.apk=
com.android.wallpaper.livepicker
package:/system/app/Development.apk=com.android.development
package:/system/app/PackageInstaller.apk= com.android.packageinstaller
package:/system/app/TelephonyProvider.apk= com.android.providers.telephony
package:/system/app/Browser.apk=com.android.browser
package:/system/app/AccountAndSyncSettings.apk=
com.android.providers.subscribedfeeds
package:/system/app/CustomLocale.apk=com.android.customlocale
package:/system/app/Music.apk=com.android.music
package:/system/app/Camera.apk=com.android.camera
package:/system/app/PicoTts.apk=com.svox.pico
package:/system/app/NetSpeed.apk=com.android.netspeed
package:/system/app/OpenWnn.apk=jp.co.omronsoft.openwnn
package:/system/app/Email.apk=com.android.email
package:/data/app/CubeLiveWallpapers.apk= com.example.android.livecubes
package:/system/app/UserDictionaryProvider.apk=
com.android.providers.userdictionary
package:/system/app/SpareParts.apk=com.android.spare_parts
package:/system/app/PinyinIME.apk=com.android.inputmethod.pinyin
package:/system/app/SettingsProvider.apk= com.android.providers.settings
package:/system/app/TtsService.apk=android.tts
package:/system/app/Mms.apk=com.android.mms
package:/system/app/MediaProvider.apk=com.android.providers.media
package:/system/app/CertInstaller.apk=com.android.certinstaller
package:/system/app/DownloadProvider.apk= com.android.providers.downloads
package:/system/app/GlobalSearch.apk=com.android.globalsearch
package:/data/app/ApiDemos.apk=com.example.android.apis
package:/system/app/VpnServices.apk=com.android.server.vpn

Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

Nro de Caso	**Juzgado**		**Lugar y fecha**
1	Tesis de Maestría		Buenos Aires, 1 de Marzo 2014
Datos Obtenidos			
Tipo	Almacenamiento	Hash	Comentarios
Archivo imagen de datos	sdcard.dd	6f4aa14c32ae05d7178adafd5def26cc36e4d61b	985985024 bytes, Imagen de memoria externa
Archivo de texto plano	sdcard.sha1	8fac0059e469640e893f441bdfff1c5d996fade7	515 bytes, código de hash par la imagen de datos de la memoria externa tipo SD
Archivo de texto plano	dmesg.text	b2c199d15fd7274d7ea5e7cad74ba8cc81941adc	6789 bytes, captura de información de dmesg
Archivo de texto plano	dumpsys.text	1b7cf3236058b76e5ae800d813dc6c9ea3612e32	297141 bytes, captura de información de dumpsys
Archivo de texto plano	logcat.text	3403a33dabd0a6fa7a9d35681d9435e01d89e4dd	51114 bytes, captura de información de logcat
Archivo de base datos SQLITE3	contacts2.db	53dacd8a741241b13e606fdf3793929cef21bd59	93184 bytes, archivo con información del sistema de contactos de Android
Archivo de base datos SQLITE3	mmssms.db	45593a59941e8222c5dbfe74b6865e16f6d6c22b	32768 bytes, archivo con información del sistema de mensajería de Android
Archivo binario	heap-dump-tm1413942861-pid128.hprof	0ee82ca6c0835dc5c329ad119c93a4d6731e781d	2926820 bytes
Archivo binario	heap-dump-tm1413942861-pid161.hprof	0c2481fbce43eb1a81574424151efc73cc0f39db	3031146 bytes
Archivo binario	heap-dump-tm1413942861-pid91.hprof	eeb34842d05c96a612079d982834291608f84a41	2943520 bytes
Archivo binario	heap-dump-tm1413942861-pid93.hprof	f931c5c622f4eff3ccf7333d0cab70cb32414be3	3228755 bytes
Archivo binario	heap-dump-tm1413942861-pid98.hprof	324951ed582581351a84f74e53a64447e2659de8	3357176 bytes

Archivo binario	heap-dump-tm1413942862-pid177.hprof	e82e40543aae03861e32eb57fbf04698fcbd30dd	3001228 bytes
Archivo binario	heap-dump-tm1413942863-pid138.hprof	a8a9199743b6e0cc3869a50a9fa9be938593ae8f	2983595 bytes
Observaciones generales:			
Perito informático forense		**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:			
		Firma: Aclaración:	

E.3. Etapa 3

El alcance de este trabajo no requiere la documentación vinculada a la cadena de custodia que ha sido descripta en el marco de referencia. Sin embargo el inventario resulta de interés para el proceso por lo que se ha incluido en esta etapa.

Nro de Caso	Juzgado	Lugar y fecha
1	Tesis de Maestría	Buenos Aires, 1 de Marzo 2014
Inventario		
Numero	Tipo	Comentarios
1	Placa de Memoria	MicroSD No disponible / SD-C01G No disponible/ 1 Gigabyte 0948RB16638
2	Dispositivo Android	Emulado
3	DVD	Disco con información extraída
Observaciones generales: Ninguna		
Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

E.4. Etapa 4

Verificar el alcance del análisis:

Dada la naturaleza de este proceso, limitado a las necesidades de prueba sobre el marco de trabajo propuesto, no existe una definición de alcance externa como ocurriría en un proceso de peritaje con origen en la necesidad de un particular o un proceso judicial.

Registrar y notificar la inconsistencia:

No se registran faltantes y/o inconsistencias entre los datos disponibles y los registros.

Recuperar e Identificar información eliminada:

No puede realizarse el procedimiento sobre las copias correspondientes a las particiones de almacenamiento interno del dispositivo debido a la imposibilidad de extraer dichas imágenes del entorno virtual.

Se procede a realizar el análisis sobre la imagen de datos correspondiente a la memoria externa. La misma se encuentra formateada con sistema *fat*[1] por lo que se ajustaron los parámetros de uso de *The Sleuth Kit* para el caso. Se han obtenido los datos correspondientes a archivos eliminados y la actividad del sistema de archivos mediante las siguientes instrucciones:

```
1 ./Downloads/sleuthkit-4.1.3/tools/fstools/fls -V
2 The Sleuth Kit ver 4.1.3
3 ../Downloads/sleuthkit-4.1.3/tools/fstools/fls -f fat -m / sdcard.dd
     {\textgreater} sdcard.dd.fs-data
4 ../Downloads/sleuthkit-4.1.3/tools/timeline/mactime -d -b sdcard.dd.
    fs-data 2014-09-01..2014-12-31 {\textgreater} reporte-actividad-
    fs.csv
5 ../Downloads/sleuthkit-4.1.3/tools/fstools/icat -s -f fat sdcard.dd
    12 {\textgreater} pensamiento\_imagen.jpg
6 ../Downloads/sleuthkit-4.1.3/tools/fstools/icat -s -f fat sdcard.dd
    6 {\textgreater} legado.text
```

Identificar los eventos del sistema relevantes:

No se requiere información sobre los procesos de inicio del sistema, por lo que no se ha encontrado información relevante al caso de estudio en *dmseg.text*.

El caso de estudio es genérico y no demanda la identificación de procesos específicos, no obstante se procedió a identificar aquellos procesos que reportan algún tipo de inconveniente en *logcat.text* mediante la siguiente instrucción.

```
1 cat logcat.text | grep -C 5 ception
```

[1] F.A.T.:File Allocation Table, o Tabla de Ubicación de Archivos

Para el caso del archivo *sysdump.text* se procedió a identificar las secciones de información disponibles en el entorno en estudio y validar la posibilidad de acceso a estos datos sin extender este proceso de análisis a los detalles de cada una de estas; dicha operación se realizo con la siguiente instrucción:

```
cat dumpsys.text | grep -n DUMP
```

Analizar la información de la agenda Android:

Siguiendo el método sugerido en la definición del marco de trabajo se logro acceder a la información de la agenda sin inconvenientes. El resultado es el siguiente:

```
account_name|display_name|normalized_number|times_contacted
|Luminosa Perales Saldivar|10000000|0
|Elias Mota Ozuna|11111111|0
|Saul Aguirre Lujan|22222222|1
|Macra Veliz Pineda|33333333|2
|Ursy Marin Sierra|44444444|2
|Betty Guevara Arreola|55555555|1
|Ulpiano Suarez Anguiano|66666666|0
|Isaias Montes Colon|77777777|2
|Crispina Narvaez Melendez|88888888|2
|Publia Muro Villalpando|99999999|0
```

Analizar la información de las aplicaciones de agenda/contactos especificas:

Este punto se encuentra fuera del alcance del análisis, el caso de estudio no requiere extender la búsqueda a aplicaciones especificas ya que el objeto en estudio no dispone de este tipo de herramientas instaladas.

Analizar la información de telefónica de Android:

Siguiendo el método sugerido en la definición del marco de trabajo se logro acceder a la información de la agenda sin inconvenientes. El resultado es el siguiente:

```
1 sqlite> select _id,number,strftime("%Y-%m-%d %H:%M:%S", date/1000, '
     unixepoch','localtime'),duration,type,new,name,numbertype,
     numberlabel from CALLS;
2 _id|number|strftime("%Y-%m-%d %H:%M:%S", date/1000, 'unixepoch','
     localtime')|duration|type|new|name|numbertype|numberlabel
3 1|44444444|2014-10-19 00:17:33|3|1|1|Ursy Marin Sierra|1|
4 2|77777777|2014-10-19 00:17:41|0|3|1|Isaias Montes Colon|1|
5 3|44444444|2014-10-19 00:17:43|5|1|1|Ursy Marin Sierra|1|
6 4|88888888|2014-10-19 00:17:50|0|3|1|Crispina Narvaez Melendez|1|
7 5|33333333|2014-10-19 00:17:52|5|1|1|Macra Veliz Pineda|1|
8 6|77777777|2014-10-19 00:17:59|0|3|1|Isaias Montes Colon|1|
9 7|88888888|2014-10-19 00:18:01|5|1|1|Crispina Narvaez Melendez|1|
10 8|55555555|2014-10-19 00:18:08|0|3|1|Betty Guevara Arreola|1|
11 9|22222222|2014-10-19 00:18:10|4|1|1|Saul Aguirre Lujan|1|
12 10|33333333|2014-10-19 00:18:17|0|3|1|Macra Veliz Pineda|1|
```

Analizar la información de las aplicaciones VoIP especificas:

Este punto se encuentra fuera del alcance del análisis, el caso de estudio no requiere extender la búsqueda a aplicaciones especificas ya que el objecto en estudio no dispone de este tipo de herramientas instaladas.

Analizar la información de mensajería de Android:

Se utilizó el procedimiento sugerido para acceder a la información de mensajería obteniendo los siguientes resultados:

```
1 sqlite3 mmssms.db
2 sqlite> .header on
3 sqlite> select _id, thread_id, type, address, strftime("%Y-%m-%d %H
     :%M:%S", date/1000, 'unixepoch','localtime') as date, read,
     subject, body from sms;
4 _id|thread_id|type|address|date|read|subject|body
5 1|1|1|22222222|2014-10-19 00:16:16|1||En teoria no existe diferencia
      entre teoria y practica en la practica si la hay
```

```
6 2|2|1|77777777|2014-10-19 00:16:20|1||Ninguna ciencia en cuanto a
    ciencia engana el engano esta en quien no sabe
7 3|3|1|66666666|2014-10-19 00:16:28|0||El conocimiento es la region
    inexplorada del manana
8 4|4|1|33333333|2014-10-19 00:16:32|0||La tecnologia no nos ahorra
    tiempo pero su lo reparte de otra manera
9 5|5|1|44444444|2014-10-19 00:16:36|0||El conocimiento es la region
    inexplorada del manana
10 6|6|1|55555555|2014-10-19 00:16:40|1||La ciencia mas util es aquella
     cuyo fruto es el mas comunicable
11 7|7|1|00000001|2014-10-19 00:16:44|0||En que consiste la ciencia? En
     conocer a los hombres
12 8|6|2|55555555|2014-10-19 00:16:56|1||La verdadera ciencia ensena
    sobre todo a dudar y a ser ignorante
13 9|6|2|55555555|2014-10-19 00:16:56|1||La verdadera ciencia ensena
    sobre todo a dudar y a ser ignorante
14 10|2|2|77777777|2014-10-19 00:17:07|1||La felicidad no esta en la
    ciencia sino en la adquisicion de la ciencia
15 11|2|2|77777777|2014-10-19 00:17:07|1||La felicidad no esta en la
    ciencia sino en la adquisicion de la ciencia
16 12|8|2|99999999|2014-10-19 00:17:19|1||La ciencia es el alma de la
    prosperidad de las naciones y la fuente de todo progreso
17 13|8|2|99999999|2014-10-19 00:17:19|1||La ciencia es el alma de la
    prosperidad de las naciones y la fuente de todo progreso
18 14|1|2|22222222|2014-10-19 00:17:30|1||El fin de la ciencia
    especulativa es la verdad y el fin de la ciencia practica es la
    accion
19 15|1|2|22222222|2014-10-19 00:17:30|1||El fin de la ciencia
    especulativa es la verdad y el fin de la ciencia practica es la
    accion
```

Analizar la información de las aplicaciones de mensajería especificas:

Este punto se encuentra fuera del alcance del análisis, el caso de estudio no requiere extender la búsqueda a aplicaciones especificas ya que el objeto en estudio no dispone de este tipo de herramientas instaladas.

Identificar los elementos de imagen sonido o vídeo:

Se realizo con éxito la búsqueda de archivos de tipo imagen, audio y vídeo sobre la imagen de partición disponible, correspondiente a la memoria externa. Con tal fin se procedió a montar la imagen y hacer una búsqueda por contenidos a fin de no estar condicionados por la extensión o manipulaciones de las mismas.

Paso 1: Montaje de la imagen

```
1 sudo mount -t vfat -o loop,ro,noexec sdcard.dd ./mnt
2 cd mnt
```

Paso 2: Búsqueda y extracción de archivos con contenido de imagen

```
1 find -type f | xargs file | grep -E "image"
2 ./images/android_nombre.png:  PNG image data, 263 x 62, 8-bit
     colormap, non-interlaced
3 ./images/android_paquete.jpg: JPEG image data, JFIF standard 1.01
4 mkdir ../extractedFiles
5 cp ./images/android_nombre.png ../extractedFiles/
6 cp ./images/android_paquete.jpg ../extractedFiles/
```

Paso 3: Búsqueda y extracción de archivos con contenido de sonido

```
1 find -type f | xargs file | grep -E "sound|audio"
```

Paso 4: Búsqueda y extracción de archivos con contenido de vídeo

```
1 find -type f | xargs file | grep -E "video|movie"
```

Como resultado solo se encontraron dos archivos con información de tipo imagen, los cuales fueron extraídos de la imagen de partición.

Identificar los elementos del tipo especifico:

Este trabajo no requiere la búsqueda e identificación de archivos correspondientes a tipos de datos específicos.; en consecuencia quedan excluidos del alcance los puntos

de trabajo asociados como identificación de aplicaciones, repositorio y análisis de datos para estos casos.

Formalizar la documentación:

Nro de Caso	Juzgado	Lugar y fecha
1	Tesis de Maestría	Buenos Aires, 1 de Marzo 2014

Análisis pericial

./Downloads/sleuthkit-4.1.3/tools/fstools/fls -V
The Sleuth Kit ver 4.1.3

../Downloads/sleuthkit-4.1.3/tools/fstools/fls -f fat -m / sdcard.dd ¿sdcard.dd.fs-data
../Downloads/sleuthkit-4.1.3/tools/timeline/mactime -d -b sdcard.dd.fs-data 2014-09-01..2014-12-31 ¿reporte-actividad-fs.csv

../Downloads/sleuthkit-4.1.3/tools/fstools/icat -s -f fat sdcard.dd 12 ¿pensamiento_imagen.jpg
../Downloads/sleuthkit-4.1.3/tools/fstools/icat -s -f fat sdcard.dd 6 ¿legado.text

cat logcat.text | grep -C 5 ception

cat dumpsys.text | grep -n DUMP

sqlite3 contacts2.db
sqlite¿.header on
sqlite¿SELECT raw_contacts.account_name, raw_contacts.display_name, phone_lookup.normalized_number, raw_contacts.times_contacted FROM raw_contacts, phone_lookup WHERE raw_contacts._id = phone_lookup.raw_contact_id;
account_name|display_name|normalized_number|times_contacted
|Luminosa Perales Saldivar|10000000|0
|Elias Mota Ozuna|11111111|0
|Saul Aguirre Lujan|22222222|1
|Macra Veliz Pineda|33333333|2
|Ursy Marin Sierra|44444444|2
|Betty Guevara Arreola|55555555|1
|Ulpiano Suarez Anguiano|66666666|0
|Isaias Montes Colon|77777777|2
|Crispina Narvaez Melendez|88888888|2
|Publia Muro Villalpando|99999999|0

sqlite¿select _id,number,strftime(" %Y- %m- %d %H: %M: %S", date/1000, 'unixepoch','localtime'),duration,type,new,name,numbertype,numberlabel from CALLS;

_id|number|strftime(" %Y- %m- %d %H: %M: %S", date/1000, 'unixepoch','localtime')|duration|type|new|name|numbertype|numberlabel
1|44444444|2014-10-19 00:17:33|3|1|1|Ursy Marin Sierra|1|
2|77777777|2014-10-19 00:17:41|0|3|1|Isaias Montes Colon|1|
3|44444444|2014-10-19 00:17:43|5|1|1|Ursy Marin Sierra|1|
4|88888888|2014-10-19 00:17:50|0|3|1|Crispina Narvaez Melendez|1|
5|33333333|2014-10-19 00:17:52|5|1|1|Macra Veliz Pineda|1|
6|77777777|2014-10-19 00:17:59|0|3|1|Isaias Montes Colon|1|
7|88888888|2014-10-19 00:18:01|5|1|1|Crispina Narvaez Melendez|1|
8|55555555|2014-10-19 00:18:08|0|3|1|Betty Guevara Arreola|1|
9|22222222|2014-10-19 00:18:10|4|1|1|Saul Aguirre Lujan|1|
10|33333333|2014-10-19 00:18:17|0|3|1|Macra Veliz Pineda|1|

sqlite3 mmssms.db
sqlite¿.header on
sqlite¿select _id, thread_id, type, address, strftime(" %Y- %m- %d %H: %M: %S", date/1000, 'unixepoch','localtime') as date, read, subject, body from sms;
_id|thread_id|type|address|date|read|subject|body
1|1|1|22222222|2014-10-19 00:16:16|1||En teoria no existe diferencia entre teoria y practica en la practica si la hay
2|2|1|77777777|2014-10-19 00:16:20|1||Ninguna ciencia en cuanto a ciencia engana el engano esta en quien no sabe
3|3|1|66666666|2014-10-19 00:16:28|0||El conocimiento es la region inexplorada del manana
4|4|1|33333333|2014-10-19 00:16:32|0||La tecnologia no nos ahorra tiempo pero su lo reparte de otra manera
5|5|1|44444444|2014-10-19 00:16:36|0||El conocimiento es la region inexplorada del manana
6|6|1|55555555|2014-10-19 00:16:40|1||La ciencia mas util es aquella cuyo fruto es el mas comunicable
7|7|1|00000001|2014-10-19 00:16:44|0||En que consiste la ciencia? En conocer a los hombres
8|6|2|55555555|2014-10-19 00:16:56|1||La verdadera ciencia ensena sobre todo a dudar y a ser ignorante
9|6|2|55555555|2014-10-19 00:16:56|1||La verdadera ciencia ensena sobre todo a dudar y a ser ignorante

10|2|2|77777777|2014-10-19 00:17:07|1||La felicidad no esta en la ciencia sino en la adquisicion de la ciencia
11|2|2|77777777|2014-10-19 00:17:07|1||La felicidad no esta en la ciencia sino en la adquisicion de la ciencia
12|8|2|99999999|2014-10-19 00:17:19|1||La ciencia es el alma de la prosperidad de las naciones y la fuente de todo progreso
13|8|2|99999999|2014-10-19 00:17:19|1||La ciencia es el alma de la prosperidad de las naciones y la fuente de todo progreso
14|1|2|22222222|2014-10-19 00:17:30|1||El fin de la ciencia especulativa es la verdad y el fin de la ciencia practica es la accion
15|1|2|22222222|2014-10-19 00:17:30|1||El fin de la ciencia especulativa es la verdad y el fin de la ciencia practica es la accion

sudo mount -t vfat -o loop,ro,noexec sdcard.dd ./mnt
cd mnt
find -type f | xargs file | grep -E ïmage"
./images/android_nombre.png: PNG image data, 263 x 62, 8-bit colormap, non-interlaced
./images/android_paquete.jpg: JPEG image data, JFIF standard 1.01
find -type f | xargs file | grep -E "sound|audio"
find -type f | xargs file | grep -E "video|movie"

mkdir ../extractedFiles
cp ./images/android_nombre.png ../extractedFiles/
cp ./images/android_paquete.jpg ../extractedFiles

Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

Nro de Caso	**Juzgado**		**Lugar y fecha**
1	Tesis de Maestría		Buenos Aires, 1 de Marzo 2014
Linea de tiempo			
Fecha-Hora	Tipo	Aplicación	Detalle
Fecha-Hora	Tipo	Aplicación	Detalle
2014/10/19 00:00:00	Actividad de archivos	Sistema de archivos	Archivo accedido, /.Trash-1000
2014/10/19 00:00:00	Actividad de archivos	Sistema de archivos	Archivo accedido, /images
2014/10/19 00:00:00	Actividad de archivos	Sistema de archivos	Archivo accedido, /legado.text (deleted)
2014/10/19 00:00:00	Actividad de archivos	Sistema de archivos	Archivo accedido, /pensamiento.text
2014/10/19 00:00:00	Actividad de archivos	Sistema de archivos	Archivo accedido, /pensamiento_imagen.jpg (deleted)
2014/10/19 00:16:16	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 22222222.
2014/10/19 00:16:20	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 77777777.
2014/10/19 00:16:28	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 66666666.
2014/10/19 00:16:32	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 33333333.
2014/10/19 00:16:36	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 44444444.
2014/10/19 00:16:40	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 55555555.
2014/10/19 00:16:44	Mensaje de texto	Mensajero Android	Mensaje entrante del numero 00000001.
2014/10/19 00:16:56	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 55555555.

2014/10/19 00:16:56	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 55555555.
2014/10/19 00:17:07	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 77777777.
2014/10/19 00:17:07	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 77777777.
2014/10/19 00:17:19	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 99999999.
2014/10/19 00:17:19	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 99999999.
2014/10/19 00:17:30	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 22222222.
2014/10/19 00:17:30	Mensaje de texto	Mensajero Android	Mensaje saliente al numero 22222222.
2014/10/19 00:17:33	Llamada telefónica	Teléfono Android	Llamada entrante del numero 44444444 recibida de 3 segundos de duración.
2014/10/19 00:17:41	Llamada telefónica	Teléfono Android	Llamada entrante del numero 77777777 rechazada o invalida, 0 segundos de duración.
2014/10/19 00:17:43	Llamada telefónica	Teléfono Android	Llamada entrante del numero 44444444 recibida de 5 segundos de duración.

2014/10/19 00:17:50	Llamada telefónica	Teléfono Android	Llamada entrante del numero 88888888 rechazada o invalida, 0 segundos de duración.
2014/10/19 00:17:52	Llamada telefónica	Teléfono Android	Llamada entrante del numero 33333333 recibida de 5 segundos de duración.
2014/10/19 00:17:59	Llamada telefónica	Teléfono Android	Llamada entrante del numero 77777777 rechazada o invalida, 0 segundos de duración.
2014/10/19 00:18:01	Llamada telefónica	Teléfono Android	Llamada entrante del numero 88888888 recibida de 5 segundos de duración.
2014/10/19 00:18:08	Llamada telefónica	Teléfono Android	Llamada entrante del numero 55555555 rechazada o invalida, 0 segundos de duración.
2014/10/19 00:18:10	Llamada telefónica	Teléfono Android	Llamada entrante del numero 22222222 recibida de 4 segundos de duración.

2014/10/19 00:18:17	Llamada telefónica	Teléfono Android	Llamada entrante del numero 33333333 rechazada o invalida, 0 segundos de duración.
2014/10/19 00:43:36	Actividad de archivos	Sistema de archivos	Archivo creado, /legado.text (deleted)
2014/10/19 00:43:38	Actividad de archivos	Sistema de archivos	Archivo creado, /pensamiento.text
2014/10/19 00:43:38	Actividad de archivos	Sistema de archivos	Archivo creado, /pensamiento_imagen.jpg (deleted)
2014/10/19 00:45:14	Actividad de archivos	Sistema de archivos	Archivo modificado, Archivo creado, /.Trash-1000
2014/10/19 00:45:14	Actividad de archivos	Sistema de archivos	Archivo modificado, Archivo creado, /images

Observaciones generales:
Se adjuntan los archivos correspondientes al análisis de sistemas de archivos y recuperación de archivos eliminados.

Información del sistema de archivos
773aa413b0040b5e2eb3d0c0fad9647e3d5b8afe reporte-actividad-fs.csv
c16a36a4dde206521053726cc5badfc515b68ac5 sdcard.dd.fs-data

Archivos de tipo especifico
016e60e49b8c22b5dd98b4df42ff9b45d5785fe5 android_nombre.png
d197d660b45f19e0887becf8dae061545e368771 android_paquete.jpg

Archivos eliminados
af71221b724100af98280e0033f5e83948e77d11 pensamiento_imagen.jpg
025ac2b6e2f3c30ffdc379996c7df5bcc025f507 legado.text

Perito informático forense	**Lugar**	**Fecha**
Apellido: Nombre: Legajo: DNI:		
	Firma: Aclaración:	

E.5. Etapa 5

A fin de completar el procedimiento se ha redactado el siguiente informe sobre la base de la información relevada y analizada para el caso en cuestión:

Nro de Caso	Juzgado	Lugar y fecha
1	Tesis de Maestría	Buenos Aires, 1 de Marzo 2014

Reporte del perito

La pericia, de índole genérico y sin solicitud de datos particulares, evidencia el registro de los siguientes contactos telefónicos en la agenda del dispositivo:

Nombre en la agenda, Numero telefónico, Cantidad de comunicaciones
Luminosa Perales Saldivar,10000000,0
Elias Mota Ozuna, 11111111, 0
Saul Aguirre Lujan, 22222222, 1
Macra Veliz Pineda, 33333333, 2
Ursy Marin Sierra, 44444444, 2
Betty Guevara Arreola, 55555555, 1
Ulpiano Suarez Anguiano, 66666666, 0
Isaias Montes Colon, 77777777, 2
Crispina Narvaez Melendez, 88888888, 2
Publia Muro Villalpando, 99999999, 0

Así mismo se registra actividad telefónica y de mensajería asociada a un subconjunto de números registrados en la agenda de contactos del dispositivo; se referencia a la documentación adjunta para los detalles y orden cronológico de los mismos.

Se ha identificado la existencia de archivos de imágenes en el espacio de almacenamiento del dispositivo, como también actividad vinculada a la eliminación de archivos. Los archivos de tipo especifico y aquellos eliminados que se han recuperado se encuentran en la documentación adjunta. Ellos son:

<table>
<tr><td colspan="3">Archivos de tipo especifico, con código SHA-1:
016e60e49b8c22b5dd98b4df42ff9b45d5785fe5 android_nombre.png
d197d660b45f19e0887becf8dae061545e368771 android_paquete.jpg

Archivos eliminados, con código SHA-1:
af71221b724100af98280e0033f5e83948e77d11 pensamiento_imagen.jpg
025ac2b6e2f3c30ffdc379996c7df5bcc025f507 legado.text

Se adjunta a este reporte la documentación correspondiente al relevamiento de Hardware y Software, Extracción de datos, Inventario y Ficha de Análisis realizado en este peritaje.</td></tr>
<tr><th>Perito informático forense</th><th>Lugar</th><th>Fecha</th></tr>
<tr><td>Apellido:
Nombre:
Legajo:
DNI:</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Firma:
Aclaración:</td></tr>
</table>