



**UNIVERSIDAD SIMÓN BOLÍVAR**  
**DECANATO DE ESTUDIOS PROFESIONALES**  
**COORDINACIÓN DE INGENIERÍA DE TELECOMUNICACIONES**

**METODOLOGÍA PARA LA INVESTIGACIÓN FORENSE EN  
DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO *ANDROID***

**Por:**

**Miriam Xurimar Cedeño Carrasquel**

**Simone José Bermúdez Pérez**

**PROYECTO DE GRADO**

Presentado ante la ilustre Universidad Simón Bolívar  
como requisito parcial para optar al título de  
Ingeniero de Telecomunicaciones

**Sartenejas, mayo de 2021**



**UNIVERSIDAD SIMÓN BOLÍVAR**  
**DECANATO DE ESTUDIOS PROFESIONALES**  
**COORDINACIÓN DE INGENIERÍA DE TELECOMUNICACIONES**

**METODOLOGÍA PARA LA INVESTIGACIÓN FORENSE EN  
DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO *ANDROID***

**Por:**

**Miriam Xurimar Cedeño Carrasquel**

**Simone José Bermúdez Pérez**

**Realizado con la asesoría de:**

**Vincenzo Mendillo**

**Orlando Sucre**

**PROYECTO DE GRADO**

Presentado ante la ilustre Universidad Simón Bolívar  
como requisito parcial para optar al título de  
Ingeniero de Telecomunicaciones

**Sartenejas, mayo de 2021**

*Página dejada en blanco intencionalmente para colocar el acta de evaluación*

*Página dejada en blanco intencionalmente para colocar el acta de evaluación*



**UNIVERSIDAD SIMÓN BOLÍVAR**  
**DECANATO DE ESTUDIOS PROFESIONALES**  
**COORDINACIÓN DE INGENIERÍA DE TELECOMUNICACIONES**

**METODOLOGÍA PARA LA INVESTIGACIÓN FORENSE EN  
DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO *ANDROID***

PROYECTO DE GRADO

PRESENTADO POR:

**Miriam Xurimar Cedeño Carrasquel, Carnet 12-10040**

**Simone José Bermúdez Pérez, Carnet 12-11016**

**RESUMEN**

La Informática Forense es una rama de la Tecnología de la Información y Comunicación (TIC) que combina elementos legales e informáticos, con el fin de asegurar, preservar, identificar, analizar y presentar un conjunto de datos extraídos de sistemas informáticos, redes, equipos de comunicaciones y dispositivos de almacenamiento. El objetivo principal de este trabajo es proponer una metodología que permita investigar de manera apropiada los datos contenidos en dispositivos móviles equipados con sistema operativo *Android*. La investigación se aborda enunciando los términos y conceptos de la informática forense, seguido de las bases legales nacionales e internacionales, normativas y estándares. Además, se estudia un caso, describiendo paso a paso la aplicación del método, esto es la extracción de los datos contenidos en un dispositivo móvil, el análisis de los mismos y el informe pericial. Finalmente se presentan las conclusiones de este trabajo de grado, así como las recomendaciones para trabajos ulteriores.

**Palabras clave:** Informática forense, Análisis forense, Forénsica digital, *Android*.

## **DEDICATORIA**

*A nuestros padres,  
ustedes lo hicieron posible.*

## **AGRADECIMIENTOS**

*Gracias a Dios por darnos la salud, sabiduría y fortaleza para superar todos los obstáculos que encontramos en la carrera.*

*A nuestros padres por habernos dado la vida, el amor y el apoyo incondicional necesario para alcanzar nuestras metas.*

*A nuestro tutor Vincenzo Mendillo por guiarnos a lo largo de este trabajo y compartir con nosotras su pasión por las telecomunicaciones. Gracias por todo el apoyo y enseñarnos tanto sobre el campo de la seguridad y la informática forense.*

*A los profesores de nuestra insigne casa de estudios, por toda la ayuda y los consejos que nos permitieron avanzar en nuestros estudios.*

# ÍNDICE GENERAL

<b>RESUMEN.....</b>	<b>iv</b>
<b>DEDICATORIA.....</b>	<b>v</b>
<b>AGRADECIMIENTOS .....</b>	<b>vi</b>
<b>ÍNDICE GENERAL.....</b>	<b>vii</b>
<b>ÍNDICE DE FIGURAS.....</b>	<b>xii</b>
<b>ÍNDICE DE TABLAS.....</b>	<b>xvi</b>
<b>LISTA DE ABREVIATURAS .....</b>	<b>xvii</b>
<b>1 INTRODUCCIÓN.....</b>	<b>1</b>
1.1 Antecedentes del estudio .....	1
1.2 Justificación y planteamiento del problema .....	3
1.3 Objetivos de la investigación. ....	3
1.3.1 Objetivo general del estudio.....	3
1.3.2 Objetivos específicos del estudio .....	4
1.4 Estructura del trabajo .....	5
<b>2 MARCO TEÓRICO .....</b>	<b>7</b>
2.1 Ciencias forenses.....	7
2.2 Informática forense .....	7
2.3 Análisis forense digital.....	7
2.4 Objetivos del análisis forense.....	8

2.4.1 Precedentes del análisis forense .....	9
2.4.2 Evidencia digital.....	10
2.5 Análisis forense en el entorno móvil.....	11
2.6 Herramientas para el análisis forense.....	12
2.6.1 Herramientas para el análisis de redes .....	12
2.6.2 Herramientas para el análisis de bases de datos.....	12
2.6.3 Herramientas para el análisis de dispositivos móviles.....	13
2.7 Dispositivos móviles .....	15
2.8 Sistema operativo .....	16
2.8.1 Sistema operativo <i>Android</i> .....	16
2.8.2 Arquitectura del sistema operativo <i>Android</i> .....	17
2.8.3 Librerías de <i>Android</i> .....	18
2.8.4 Sistema de archivos y particiones de <i>Android</i> .....	19
2.8.5 Almacenamiento de datos en <i>Android</i> .....	20
2.8.6 Componentes de aplicaciones <i>Android</i> .....	20
2.8.7 Seguridad en aplicaciones <i>Android</i> .....	21
2.9 Programas maliciosos: Malware .....	23
2.9.1 Clasificación de <i>Malware</i> .....	23
<b>3 MARCO LEGAL .....</b>	<b>26</b>
3.1 Constitución de la República Bolivariana de Venezuela .....	27
3.2 Ley contra delitos informáticos del 2001 – Gaceta oficial No. 37.313.....	27
3.3 Ley de Infogobierno del 2013 – Gaceta oficial No. 40.274.....	30
<b>4 ESTÁNDARES Y NORMAS .....</b>	<b>36</b>
4.1 Estándares a nivel internacional .....	36

4.1.1 Estándar ISO/IEC 27037:2012.....	36
4.1.2 Estándar ISO/IEC 27042:2015.....	37
4.2 Referencias internacionales.....	39
4.2.1 El Documento RFC 3227.....	39
4.2.2 El documento RFC 4810.....	42
4.2.3 El documento RFC 4998.....	42
4.2.4 El documento RFC 6283.....	42
4.3 Convenio de Budapest.....	42
<b>5 METODOLOGÍA .....</b>	<b>44</b>
5.1 Fases fundamentales de una investigación forense .....	46
5.1.1 Fase de identificación de la escena .....	46
5.1.2 Fase de preservación de la evidencia .....	46
5.1.3 Fase de análisis de la evidencia.....	47
5.1.4 Fase de documentación del incidente.....	47
5.2 Desarrollo de la metodología .....	47
5.2.1 Fase de preparación.....	48
5.2.2 Fase de identificación.....	49
5.2.3 Fase de adquisición .....	51
5.2.4 Fase de análisis.....	56
5.2.5 Fase de presentación .....	57
5.3 Recomendaciones para la implementación de la metodología.....	58
<b>6 INVESTIGACIÓN FORENSE EN DISPOSITIVOS MÓVILES .....</b>	<b>59</b>
6.1 Adquisición de datos .....	59
6.1.1 Adquisición manual de datos .....	59

6.1.2 Adquisición lógica de datos mediante MTP y conexión USB.....	61
6.1.3 Extracción lógica de datos mediante conexión USB y ADB.....	63
6.1.4 Adquisición lógica mediante <i>MOBILedit Forensic Express PRO</i> ..	70
6.1.5 <i>Rooting</i> de un equipo <i>Android</i> .....	79
6.1.6 Adquisición física de datos mediante <i>dd</i> .....	83
6.2 Análisis de datos.....	87
6.3 Detección de spyware.....	93
6.3.1 <i>Free Android Spy</i> .....	94
6.3.2 Proceso de descarga y uso.....	94
6.3.3 Detección y eliminación de un <i>spyware</i> .....	100
6.3.4 Desinstalación mediante <i>Google Protect</i> .....	101
6.3.5 Desinstalación mediante aplicación <i>anti-spy</i> .....	103
<b>7 IMPLEMENTACIÓN Y DESARROLLO DE METODOLOGÍA .....</b>	<b>107</b>
7.1 Descripción del caso práctico de prueba .....	107
7.1.1 Características del dispositivo.....	107
7.1.2 Descripción de herramientas .....	107
7.2 Implementación de la metodología .....	108
7.2.1 Preparación e Identificación:.....	108
7.2.2 Adquisición de la evidencia .....	109
7.2.3 Análisis de los resultados .....	117
7.2.4 Presentación .....	124
<b>8 CONCLUSIONES Y RECOMENDACIONES.....</b>	<b>127</b>
<b>Conclusiones .....</b>	<b>127</b>
<b>Recomendaciones .....</b>	<b>130</b>

<b>BIBLIOGRAFÍA.....</b>	<b>132</b>
<b>ANEXO 1 .....</b>	<b>135</b>



## ÍNDICE DE FIGURAS

Figura 2.01: Arquitectura interna del sistema <i>Android</i> .....	18
Figura 5.01: Etapas de la metodología propuesta .....	48
Figura 5.02: Etapa de preparación .....	48
Figura 5.03: Etapa de identificación .....	49
Figura 5.04:Etapa de adquisición.....	51
Figura 5.05:Etapa de análisis .....	56
Figura 5.06: Etapa de presentación .....	57
Figura 6.02:Sistema de administración de archivos del Motorola G3 .....	60
Figura 6.03: Detección automática de un dispositivo en sistema <i>Window</i> . .....	61
Figura 6.04:Ejemplo de <i>Media Transfer Protocol</i> (MTP).....	62
Figura 6.05:Ejemplo de acceso al sistema de carpetas internas de un dispositivo móvil desde el sistema <i>Windows</i> .....	63
Figura 6.06: Activación de la depuración por USB en un dispositivo <i>Android</i> .....	64
Figura 6.07:Resultado de la correcta instalación de los driver de un dispositivo .....	64
Figura 6.08:Resultado de la instalación fallida de un <i>driver</i> en <i>Windows</i> .....	65
Figura 6.09:Pantalla para la habilitación de permisos de depuración USB .....	65
Figura 6.10: Proceso de comunicación del aplicativo <i>ADB Daemon</i> con el dispositivo en prueba .....	66
Figura 6.11:Activación de la pantalla CMD para inicio del intercambio de datos .....	66
Figura 6.12: Resultado exitoso de la aplicación del comando <i>devices</i> .....	67
Figura 6.13:Activación de la pantalla para utiliza el comando <i>shell</i> .....	67
Figura 6.14:Ejemplo del contenido de archivos de un sistema típico.....	68
Figura 6.15:Ejemplo de la aplicación del comando <i>adb</i> .....	68
Figura 6.16:Uso del comando <i>df</i> .....	69
Figura 6.17:Resultado de la aplicación del comando <i>pull</i> .....	69
Figura 6.18:Ejemplo de la distribución de datos de un dispositivo .....	69
Figura 6.19:Ejemplo del listado de paquetes instalados por terceros .....	70

Figura 6.20:Proceso de instalación de la herramienta <i>MOBILedit</i> .....	71
Figura 6.21:Pantalla principal de la herramienta .....	72
Figura 6.22:Selección del dispositivo a diagnosticar .....	72
Figura 6.23:Solicitud de pre-visualización de datos .....	73
Figura 6.24:Obtención de la información contenida en el dispositivo.....	73
Figura 6.25:Ejemplo de como se muestra el directorio telefónico.....	74
Figura 6.26:Ejemplo de la obtención de los datos de mensajes .....	74
Figura 6.27:Ejemplo de la obtención del registro de llamadas .....	75
Figura 6.28:Obtención de la información de otros eventos .....	75
Figura 6.29:Pantalla donde se indica que el dispositivo móvil no es <i>root</i> .....	76
Figura 6.30:Ejemplo de cómo seleccionar la data a extraer.....	77
Figura 6.31:Pantalla donde se especifican los detalles del informe solicitado .....	77
Figura 6.32:Pantalla donde se seleccionan los detalles del formato del reporte .....	78
Figura 6.33:Pantalla indicativa del nombre y dirección del reporte .....	78
Figura 6.34:Pantalla indicativa de que comienza el respaldo de la información .....	79
Figura 6.35:Pantalla principal de <i>KingRoot</i> .....	80
Figura 6.36:La herramienta <i>KingRoot</i> realizando la evaluación del equipo .....	81
Figura 6.37:Pantalla indicativa de que se están concediendo los permisos de superusuario .....	81
Figura 6.38:Pantalla indicativa del estado del dispositivo .....	82
Figura 6.39:Pantalla indicativa que el <i>root</i> fue aplicado correctamente.....	83
Figura 6.40:Particiones típicas de un dispositivo móvil .....	84
Figura 6.41:Pantalla que muestra la utilización del espacio de memoria dentro del dispositivo .....	84
Figura 6.42:Pantalla que muestra el resultado de copia de una partición .....	85
Figura 6.43:Ubicación del bloque de datos a transferir <i>mmcblk0p39</i> .....	86
Figura 6.44:Pantalla que muestra el volcado con el comando <i>Netcat</i> .....	86
Figura 6.45:Resultados del proceso de transferencia.....	86
Figura 6.46:Pantalla principal de la herramienta <i>Autopsy</i> .....	87
Figura 6.47:Pantalla para la introducción de los datos del caso .....	88

Figura 6.48:Pantalla para la selección de la fuente de datos.....	88
Figura 6.49:Selección de los módulos a procesar .....	89
Figura 6.50:Muestra del avance del proceso de análisis .....	89
Figura 6.51:Pantalla que muestra los resultados del proceso de análisis de la imagen .....	90
Figura 6.52:Muestra del árbol de directorios de una partición con datos para el análisis .....	91
Figura 6.53:Ejemplo de árbol de directorios obtenido con <i>Autopsy</i> .....	91
Figura 6.54:Pantalla que muestra la visualización con la opción <i>Views</i> .....	92
Figura 6.55:Pantalla que muestra los resultados de la aplicación complementos del <i>software</i> .....	92
Figura 6.56:Pantalla con los resultados de la opción <i>Listing</i> .....	93
Figura 6.57:Desconexión del <i>Scan</i> de seguridad de <i>Google Play Protect</i> .....	94
Figura 6.58:Habilitación de los permisos para instalar aplicaciones desconocidas....	95
Figura 6.59:Proceso de instalación de <i>Free Android Spy</i> .....	96
Figura 6.60:Instalación de la herramienta <i>Anti Spy</i> .....	96
Figura 6.61:Pantalla que indica que la instalación se completó adecuadamente .....	97
Figura 6.62:Recibiendo el <i>mail</i> con el <i>password</i> para operar la herramienta.....	97
Figura 6.63:Accediendo al área privada de la herramienta.....	98
Figura 6.64:Pantalla que muestra la información del equipo en prueba .....	98
Figura 6.65:Información de llamadas entrantes y salientes .....	99
Figura 6.66:Detalle de la información de los mensajes de texto.....	99
Figura 6.67:Detalle de la agenda de contactos del dispositivo .....	99
Figura 6.68:Muestra de las fotos contenidas en el dispositivo en prueba.....	100
Figura 6.69:Reporte de las aplicaciones instaladas en el dispositivo.....	100
Figura 6.70:Pantalla principal de <i>GlassWire</i> .....	101
Figura 6.71:Ubicación de <i>Play Protect</i> en <i>Google Play</i> .....	102
Figura 6.72 :Pantalla de alarma en caso de detectar <i>spyware</i> .....	103
Figura 6.73:Escáner <i>Anti-Spy</i> en <i>Google Play</i> .....	103
Figura 6.74: Proceso de análisis con Escáner <i>Anti-Spy</i> y <i>spyware</i> .....	104

Figura 6.75: Proceso de detección y anulación de un programa malicioso .....	105
Figura 6.76: Pantalla de notificación de ruptura del envío de datos .....	106
Figura 7.01: Pantalla principal de la herramienta <i>MOBILedit</i> .....	110
Figura 7.02: Pantalla de reconocimiento de dispositivo de <i>Forensic Connector</i> .....	110
Figura 7.03: Pantalla donde <i>MOBILedit</i> reconoce el dispositivo conectado .....	111
Figura 7.04: Reconocimiento de que el dispositivo está rooteado .....	111
Figura 7.05: Selección de análisis de aplicaciones .....	112
Figura 7.06: Selección de las aplicaciones que se extraerán del dispositivo .....	112
Figura 7.07: Selección del formato de salida del informe final .....	113
Figura 7.08: Selección del formato de visualización del informe final .....	113
Figura 7.09: Pantalla que muestra el inicio de la extracción de los datos .....	114
Figura 7.10: Pantalla que indica que el proceso de extracción se completó con éxito .....	114
Figura 7.11: Resumen de los datos del equipo y el sistema de extracción .....	115
Figura 7.12: Informe de resultados .....	116
Figura 7.13: Indicador de información básica del dispositivo .....	117
Figura 7.14: Ejemplo de los datos del directorio telefónico .....	118
Figura 7.15: Muestra del informe de registro de llamadas .....	118
Figura 7.16: Resumen del resumen de mensajería .....	119
Figura 7.17: Detalle del resumen de mensajería del dispositivo .....	119
Figura 7.18: Reporte de los juegos encontrados en el dispositivo .....	120
Figura 7.19: Muestra de la visualización de los datos de las aplicaciones .....	120
Figura 7.20: Ejemplo de visualización de los datos de archivos multimedia .....	121
Figura 7.21: Reporte de otros archivos encontrados en el dispositivo .....	122

## ÍNDICE DE TABLAS

Tabla 4.1: Volatilidad de la información.....	40
Tabla 7.2: Condiciones de entrega del dispositivo en estudio.....	109
Tabla 7.3: Resumen de la cadena de custodia.....	123
Tabla A1.1: Datos del tribunal de la causa.....	135
Tabla A1.2: Identificación del dispositivo.....	136
Tabla A1.3: Características técnicas del dispositivo en prueba.....	138

## LISTA DE ABREVIATURAS

<b>ADB</b>	<i>ADB Daemon.</i>
<b>ADB</b>	Puente para la depuración en sistema <i>Android</i> (del inglés <i>Android Debug Bridge</i> ).
<b>MTP</b>	Protocolo de transferencia de archivos multimedia (del inglés <i>Media Transfer Protocol</i> ).
<b>JTAG</b>	Método de extracción física, que consiste en acceder a un determinado <i>chip</i> mediante conexiones eléctricas con los pines del circuito (del inglés <i>Joint Test Action Group</i> ).
<b>SDK</b>	Juego para el desarrollo de aplicaciones (del inglés <i>Software Development Kit</i> ).
<b>TSK</b>	Interfaz gráfica utilizada por la herramienta <i>Autopsy</i> (del inglés <i>The Sleuth Kit</i> ).

# CAPÍTULO I

## INTRODUCCIÓN

Desde el comienzo de Internet y las nuevas tecnologías para la información, los delincuentes han encontrado en éstas una gran oportunidad para cometer una extensa cantidad de actividades delictivas. Algunos ejemplos son: sustracción de datos, obtención de beneficios económicos, extorsión, secuestro, pornografía infantil y robo de propiedad intelectual.

Es justo pensar que los avances tecnológicos han construido la base de la sociedad moderna, sin embargo, también han contribuido en el crecimiento de los delitos informáticos y de las formas en que estos pueden llevarse a cabo.

Cifras recientes como las mostradas en el boletín de seguridad 2019 por *Kaspersky* (una de las empresas más reconocidas en materia de *malware* y cibercrimen) registran que durante ese año el 19,8% de los equipos conectados a Internet recibieron al menos un ataque del tipo *malware*. Con las soluciones de *Kaspersky* se logró neutralizar cerca de un millón de ataques en varios países del mundo, incluyendo programas maliciosos para robar dinero de cuentas bancarias.

El incremento de la ciberdelincuencia y la gigantesca cantidad de incidentes de seguridad obligan a enfocarse en mecanismos más apropiados para investigar este tipo de sucesos, y de esta manera nacen las ciencias forenses digitales.

Este trabajo de grado se centra en las consideraciones metodológicas para proceder frente a un incidente de seguridad en dispositivos móviles, tomando en cuenta *software*, *hardware*, así como normativas y leyes de acuerdo al tipo de incidente.

### **1.1 Antecedentes del estudio**

Desde su aparición, los teléfonos celulares han ganado gran popularidad y se han convertido en una de las herramientas básicas de comunicación en la sociedad moderna. Su uso aumenta con el pasar de los días y esto se debe a la gran cantidad de

beneficios que brindan, más allá de la alta gama de modelos, portabilidad y variedad de precios.

Con el nacimiento de la nueva generación de *smartphones*, se deja de lado el paradigma de usar el teléfono únicamente con la intención de realizar y recibir llamadas, sino que ahora se integran una nueva variedad de servicios, entre los cuales resalta:

- Almacenar y compartir información y datos de cualquier tipo (texto, voz, imágenes, videos, documentos).
- GPS.
- Conexión a Internet.
- Uso de distintas aplicaciones.

Por estos y otros beneficios ha sido fácil lograr que las personas migren de la tecnología analógica a la digital, sin embargo, esto no sólo abarca al usuario promedio, sino también a los delincuentes.

Sería un error clasificar a esta tecnología como “buena” o “mala”, ya que puede ser utilizada de distintas maneras, inclusive para cometer delitos o realizar algún tipo de ataque informático.

Su crecimiento acelerado y masificado ha causado que los actos delictivos informáticos fueran aumentando a la misma velocidad y varios de ellos con los siguientes fines:

- Robo de información.
- Fraude.
- Extorsión.
- Hostigamiento y acoso.
- *Bullying*.
- Secuestro.
- Terrorismo cibernético.
- Pornografía infantil.



- Narcotráfico.
- Robos de secretos comerciales.
- Robo o destrucción de propiedad intelectual.

## 1.2 Justificación y planteamiento del problema

La gran velocidad con la que ha evolucionado la tecnología hace que los delincuentes encuentren en ella una poderosa herramienta para cometer una amplia variedad de actividades ilícitas. Cada vez son más los distintos tipos de delitos que se apoyan en el sector de las Tecnologías de la Información y la Comunicación (TIC).

La proliferación de incidentes de seguridad y hechos delictivos del tipo informático, ha hecho que la informática forense sea ahora un campo fundamental para manejar los casos que se presentan.

Este trabajo investigativo se centra en dispositivos móviles con sistema operativo *Android*, debido a que es uno de los sistemas operativos para *Smartphones* más utilizado entre los usuarios. Para finales del 2019, *Google* publicó cifras de su desempeño en *Google Play* y en el reporte se menciona que durante ese año se tuvieron más de 2.500 millones de usuarios activos en dispositivos *Android*.

Dentro de las bondades de este sistema operativo, tenemos que basa su núcleo en *Linux*, lo cual lo convierte en un sistema operativo accesible, completo, muy funcional y con una comunidad muy grande de desarrolladores. Al tener una comunidad tan grande de usuarios y de desarrolladores, se convierte en uno de los sistemas operativos con una cantidad importante de ataques de seguridad y por supuesto algo digno de estudiar en esta investigación.

## 1.3 Objetivos de la investigación.

### 1.3.1 Objetivo general del estudio

Desarrollo de un método en el campo de la Informática Forense para investigar incidentes de seguridad y delitos informáticos en los que se encuentre involucrados dispositivos móviles con sistema operativo *Android*, que permita la correcta

extracción manual, lógica y física de los datos, con el fin aplicar las técnicas y herramientas apropiadas para analizar la evidencia del caso.

### 1.3.2 Objetivos específicos del estudio

- Definición del concepto de análisis forense y descripción de sus objetivos y etapas.
- Análisis del sistema operativo *Android* y de sus características.
- Estudio de las formas de acceso a dispositivos *Android*.
- Estudio de herramientas forenses utilizadas en sistemas *Android*.
- Desarrollo de un método para realizar un análisis forense en dispositivos móviles con sistema operativos *Android*.
- Implementación del método para realizar el análisis forense en dispositivos móviles con sistema operativos *Android*.
- Aprendizaje del uso de herramientas de análisis forense.
- Extracción de la evidencia con diferentes técnicas.
- Investigación forense de diferentes muestras de *malware*.
- Selección e instalación de una herramienta forense de *Android* para un laboratorio de prueba.
- Investigación forense sobre un caso simulado.

La tecnología y su uso han evolucionado velozmente al igual que delitos en los que ésta se ve envuelta. El incremento de crímenes y ataques informáticos han generado la necesidad de crear un área de investigación como lo son las ciencias forenses orientadas a Tecnologías de la Información (TI), también conocida bajo el término de “computo forense”.

Existen otros términos para referirse a esta rama de la ciencia forense, como “informática forense”, “forensica digital”, “computación forense”, “análisis forense digital” e inclusive “examinación forense digital”, sin embargo, todos estos términos hacen referencia a la rama de las ciencia forense que se encarga de aplicar un conjunto de técnicas científicas y analíticas que permiten identificar, analizar y recolectar un

conjunto de datos o pruebas, tal que puedan brindar apoyo dentro de un proceso legal y/o judicial.

Cuando se está en presencia de algún delito informático, es porque se ha perpetrado algún hecho punible (secuestro, sustracción de datos, delincuencia organizada, delitos informáticos, entre otros) directamente relacionado con la tecnología. Para proceder ante un incidente de este tipo, es conveniente disponer de un profesional calificado, es decir, un perito informático, capaz de recolectar y verificar las pruebas digitales. A éste se le define como “un profesional experto y titulado, dotado de conocimientos legales, teóricos y prácticos especializados en informática y tecnologías de la información, capaz de asesorar o elevar un dictamen comprensible y a la vez técnico sobre un litigio o cualquier otra situación que se le requiera” (del Peso Navarro, 2001).

#### **1.4 Estructura del trabajo**

Luego de presentar en este Capítulo 1 el planteamiento del problema y la descripción del proyecto, el resto del trabajo se encuentra estructurado en 8 capítulos, organizados de la siguiente manera:

En el Capítulo 2 se hace una revisión de los conceptos y procedimientos utilizados en el área de la Informática Forense, se definen los conceptos fundamentales y los diversos procedimientos. El objetivo aquí es proporcionar una base conceptual común, que permita la interpretación correcta al momento de describir los diversos procedimientos y herramientas utilizadas en el desarrollo de este trabajo de grado.

En el Capítulo 3 se aborda la normativa legal vigente para el tratamiento de la información y que colinda con las áreas de la telefonía móvil y los dispositivos de uso personal al momento de tener que ser intervenidos mediante procedimientos forenses. Partiendo de la Constitución Nacional de Venezuela y mediante el análisis de diversas leyes y estándares, se argumenta la base legal coincidente con los objetivos del presente trabajo.

En el Capítulo 4 se analizan los diversos estándares aplicados en el tratamiento de la información, en procesos de auditoria e informática forense. También se revisa documentación, recomendaciones y normas aplicadas en diferentes países.

En el Capítulo 5 se describe la metodología aplicada para la implementación, obtención y análisis de la información durante la ocurrencia de un evento forense.

En el Capítulo 6 se describe de forma detallada el proceso de adquisición de datos, análisis de los mismos y los procesos específicos para determinar la ocurrencia de diversos eventos de adquisición de información durante el desarrollo de una investigación forense en un dispositivo móvil con sistema operativo *Android*.

En el Capítulo 7 se implementa y desarrolla el proceso de adquisición de datos para un caso de estudio, el análisis de los resultados y la descripción detallada de la operación de cada una de las herramientas utilizadas.

En el Capítulo 8 se presentan las conclusiones pertinentes a la comparación de los objetivos propuestos y los resultados obtenidos al aplicar el procedimiento de análisis informático forense.

Finalmente se presentan las conclusiones de este trabajo de grado, así como las recomendaciones para trabajos ulteriores.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1 Ciencias forenses**

Las ciencias forenses se encargan de la aplicación de prácticas y métodos científicos, dentro de estándares legales, que permiten la identificación, recepción, recolección y procesamiento de evidencias físicas de interés criminalístico, para la obtención de elementos que contribuyan con el esclarecimiento de hechos delictivos. [5]

#### **2.2 Informática forense**

La informática forense es una rama de las ciencias forense que tiene como principal objetivo asegurar, preservar, identificar, analizar y presentar un conjunto de datos extraídos de sistemas informáticos, redes, equipos de comunicaciones y dispositivos de almacenamiento. También se define como un conjunto de herramientas y técnicas que facilitan la investigación de sistemas digitales, con el fin de preservar la evidencia de forma tal que sea admisible como prueba ante la justicia.

#### **2.3 Análisis forense digital**

En el área de tecnología de la información, el análisis forense es el conjunto de procedimientos que involucra la recolección y estudio de evidencias, con el fin de conocer las causas de un incidente en el que se encuentra implicado un dispositivo informático.

Este análisis puede llegar a determinar dónde, cómo, cuándo y cuál ha sido el delito que se ha llevado a cabo y quien lo realizó. Además, contribuye con el esclarecimiento de acciones ilegales perpetradas en relación con equipos de procesamiento de datos.

Durante el desarrollo del análisis forense digital, es oportuno tener en cuenta el Principio de Intercambio de Locard. Este principio ha sido propuesto por Edmond Locard (autor y criminalista francés) y plantea que cada vez que se tiene contacto con otra persona, lugar o cosa, se genera como resultado un intercambio de material físico.

El autor explica en libro “Manual de Técnica Policiaca” que es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia”.

Cuando ocurre un delito informático, el investigador a cargo debe identificar, documentar y reunir evidencia de la escena del crimen. A pesar de que no ocurre un intercambio físico entre dispositivos, de igual manera este principio resulta aplicable al análisis forense digital, pues igualmente se realiza una transferencia de evidencias, aunque no sean físicas.

## **2.4 Objetivos del análisis forense**

El objetivo principal de todo análisis forense es contestar a las preguntas de qué, cómo, dónde, quién y cuándo se ha cometido un delito o un incidente. Esto puede ser explicado en resumen de la siguiente manera:

- Identificación del tipo incidente ocurrido y los dispositivos involucrados. Esto dictaminará el tipo de investigación y procedimiento a seguir ya que esto varía según el tipo de hecho a analizar.
- En caso de una intrusión, es importante saber cómo se realizó y bajo que procedimiento se llevó a cabo la irrupción del sistema y/o del equipo. Asimismo, cuál fue el alcance de los daños y sus consecuencias.
- Otro punto a considerar, es el determinar el rol del dispositivo envuelto en el incidente, es decir, identificar si este ha sido un elemento dentro del crimen o si ha sido un medio para obtener información.
- Finalmente, identificar al responsable del evento delictivo. Descubrir por medio del análisis, quién o quiénes son los sujetos involucrados.

### 2.4.1 Precedentes del análisis forense

En una investigación forense, la importancia de los métodos y las herramientas que se utilicen no serán importantes si la información obtenida no es auténtica. Lo cual implica que debe cumplirse una serie de requisitos para recolectar la evidencia de manera tal que garantice una investigación confiable.

Algunos de los requisitos fundamentales que toda investigación forense debe cumplir son:

- **Aceptabilidad:** dentro de la seguridad de la información existe una gran variedad de aplicaciones que permiten realizar un buen estudio forense. Muchas de estas aplicaciones son reconocidas y certificadas por expertos en el área. Por tal razón, para hacer entrega de un análisis forense creíble es importante emplear las herramientas recomendadas, de esta manera se garantiza que la evidencia no sea repudiada.
- **Integridad:** es de suma importancia que la información obtenida del análisis no sufra de ninguna alteración. Como prueba de esto, los procesos y herramientas utilizados para el almacenamiento de la evidencia que se está investigando deben estar sellados, con juegos de 2 o más copias en la que sus *hashes* sean iguales.  
En el proceso de análisis, a una de las copias se le realizará el estudio forense de datos, mientras que la otra copia corresponde al respaldo y queda al resguardo para la defensa del incidente en caso de que presenten objeciones.
- **Credibilidad:** todas las actividades realizadas deben ser demostrables; la adquisición de la información, la implementación de las herramientas debe ser conocidas, los conocimientos del investigador deben estar certificados para llevar la investigación forense.
- **Repetibilidad:** sin importar cuáles fueron los métodos de trabajo implementados o la persona que realiza la investigación, los datos de entrada deberán generar los mismos resultados.

### 2.4.2 Evidencia digital

En informática forense, la evidencia digital o prueba digital es uno de los términos más sobresalientes y se le define como la información que se encuentra almacenada y que puede ser extraída.

Como se mencionó con anterioridad, para que la evidencia digital sea probatoria debe ser: aceptable, auténtica, íntegra, creíble, segura y repetible. Según ISO/IEC 27037:2012 [11], la evidencia digital, es descrita como: “información o datos, almacenados o transmitidos de forma binaria que pueden ser tomado en cuenta como evidencia o prueba”.

Con el fin de garantizar la credibilidad a la hora de replicar información y convertirla en evidencia digital, es necesario tomar medidas de seguridad informática. Uno de los recursos más utilizados para certificar la integridad de los datos es el uso de *hashes*.

Un *hash* es el resultado de una función criptográfica que mediante un algoritmo matemático transforma cualquier bloque arbitrario de datos en una serie de caracteres alfanuméricos de longitud fija sin importar la longitud de los datos de entradas.

La evidencia digital es la base fundamental para cualquier investigación forense. Es preciso tener un protocolo del procedimiento a seguir durante toda la vida útil de la evidencia, es decir, a partir del instante en el que se obtienen los datos hasta que se destruye o ya no tiene relevancia para la investigación. A este seguimiento se le conoce como “cadena de custodia” [19]. Este procedimiento de control debe ser minucioso, tanto con el manejo de las pruebas y los hechos, como también con el personal que pueda tener acceso a la evidencia.

Es fundamental mantener la línea temporal o línea de tiempos (*timeline*), pues de esta manera es posible indagar en la información requerida en base a un criterio de tiempo útil definido para la investigación.



Para cualquier tipo de análisis, se debe crear una línea temporal con los acontecimientos o actividades que experimentó el dispositivo mientras estuvo en manos de su propietario.

## **2.5 Análisis forense en el entorno móvil**

Uno de los problemas que enfrenta el proceso de análisis forense es la constante aparición de nuevos dispositivos móviles. En un principio, el estudio forense investigaba delitos cometidos a través de medios informáticos. Lo que implicaba que las investigaciones estaban especialmente enfocadas en computadores personales (PC), estaciones de trabajo, servidores y redes.

Con el ascenso de la tecnología y la aparición de dispositivos móviles, se abrió un abanico de nuevos datos e información (*SMS*, llamadas efectuadas, llamadas recibidas, correos electrónicos, localización, etc.) a recopilar, por lo que la investigación forense se empezó a orientar a delitos que suceden en esos entornos.

Este tipo de dispositivos cuenta con un conjunto de características que hacen del estudio forense una tarea compleja y dificultosa, lo que constituye un desafío para los especialistas del área por las siguientes razones:

- Diferentes sistemas operativos: *Android* es el sistema operativo móvil de mayor uso de forma global, sin embargo, existen otros que tienen alta relevancia en el mercado, que también deberían ser conocidos en profundidad para poder llevar a cabo el proceso recolección de datos y extracción de evidencias. Algunos de ellos son: *iOS*, *Windows Phone*, etc.
- Observaciones legales: En el proceso de investigación forense es importante cumplir en todo momento con las leyes y normativas vigentes, a fin de mantener un respaldo legal de las pruebas en caso de que sea necesario.
- Técnicas anti-forenses: En un proceso investigativo es posible que la parte contraria realice diferentes acciones para entorpecer la identificación de pruebas. Por ejemplo: la pérdida, ocultación o falsificación de las pruebas.

## 2.6 Herramientas para el análisis forense

En la actualidad existe una gran variedad de herramientas tecnológicas digitales para el análisis forense que facilitan llevar a cabo la investigación de delitos informáticos. Algunas son comerciales y bastante costosas, pero a veces cuentan con versiones gratuitas con ciertas limitaciones en sus funciones.

### 2.6.1 Herramientas para el análisis de redes

Una categoría importante en las que se enfoca el estudio forense, es en las redes de datos, donde el fin fundamental es analizar el tráfico de la red (que puede estar cifrado), examinar actividades maliciosas dentro de la red e identificar conexiones desde donde se generan ataques.

Las siguientes herramientas ayudan en el análisis forense en las redes de datos:

- **Wireshark:** Permite capturar y realizar un análisis detallado de lo que sucede en la red. Generalmente es utilizado para examinar problemas de desempeño y seguridad, facilitando su solución. Disponible en <https://www.wireshark.org>
- **NetworkMiner:** Lleva a cabo diferentes tareas que facilitan el análisis forense de una red de forma sencilla, clara y rápida. Realiza capturas de paquetes para detectar los problemas que representan un riesgo para la seguridad. Disponible en <http://www.netresec.com>
- **Xplico:** es una herramienta orientada principalmente en el análisis forense de la red, mediante la extracción de los paquetes capturados del tráfico, lo que permite realizar un estudio de los datos que viajan por la red. Disponible en <http://www.xplico.org>

### 2.6.2 Herramientas para el análisis de bases de datos

Las bases de datos facilitan el manejo de una gran cantidad de datos, lo que permite el ahorro del espacio físico y tiempo al realizar consultas de información contenida en ellas. La concentración de estos datos puede utilizarse para la consumación de delitos

de diferente índole, por lo que es necesaria la utilización de herramientas especializadas que realicen un análisis forense que ayuden al esclarecimiento de hechos delictivos.

Las siguientes herramientas ayudan en la ejecución de un análisis forense en las bases de datos:

- ***Windows Forensic Tool Chest***: es un *software* que ofrece un estudio forense estructurado y repetible y da respuesta forense en vivo de forma automatizada para la consulta de incidentes, auditoría o recaudación de información relevante en un sistema operativo. Disponible en <http://www.netresec.com/?page=NetworkMiner>.
- ***SQLite***: es una biblioteca en lenguaje C que implementa un motor de base de datos *SQL* pequeño, rápido, autónomo, de alta confiabilidad y con todas las funciones. *SQLite* es el motor de base de datos más utilizado en el mundo. Está integrado en la mayoría de los teléfonos móviles y en innumerables aplicaciones que la gente usa todos los días. Disponible en <https://www.sqlite.org/index.html>
- ***DB Browser for SQLite (DB4S)***: es una herramienta de código abierto visual de alta calidad para crear, diseñar y editar archivos de bases de datos compatibles con *SQLite*. Disponible en <https://sqlitebrowser.org>
- ***MD5SUM***: es un programa que permite realizar sumas de comprobación MD5 de un archivo o una carpeta entera y almacena los resultados en un archivo texto. Lo que devuelve un único *hash* para cada archivo. Cuando se modifica un archivo, éste devuelve un *hash* distinto, lo que garantiza la integridad de los datos. Disponible en <http://www.md5summer.org>

### 2.6.3 Herramientas para el análisis de dispositivos móviles

- ***MOBILedit! Forensic***: es una herramienta comercial certificada por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU.. Facilita la extracción de información de dispositivos móviles mediante

los puertos USB o mediante *Bluetooth*, infrarrojo y Ethernet. Se encuentra disponible en <https://www.mobiledit.com/downloads>. Posee la capacidad de acceder a los datos de IMEI del dispositivo para ser registrados, para así comprobar si estos han sido reportados como robados. Los datos extraídos son guardados en formato .med y genera reportes en *Word*, PDF XSL y XML.

- ***Cellebrite***: es una empresa líder en el análisis forense informático que ofrece una amplia gama de productos tecnológicos, entre ellos su famosa herramienta *UFED Touch* para el análisis de dispositivos móviles. El *hardware* de *Cellebrite* posee batería incorporada, pantalla táctil y una interfaz de fácil manejo para el usuario. Es capaz de generar informes claros y concisos en formato HTML y XML para consultas judiciales. Disponible en <https://www.cellebrite.com/es/cellebrite-ufed-es/>
- ***Oxygen Forensic Suite***: es un *software* diseñado específicamente para el análisis lógico, búsqueda de pruebas en dispositivos móviles y presentación de informes. La herramienta comercial permite extraer información de contactos, calendario, mensajes, imágenes, videos, aplicaciones. También facilita la recuperación de una amplia variedad de datos borrados. Disponible en <https://www.oxygen-Forensic.com/es>
- ***Autopsy***: es un *software* que simplifica el despliegue de muchos de los programas y complementos de código abierto que se usan en “*The Sleuth Kit*”. La interfaz gráfica de usuario muestra los resultados de la búsqueda forense del volumen subyacente, lo que facilita a los investigadores marcar las secciones de datos pertinentes. Disponible en <https://www.Autopsy.com>
- ***Paraben’s E3 Universal***: es una herramienta que facilita el proceso de análisis forense de las unidades de disco duro, móviles e IoT, haciéndolo más eficiente y eficaz. En cuanto a dispositivos móviles, permite

realizar adquisición de evidencia lógica y física. Disponible en <https://www.paraben.com>

- **Andriller:** es una aplicación comercial que contiene, al igual que las anteriormente mencionadas, un conjunto de funciones que permiten la adquisición de datos de forma no destructiva, facilita descifrar contraseñas como patrón y PIN para dispositivos con sistema operativo *Android*, algunos dispositivos *iOS* y *Windows*. Disponible en <https://www.andriller.com>

## 2.7 Dispositivos móviles

En la actualidad muchos dispositivos electrónicos son clasificados como dispositivos móviles, desde teléfonos celulares hasta tabletas. Con tanta tecnología descrita como móvil, resulta complejo determinar cuáles son las características de los dispositivos móviles.

Un dispositivo móvil puede definirse como un elemento electrónico que cumple con cuatro características que lo diferencia y destaca de otros dispositivos. Estas cuatro características son:

- **Movilidad:** Es la cualidad de un dispositivo para ser trasladado con frecuencia y facilidad.
- **Tamaño reducido:** Es la característica de un dispositivo móvil para ser fácilmente usado con una o dos manos sin necesidad de soporte externo. El tamaño reducido permite al usuario transportar el dispositivo de forma cómoda.
- **Comunicación inalámbrica:** Es la capacidad que tiene un dispositivo de enviar o recibir datos sin la necesidad de un enlace cableado.
- **Interacción con el usuario:** Es el proceso de uso que establece un usuario con un dispositivo. Entre otros factores, en el diseño de la interacción intervienen disciplinas como la usabilidad y armonía.

## 2.8 Sistema operativo

Un sistema operativo es el conjunto de programas dedicados al control del *hardware* y *software* de un dispositivo. En otras palabras, es la interacción entre los programas o aplicaciones instaladas y el *hardware* del dispositivo, como es la pantalla, la cámara, el teclado, etc.

En un principio, esos programas fueron desarrollados para las computadoras, pero con el transcurrir del tiempo y en un entorno donde los usuarios desean realizar varios tipos de tareas en un solo dispositivo, los teléfonos móviles se abrieron paso en el avance tecnológico, hasta convertirse en una computadora que se puede llevar a cualquier lugar.

En el mundo existe una gama amplia en cuanto a sistemas operativos de teléfonos móviles se refiere y muchos de los fabricantes compiten por desarrollar un *software* que reúna todas las necesidades del usuario y llegar a ser los primeros en el mercado.

Entre los principales y más utilizados sistemas operativos en teléfonos móviles se encuentra *iOS* y *Android*. Estos sistemas cuentan con características específicas, que los hacen líderes en el mercado global y su popularidad representa un reto para sus competidores. Otros sistemas operativos son *Windows Phone*, *Symbian*, *Firefox OS*, *Ubuntu Touch*, *Tizen*, *WebOS*. Algunos han desaparecido o tienden a desaparecer.

### 2.8.1 Sistema operativo *Android*

*Android* es un sistema operativo que se desarrolló con el fin de ser utilizado en teléfonos móviles, pero que con el paso del tiempo evolucionó hasta convertirse en un sistema operativo para diferentes dispositivos, como por ejemplo, televisores, relojes inteligentes, tabletas y automóviles.

Este sistema operativo está basado en *Linux*. Es multiplataforma, libre y sobre todo gratuito, creado por la compañía *Android* INC., y que más tarde adquirió *Google*.

El constante avance de *Android*, su crecimiento, la disposición de código abierto y las licencias permisivas hacen que el *software* pueda ser modificado y distribuido

libremente por los fabricantes de dispositivos, operadores inalámbricos, etc. Además, ha permitido que desarrolladores, analistas forenses y delincuentes conozcan *Android* a un nivel mucho más profundo.

### 2.8.2 Arquitectura del sistema operativo *Android*

*Android OS* utiliza un *kernel* de *Linux* con la Interfaz de Programación de Aplicaciones (API) de alto nivel escrito en el lenguaje de programación C. Las aplicaciones se encuentran programadas en Java y se ejecutan con la Máquina Virtual Dalvik (DVM) [14]. Como se muestra en la Figura 2.1, la arquitectura de *Android* está organizada por capas. Las capas se interrelacionan entre ellas, pues cada una utiliza servicios de las capas anteriores y de forma inversa brinda sus servicios a las capas superiores. [14]

La estructura del sistema operativo de *Android* se constituye de los siguientes segmentos, tal como se muestra en la Figura 2.1:

- ***Application (Aplicaciones)***: son aquellos programas instalados por el usuario o que han sido pre-instalados en el sistema.
- ***Application Framework (Entorno de Aplicaciones)***: brinda servicios a las aplicaciones, estos servicios, generalmente, se encuentran desarrollados en Java. Mediante el *framework*, las aplicaciones que funcionan en la última capa de la estructura de *Android*, tienen acceso a las opciones básicas del sistema, como, por ejemplo, administración de actividades, notificaciones, etc.
- ***Libraries (Librerías)***: corresponde a los módulos que dan servicios al entorno de aplicaciones. Se encuentran desarrollados en C/C++ y compilados en el código de cada plataforma, además son usadas tanto por el sistema operativo como por las aplicaciones.

Estas librerías cuentan con rutinas de código reutilizables para la ejecución de funciones específicas, lo que evita la inclusión del mismo código cada vez que escribe un programa. Es decir, se garantiza que no exista redundancia de

*software*, a la vez que se ahorra recursos de memoria RAM y espacio de almacenamiento en los soportes de datos.

- **Android Runtime:** en este nivel, cada aplicación ejecuta su propia máquina virtual de Java, denominada Dalvik VM.
- **Kernel:** corresponde a la capa de más bajo nivel en la estructura del sistema operativo. El *kernel* al estar en contacto directo con el *hardware*, se encarga de gestionar procesos, memoria y herramientas de seguridad del sistema de archivos *Linux*.

Mediante diversos controladores de pantalla, teclado, cámara de vídeo, memoria flash, audio, administrador de energía, etc., el *kernel* coloca todas las funcionalidades del *hardware* al servicio del sistema operativo.

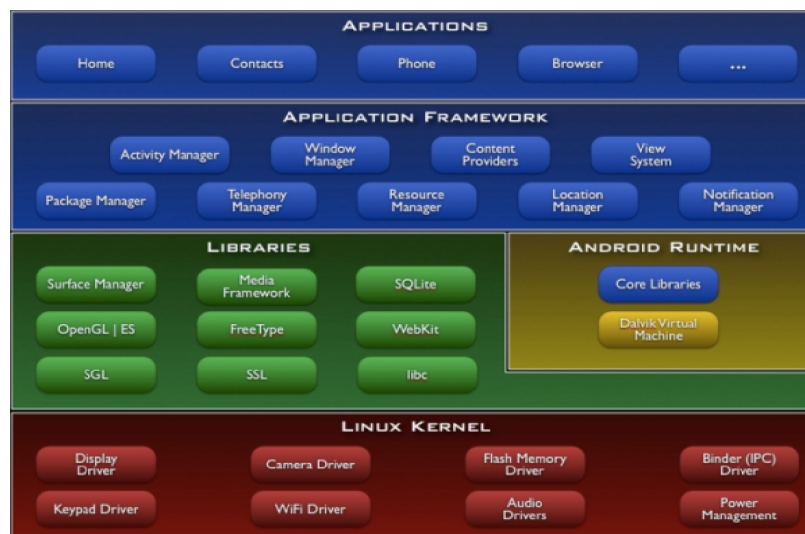


Figura 2.01: Arquitectura interna del sistema Android

Fuente: <https://developer.Android.com/images/system-architecture.jpg>

### 2.8.3 Librerías de *Android*

Las aplicaciones tienen acceso a las librerías mediante el *Application Framework* y las más destacadas son:

- **Package Manager:** controla la instalación de paquetes.



- **Activity Manager:** gestiona las actividades que son mostradas en pantalla.
- **Location Manager:** brinda información de la localización del dispositivo.
- **Notification Manager:** maneja las notificaciones recibidas por una aplicación.
- **Content Providers:** otorga el acceso a datos de aplicaciones almacenados en bases de datos.
- **View System:** controla las diferentes interfaces que se muestran al usuario.
- **Bluetooth API:** controla las conexiones *Bluetooth* del dispositivo.

#### 2.8.4 Sistema de archivos y particiones de *Android*

El sistema de archivos es el módulo dentro del sistema operativo que se encarga de administrar, gestionar y usar las memorias del terminal. Su función principal es organizar archivos mediante particiones, asignar espacio a cada uno y administrar el espacio libre restante, así como gestionar el acceso a los datos protegidos.

El sistema operativo *Android* cuenta con múltiples particiones, generalmente ubicadas en el sistema de archivos *Journal Flash File System 2* (JFFS2). En un inicio, *Android* funcionaba con YAFFS para particiones con aplicaciones preinstaladas de fábrica.

Además guardaba los datos del usuario, como por ejemplo; contactos, cuentas de correo, archivos temporales, etc. En la actualidad, YAFFS es un sistema de archivos que no se utiliza, y ha sido reemplazado por *Linux EXT4*, pues brinda mayor rendimiento y compatibilidad con los nuevos procesadores multicore.

Principales directorios:

- **/boot:** arranque.
- **/system:** información del sistema operativo e interfaz de usuario.
- **/proc:** información de los procesos en ejecución.
- **/recovery:** recuperación.
- **/mnt:** punto de montaje para otros tipos de almacenamiento.
- **/sdcard:** redirige a */mnt/sdcard*, punto de montaje de la tarjeta SD.

- **/cache:** guarda la caché de datos de las aplicaciones y del sistema.
- **/data:** directorio en el que se almacenan las aplicaciones.

### 2.8.5 Almacenamiento de datos en *Android*

El sistema operativo *Android* cuenta con diversas opciones para guardar en el dispositivo información proveniente de las diferentes aplicaciones instaladas. El almacenamiento de los datos dependerá de las necesidades del usuario, según el interés de privacidad que desea tener en esta información. *Android* cuenta principalmente con los siguientes tipos de almacenamiento:

- **Almacenamiento interno:** los archivos se almacenan en el subdirectorio `/data/data` de la aplicación y el desarrollador tiene control sobre el tipo, nombre y ubicación del archivo. El propietario debe tener privilegios de *root* para ver los archivos. Al anular la configuración de seguridad, el analista podrá leer o modificar los archivos.
- **Almacenamiento externo:** es posible que los archivos se almacenen en una tarjeta SD extraíble. Estos archivos tienen menos restricciones y son fácilmente legibles y modificables. La tarjeta SD y los datos internos también se pueden usar en otros dispositivos, lo que le da al analista un gran control sobre los nombres, formatos o ubicaciones de los archivos.
- **SQLite:** este método se utiliza para el almacenamiento de datos estructurados y es popular debido a la alta calidad de la base y su naturaleza de código abierto. Proporciona también gran material forense de datos con alta probabilidad de recuperarlos.

### 2.8.6 Componentes de aplicaciones *Android*

Los componentes de una aplicación *Android* son elementos esenciales para que se logre un funcionamiento adecuado de las mismas en el sistema operativo. Estos componentes pueden ser clasificarse como:

- **Públicos:** otras aplicaciones pueden interactuar con ellos.

- **Privados:** sólo los elementos de la misma aplicación pueden interactuar con ellos.

La mayoría de los componentes dentro de una aplicación se ejecutan dentro del mismo proceso, a menos que el desarrollador indique lo contrario.

Los componentes más importantes que se encuentran presentes en aplicaciones *Android* son:

- **Activity:** las actividades conforman la capa de presentación de la aplicación y brindan una interfaz visible de la aplicación. Por lo general, las aplicaciones tienen una o más actividades, y el objetivo principal de una actividad es interactuar con el usuario.
- **Services:** los servicios son los encargados de realizar operaciones en segundo plano sin una interfaz explícita de interacción con el usuario. Cuando una aplicación deja de estar en primer plano puede seguir ejecutándose a través de servicios.
- **Content Provider:** los proveedores de contenido están diseñados para compartir datos estructurados entre aplicaciones por medio de una interfaz, de esta manera otras aplicaciones puedan tener acceso a los datos almacenados por la aplicación.
- **Broadcast receivers:** los receptores de multidifusión son tareas que se ejecutan cuando llegan mensajes (*Intents*) generados por otros componentes de la aplicación o por otras aplicaciones. Los *broadcasts receivers* recogen el *intent*, analizan los datos transportados por el mismo y en base a ellos lanzan la aplicación o *activity* encargada de procesarlos.

### 2.8.7 Seguridad en aplicaciones *Android*

El sistema operativo *Android* cuenta con características que garantizan el amplio alcance de seguridad de la información y la privacidad de sus usuarios. Es importante considerar que *Android* es un sistema operativo abierto, que se encuentra a disposición

de los desarrolladores y los usuarios, por lo que resulta imprescindible cumplir y garantizar los siguientes principios de seguridad [1]:

- Sólida seguridad en el sistema operativo: *Android* permite limitar el código nativo que se ejecuta en los dispositivos. En el caso de que una aplicación trate de explotar una vulnerabilidad, el sistema impedirá que las zonas de memoria reservadas por otras aplicaciones se vean afectadas.

El *kernel* también proporciona un mecanismo de seguridad para las comunicaciones entre procesos. Como el sistema operativo es multiusuario, es necesario aislar los recursos de una aplicación respecto a otras, con el fin de evitar que entre distintos usuarios puedan leerse los archivos, agotar su memoria o recursos de procesamiento entre sí.

- Ejecutar todas las aplicaciones en un entorno *sandbox*: *Android* asigna un identificador único a cada aplicación que ejecuta, otorgándole un espacio de memoria reservado, que permite establecer mayor seguridad entre las aplicaciones y el sistema.

Por defecto, las aplicaciones no pueden interactuar entre sí y cuentan con un acceso limitado al sistema operativo, por ejemplo, en el caso de que una aplicación trate de invadir el espacio asignado a otra, el sistema operativo se encargará de evitarlo gracias a los permisos y privilegios establecidos para cada aplicación.

- Proceso de comunicación interno seguro: sólo es posible realizar operaciones de lectura por defecto, exceptuando carpetas especiales como la asignada a la tarjeta SD. Hay disponible un modo seguro de arranque en el que sólo están disponibles las herramientas del núcleo que fueron instaladas por defecto, asegurando un sistema libre de aplicaciones de terceros.

Al tener un sistema de archivos en permisos, se asegura que ningún usuario, excepto el autor, puede modificar o alterar el espacio reservado para una aplicación o los archivos pertenecientes a ella.

- Firmado de aplicaciones: todas las aplicaciones en el sistema operativo *Android* están encapsuladas en el formato APK. Este formato se usa para realizar la instalación y distribución de aplicaciones.

Todos los archivos tipo APK están firmados con un certificado que permite identificar al autor. En el proceso de instalación se comprueban los permisos que requiere la aplicación y usualmente se le pregunta al usuario, acción que no se realizará nunca más. Por lo tanto, la firma es uno de los mecanismos más importantes a la hora de publicar o instalar cualquier aplicación y tiene un significado diferente dependiendo del entorno en el cual se verifique.

## 2.9 Programas maliciosos: Malware

El término *malware* es el acrónimo en inglés de “*malicious software*” que se traduce al español como programa malicioso o malintencionado y puede referirse a cualquier archivo (programa, código, documento, mensaje, etc.) creado con la finalidad de ocasionar daños y perjuicios sobre la información y equipamiento de sistemas informáticos. [15]

Según *KasperskyLab*, los *softwares* maliciosos son un tipo de aplicación con archivos ejecutables que se pueden activar por sí solos y tomar distintas formas, como por ejemplo, *plug-ins*, lenguajes de *scripts* u otros lenguajes de programación que están diseñados para las mejoras de páginas web o correos electrónicos. [16]

### 2.9.1 Clasificación de *Malware*

Existen diversas maneras de clasificar los programas maliciosos, usualmente según la forma de propagación, por la capacidad de evadir mecanismos de seguridad y por un fin lucrativo. [15]

- Por su propagación:

**Virus:** es un tipo de *software* malicioso que altera el funcionamiento regular de los equipos, sin el permiso del usuario. Los virus, generalmente, se auto replican y reemplazan archivos ejecutables por otros archivos infectados y pueden destruir de manera intencionada información almacenada en los dispositivos.

**Gusanos:** es un *malware* que comparte las mismas características de un virus, se replica de forma automática, con la diferencia de que utiliza la red para enviar copias de sí mismo a otros dispositivos que se encuentren conectados a ella, provocando una enorme lentitud y bloqueo de las comunicaciones en poco tiempo.

- Por su elusión de los sistemas de seguridad.

**Trojanos:** son programas que aparentan ser aplicaciones legítimas e inofensivas. Este tipo de *malware* simula realizar la función deseada por el usuario, pero en realidad tiene características ocultas que roban información, dañan el sistema o abren puertas traseras, logrando evadir los mecanismos de seguridad del equipo. Los trojanos pueden dividirse según el daño que causan, de la siguiente manera:

- *Downloader:* descarga y ejecuta códigos maliciosos.
- *Banker:* roba credenciales de acceso financieras.
- *Dropper:* se ejecuta en paralelo con un programa legítimo.
- *Clicker:* busca beneficio económico a través de clics en publicidad.
- *Keylogger:* registra actividades que se realizan en el sistema.
- *Backdoor:* abre puertos en el sistema sin autorización.
- *Bot:* convierte el sistema en zombi.

**Rootkits:** es un conjunto de programas que modifican el sistema operativo de los dispositivos ocultando ciertos objetos o actividades en el sistema, con el fin de evadir su detección por parte del usuario o de herramientas de seguridad.

- Por su carácter lucrativo.

**Spyware:** es un *software* malicioso que se encarga de recopilar información del usuario sin consentimiento. El *spyware*, generalmente, no representa un peligro de manipulación ajena del sistema, ni suele ocasionar daños en los equipos infectados por parte de terceros. Los efectos de este *malware* son la violación de los derechos de confidencialidad de datos e información y una navegación más lenta en la red en la que se encuentra conectado el equipo.

**Adware:** Es un *malware* que despliega anuncios de productos o servicios de forma automática en una aplicación. Se encarga de mostrar textos o imágenes publicitarias en la pantalla del usuario mediante ventanas emergentes.

**Ransomware:** Es un *software* que es utilizado para extorsionar al usuario, exigiendo un pago para deshacer los cambios efectuados en los archivos. Cuando un equipo es atacado con este tipo de *malware*, bloquea el acceso del usuario o cifra la información almacenada en el disco, mostrando luego un mensaje de rescate en el que solicita el pago para recuperar la información.

## **CAPÍTULO III**

### **MARCO LEGAL**

La tecnología ha tenido y sigue teniendo un gran impacto en la sociedad, pues el fácil acceso a la información y el crecimiento de nuevas economías han marcado de manera radical el mundo tal cómo se conocía.

El uso de Internet y de dispositivos tecnológicos no sólo trajo beneficios para la sociedad moderna, sino que también ha desencadenado una ola de nuevos delitos de tipo informático. Es por ello que nace la necesidad de un marco legislativo y reglamentario que permita trabajar en el campo de las TIC bajo lineamientos jurídicos que regulen la vida en la sociedad digital.

Es por esto que los organismos reguladores nacionales e internacionales se han visto en la obligación de crear un conjunto de leyes, regulaciones y estandarizaciones que permitan que la justicia intervenga de alguna manera en las actividades informáticas.

Todo proceso de peritaje informático debe apegarse a regulaciones nacionales e internacionales. Es de suma importancia que cualquier proceso de peritaje tenga en vigor el marco legal y a pesar de que el perito no necesariamente sea un experto en el área legal, éste debe conocer y tener presente la legislación.

En Venezuela, para realizar un proceso de peritaje informático (recolección de datos, informes, dictámenes y análisis), es importante que éste se encuentre siempre apegado a la legislación venezolana.



Es indispensable tener en vigor el marco legal vigente y aunque el entendimiento de los textos legales para los inexpertos en el área pueda resultar complicado y ambiguo, es necesario tenerlos presente y tratar de clasificarlos lo mejor posible.

A continuación, se citan los artículos relevantes de las regulaciones vigentes en Venezuela en materia de seguridad de la información.

### **3.1 Constitución de la República Bolivariana de Venezuela**

#### Artículo 60

Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

### **3.2 Ley contra delitos informáticos del 2001 – Gaceta oficial No. 37.313**

#### TÍTULO I - DISPOSICIONES GENERALES

##### Artículo 1 - Objeto de la Ley.

La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

#### TÍTULO II - DE LOS DELITOS

Capítulo I - De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.

##### Artículo 6 - Acceso indebido.

Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información,

será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7 - Sabotaje o daño a sistemas.

Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientos unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizarán mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.

Artículo 10 - Posesión de equipos o prestación de servicios de sabotaje.

Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientos unidades tributarias.

Artículo 11 - Espionaje informático.

Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas (300) a seiscientas (600) unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las

instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

### Capítulo III - De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

Artículo 20 - Violación de la privacidad de la data o información de carácter personal.

Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas (200) a seiscientas (600) unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21 - Violación de la privacidad de las comunicaciones.

Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Artículo 22 - Revelación indebida de data o información de carácter personal.

Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidas por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas (200) a seiscientas (600) unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV - De los Delitos Contra Niños, Niñas o Adolescentes

Artículo 23 - Difusión o exhibición de material pornográfico.

Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Artículo 24 - Exhibición pornográfica de niños o adolescentes.

Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas (400) a ochocientas (800) unidades tributarias.

### **3.3 Ley de Infogobierno del 2013 – Gaceta oficial No. 40.274**

Ley de Infogobierno publicada en conformidad con lo previsto en el artículo 213 de la Constitución de la República Bolivariana de Venezuela el 10 de octubre del 2013.

Artículo 1 - Objeto de la ley

Esta Ley tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación.

Artículo 2 - Ámbito de aplicación

Están sometidos a la aplicación de la presente Ley:

- 1.- Los órganos y entes que ejercen el Poder Público Nacional.
2. Los órganos y entes que ejercen el Poder Público Estatal.

3. Los órganos y entes que ejercen el Poder Público en los distritos metropolitanos.
4. Los órganos y entes que ejercen el Poder Público Municipal y en las demás entidades locales previstas en la Ley Orgánica del Poder Público Municipal.
5. Los órganos y entes que ejercen el Poder Público en las dependencias federales.
6. Los institutos públicos nacionales, estatales, de los distritos metropolitanos y municipales.
7. El Banco Central de Venezuela.
8. Las universidades públicas, así como cualquier otra institución del sector universitario de naturaleza pública.
9. Las demás personas de derecho público nacionales, estatales, distritales y municipales.
10. Las sociedades de cualquier naturaleza, las fundaciones, empresas, asociaciones civiles y las demás creadas con fondos públicos o dirigidas por las personas a las que se refiere este artículo, en las que ellas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones en un ejercicio efectuados por las personas referidas en el presente artículo represente el cincuenta o más de su presupuesto.
11. Las organizaciones y expresiones organizativas del Poder Popular.
12. Las personas naturales o jurídicas, en cuanto les sea aplicable, en los términos establecidos en esta Ley.
13. Las demás que establezca la Ley.

#### Artículo 3 - Finalidad de la ley

Esta Ley tiene como fines:

- 1.- Facilitar el establecimiento de relaciones entre el Poder Público y las personas a través de las tecnologías de información.

2. Establecer las condiciones necesarias y oportunas que propicien la mejora continua de los servicios que el Poder Público presta a las personas, contribuyendo así en la efectividad, eficiencia y eficacia en la prestación de los servicios públicos.

3. Universalizar el acceso de las personas a las tecnologías de información libres y garantizar su apropiación para beneficio de la sociedad.

4. Garantizar el ejercicio de los derechos y el cumplimiento de los deberes de las personas, a través de las tecnologías de información.

5. Promover el empoderamiento del Poder Popular a través de la generación de medios de participación y organización de las personas, haciendo uso de las tecnologías de información.

6. Garantizar la transparencia de la gestión pública, facilitando el acceso de las personas a la información pública.

7. Apoyar el fortalecimiento de la democracia participativa y protagónica en la gestión pública y el ejercicio de la contraloría social.

8. Contribuir en los modos de organización y funcionamiento del Poder Público, apoyando la simplificación de los trámites y procedimientos administrativos que éstos realizan.

9. Establecer los principios para la normalización y estandarización en el uso de las tecnologías de información, a los sujetos sometidos a la aplicación de esta Ley.

10. Promover la adquisición, desarrollo, investigación, creación, diseño, formación, socialización, uso e implementación de las tecnologías de información libres a los sujetos sometidos a la aplicación de esta Ley.

11. Establecer las bases para el Sistema Nacional de Protección y Seguridad de la Información, en los términos establecidos en la presente Ley y por otros instrumentos legales que regulen la materia.

12. Fomentar la independencia tecnológica y con ello fortalecer el ejercicio de la soberanía nacional, sobre la base del conocimiento y uso de las tecnologías de información libres en el Estado.

#### Artículo 23 - Principio de seguridad

En las actuaciones electrónicas que realicen el Poder Público y el Poder Popular se debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, documentos y comunicaciones electrónicas, en cumplimiento a las normas y medidas que dicte el órgano con competencia en materia de seguridad de la información.

#### Artículo 54 - De la Superintendencia de Servicios de Certificación Electrónica

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) es el órgano competente en materia de seguridad informática, y es responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos obtenidos y generados por el Poder Público y por el Poder Popular, así como la generación de contenidos en la red.

#### Artículo 55 - Competencias

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) tendrá, en el ámbito de aplicación de esta Ley, las siguientes competencias:

1. Desarrollar, implementar y coordinar el Sistema Nacional de Seguridad Informática.
2. Dictar las normas instruccionales y procedimientos aplicables en materia de seguridad informática.

3. Establecer los mecanismos de prevención, detención y gestión de los incidentes generados en los sistemas de información y en las infraestructuras críticas del Estado, a través del manejo de vulnerabilidades e incidentes de seguridad informática.

4. Articular e insertar en el Poder Público y en el Poder Popular las iniciativas que surjan en materia de seguridad informática, dirigidas a la privacidad, protección de datos y de infraestructuras críticas, así como intervenir y dar respuesta ante los riesgos y amenazas que atenten contra la información que manejen.

5. Proponer al órgano rector líneas de investigación asociadas a la seguridad informática que apoye la solución de problemas en el Poder Público y en el Poder Popular.

6. Contribuir en la formación de las personas y del componente laboral, que promueva el establecimiento de una cultura de resguardo y control sobre los activos de información presentes en los sistemas de información.

7. Realizar peritajes en soportes digitales, previo cumplimiento del procedimiento legal pertinente, apoyando a las autoridades competentes en investigaciones, experticias e inspecciones relacionadas con evidencias digitales.

8. Evaluar los medios de almacenamiento digital, de acuerdo a los criterios de búsquedas establecidos en la solicitud de entes u organismos del Estado que así lo requieran.

9. Extraer, revisar y analizar las trazas y bitácoras de equipos y herramientas de redes.

10. Auditar el funcionamiento e integridad de aplicaciones y base de datos donde se presuma inconsistencias incorporadas con el objeto de causar daños.

11. Prestar asesoría técnica en materia de informática forense a los órganos de apoyo a la investigación penal.



12. Administrar el registro público de homologación de equipos o aplicaciones con soporte criptográfico.

13. Ejecutar las funciones de unidad de apoyo especializado de la Comisión Nacional de las Tecnologías de Información en el Poder Público, en el área de su competencia.

14. Presentar el informe anual sobre su gestión al órgano rector y a la Comisión Nacional de las Tecnologías de Información.

15. Coordinar con el órgano competente los procedimientos, acciones y actividades necesarias para el desarrollo de la gestión del Sistema Venezolano de la Calidad en materia de seguridad informática en el Poder Público y en el Poder Popular.

16. Las demás que establezca la ley.

Artículo 57 - Subsistemas que integran el Sistema Nacional de Protección y Seguridad Informática.

El Sistema Nacional de Protección y Seguridad Informática tiene como objeto proteger, resguardar, mitigar, y mejorar la capacidad de respuesta del Poder Público y del Poder Popular frente a riesgos y amenazas derivados del desarrollo de los sistemas de información. El Sistema Nacional de Protección y Seguridad Informática está integrado por:

1. Subsistema de Criptografía Nacional.
2. Subsistema Nacional de Gestión de Incidentes Telemáticos.
3. Subsistema Nacional de Informática Forense.
4. Subsistema Nacional de Protección de Datos.

# CAPÍTULO IV

## ESTÁNDARES Y NORMAS

### 4.1 Estándares a nivel internacional

#### 4.1.1 Estándar ISO/IEC 27037:2012

El estándar ISO/IEC 27037:2012 “*Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*”, son regulaciones y estandarizaciones específicas sobre la identificación, recolección y obtención de los datos a usar como evidencia en un entorno judicial.

Este estándar guía al perito sobre el proceso de manejo de la evidencia y sobre el intercambio entre jurisdicciones de la misma.

El estándar ISO/IEC 27037:2012 incluye la normativa sobre cómo se debe llevar la cadena de custodia de cualquier tipo de dispositivo tecnológico con capacidad de almacenamiento, tales como: *pendrives* USB, discos duros, computadoras, teléfonos celulares, sistemas de circuito cerrado de televisión digital, equipos con conexión a Internet, redes TCP/IP y cualquier otro similar.

Las directrices básicas de la norma sobre el proceso de recolección de evidencia, son:

- **Aplicación del método:** la evidencia digital debe ser obtenida de la manera menos invasiva, de forma tal que se preserve la originalidad de la prueba y de ser posible obteniendo copias de respaldo.
- **Proceso auditable:** el procedimiento seguido y la documentación generada deben ser auditadas por un perito ajeno al proceso de adquisición y recopilación de datos: esto garantiza mayor grado de confianza e imparcialidad. Se debe proporcionar trazas y evidencia de lo realizado y sus resultados.

- **Proceso reproducible:** los métodos y procedimientos aplicados deben ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia. Es decir, otros peritos informáticos distintos deben poder repetir el proceso de recolección de evidencia, con las mismas herramientas y deben obtener los mismos resultados.
- **Proceso defendible:** las herramientas de peritaje utilizadas en el proceso deben ser mencionadas, validadas y contrastadas según su uso y acorde al procedimiento. Además se deben tener en consideración las normas y regulaciones sobre el tratamiento de evidencia para cada tipo de tecnología. Para cada tipo de tecnología la norma divide su tratamiento en tres procesos distintos, pero como modelo genérico se debe cumplir:
  - **Identificación:** consiste en localizar e identificar la información de interés o los elementos de prueba en sus dos posibles estados, el físico y el lógico.
  - **Adquisición:** recolección de la evidencia o de una copia forense de la misma, así como de la documentación asociada a ésta.
  - **Preservación:** la evidencia ha de ser conservada y preservada para garantizar su utilidad, es decir, debe permanecer inalterada e intacta para que pueda ser admitida como prueba en el proceso legal. Este punto está dirigido a conservar la cadena de custodia y la originalidad de la prueba.

#### 4.1.2 Estándar ISO/IEC 27042:2015

El estándar ISO/IEC 27042:2015 “*Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*”, es una norma para el análisis e interpretación de evidencias digitales.

El estándar ISO/IEC 27042:2015 básicamente es una guía para la realización de análisis e interpretación de la evidencia digital, mediante la selección, desarrollo e implementación de procesos de investigación y registro de información, con el fin de

permitir que dichos procesos sean sometidos a un análisis independiente cuando sea necesario.

Para realizar un peritaje informático, la norma indica que debe considerarse lo siguiente:

- **Evidencia digital potencial:** la información debe estar identificada como posible evidencia digital.
- **Evidencia digital:** la información debe identificarse como evidencia digital, luego de que se haya realizado el correspondiente levantamiento de información y análisis forense.
- **Evidencia digital legal:** la información debe ser identificada como evidencia digital que ha sido aceptada judicialmente como prueba.
- **Investigación:** desarrollo de análisis sobre una potencial evidencia digital hasta convertirla en una evidencia digital legal aceptable.
- **Examen:** procedimientos que se implementa para identificar y recuperar una evidencia digital potencial de una o varias fuentes.
- **Análisis:** estudio de la evidencia digital potencial, con el fin de darle su posible importancia en la investigación.
- **Interpretación:** resultados de los hechos llevados a cabo en los exámenes y análisis que componen la investigación.

El estándar plantea los modelos de análisis que pueden ser usados por los peritos informáticos:

- **Análisis estático:** consiste en una inspección de la evidencia digital potencial (archivos, datos borrados, etc.), para determinar si es apta para ser considerada evidencia digital.
- **Análisis en vivo:** consiste en una inspección de evidencias digitales potenciales en sistemas que se encuentran activos, como memorias RAM, teléfonos móviles, *tablets*, redes, etc., con el objetivo de evaluar su valor como evidencia digital. A su vez, el análisis en vivo, se divide en:

- **Análisis en vivo de sistemas que no pueden ser copiados:** mediante este análisis no es posible obtener una imagen de la evidencia digital potencial, lo que implica el riesgo de perder información, al no poderse realizar una copia de la misma.
- **Análisis en vivo de sistemas que pueden ser copiados:** mediante este análisis se puede obtener una imagen digital de la información, lo que resulta más confiable a la hora de procesar los datos como evidencia digital potencial. Este tipo de sistemas realizan emulaciones de *software* o *hardware* y se utiliza para ello máquinas virtuales certificadas y entornos reales para obtener unos resultados más cercanos a la realidad.

## 4.2 Referencias internacionales

Las *Request for Comments* (mejor conocidas por sus siglas RFC), son un conjunto de publicaciones y referencias redactadas por la IETF (*Internet Engineering Tasking Force*, Grupo de Trabajo de Ingeniería de Internet). Estos documentos describen procedimientos, protocolos, métodos y diversos aspectos que sirven como pauta para llevar a cabo un proceso, creación de estándares o implantación de algún protocolo en el campo de las TIC.

Ya que muchas RFC se han convertido oficialmente en estándares, es importante mencionar algunos que son de gran interés en sector de las ciencias forenses digitales.

### 4.2.1 El Documento RFC 3227

La RFC (*Request For Comments*) 3227 es una guía de alto nivel que ayuda al perito informático a recolectar y archivar la evidencia digital. En este documento se explican las mejores prácticas para determinar la volatilidad de los datos, decidir cómo realizar o desarrollar la recolección y determinar cómo efectuar el almacenamiento y la documentación de los datos. Además, se incluyen algunos conceptos y aspectos legales a considerar.

Esta guía se puede aplicar desde la comisión de un delito informático hasta su solución en los estrados judiciales. Las directrices generales establecen lo siguiente:

- El perito debe llevar a cabo la extracción de la información tratando por todos los medios de que la pérdida sea mínima. Debe minimizar en la mayor medida posible los cambios en la información que se recolecta.
- Al desconectar la máquina de red, el perito debe evitar que se active algún programa informático que elimine información de la unidad al conectarse a alguna red o a la máquina de red.
- El perito debe saber que para cada dispositivo la recolección de información puede llevarse a cabo con un proceso distinto.
- En caso de enfrentarse en un dilema entre recolección y análisis, se debe elegir primero recolección y luego el análisis.
- La información debe ser recolectada por orden de volatilidad, de mayor a menor.
- Se deben incluir notas detalladas que incluyan la hora y la fecha.
- Se debe capturar una imagen digital del sistema.
- Se debe anotar el sitio de la evidencia, sistemas involucrados en el incidente, así como datos sobre las personas y/o departamentos involucrados. De igual manera se deben incluir las respuestas a las preguntas sobre dónde ocurrió, qué estaban haciendo y cómo reaccionaron.



Tabla 4.1: Volatilidad de la Información..

Asimismo, la recolección de evidencia debe cumplir con los principios de:

- **Admisibilidad:** las pruebas deben cumplir las leyes del país donde se ejecute el caso.
- **Autenticidad:** se debe comprobar que la evidencia es genuina.
- **Completitud (suficiencia):** las pruebas deben ser completas, no parciales. Estas deben ser las requerida para sustentar y verificar las afirmaciones efectuadas sobre el caso.
- **Confiabilidad:** no se debe poner en duda el proceso de recolección de las pruebas. No debe haber duda sobre la legitimidad y autenticidad.
- **Credibilidad:** las pruebas deben entenderse y ser fidedignas para el tribunal. Para tal fin es necesario:
  - Un programa para examinar el estado del sistema.
  - Un programa para realizar copias bit a bit.
  - Un programa para calcular sumas de verificación o códigos *hash*.
  - Un programa para la generación de imágenes básicas y para analizar éstas.
  - Una secuencia de comandos para automatizar la recopilación de pruebas.

#### **4.2.2 El documento RFC 4810**

Es necesario para un investigador forense poder probar la existencia de datos en un instante específico y poder demostrar la integridad de los datos desde ese momento, incluso cuando la duración desde el inicio de la existencia de la información hasta el final de la demostración abarca una gran cantidad de tiempo. Además, los investigadores forenses deben poder verificar firmas en datos firmados digitalmente muchos años después de la generación de la firma. La RFC 4810 es un documento que describe una clase de servicios de archivos para soportar tales escenarios y la técnica para interactuar con dichos servicios.

#### **4.2.3 El documento RFC 4998**

La RFC 4998 define una guía para la preservación de la información, incluyendo la información firmada digitalmente. Explica cómo demostrar su existencia e integridad durante un periodo de tiempo que puede ser desconocido o indeterminado.

Aquí se definen qué tipo de sistema de archivos que pueden ser usados según el escenario y los requisitos que se deben cumplir en el registro de evidencias para evitar que éstas sean rechazadas.

#### **4.2.4 El documento RFC 6283**

La RFC 6283 es un documento que plantea un modelo para demostrar la integridad de la información y la validez de los datos, mediante la sintaxis de registro de pruebas en formato XML. Esta RFC especifica la sintaxis y procesamiento de reglas para la creación de evidencias con el fin de que no sean rechazadas a largo plazo.

### **4.3 Convenio de Budapest**

El Convenio de Budapest es un tratado internacional establecido con el fin de proteger a la sociedad, inmersa en el mundo digital, de los delitos informáticos y los delitos que se suscitan en Internet, mediante la formulación de leyes y normativas, la mejora de las técnicas de investigación y el aumento del apoyo internacional.



El tratado fue firmado en la ciudad de Budapest, el 23 de noviembre de 2001 y entró en vigencia el 1 de julio de 2004. En la actualidad, este convenio ha sido aprobado por más de 50 países de todo el mundo, sin embargo, Venezuela no es uno de ellos.

El Convenio de Budapest surgió como resultado de:

- La necesidad de cooperación entre los países en la lucha contra la ciberdelincuencia.
- La necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.

Es el único acuerdo internacional sobre delitos informáticos que enfatiza las infracciones de derechos de autor, fraude informático, pornografía infantil, delitos de odio y violaciones de seguridad de red. Tiene como fin prevenir, detectar, investigar y sancionar actos que pueden poner en peligro la confidencialidad, integridad y disponibilidad de la información, estableciendo acciones que permitan una cooperación internacional rápida y fiable.

También busca homogeneizar las definiciones sobre delitos informáticos, garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos de individuos que buscan defender su propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto por la vida privada.

El Convenio de Budapest representa un instrumento internacional que permite la cooperación contra el cibercrimen de cualquier tipo de nivel.

## **CAPÍTULO V**

### **METODOLOGÍA**

Llevar a cabo un proceso forense en equipos móviles no es más que un tipo de investigación forense que se orienta en recopilar y analizar los datos, considerados evidencia digital, almacenados dentro de un dispositivo electrónico móvil involucrado en algún tipo de incidente de seguridad.

La labor de extracción y análisis de las pruebas debe llevarse a cabo procurando la menor alteración posible de estos datos, pues de lo contrario, no se tendría una evidencia sólida ni confiable en términos forenses. Para lograr conservar la integridad de la evidencia, durante el proceso de evaluación forense digital se deben establecer reglas precisas para que se efectúe de forma correcta la incautación, aislamiento, transporte, almacenamiento, análisis y documentación de la evidencia.

Un proceso de análisis forense consistente garantizará que los resultados pueden ser repetibles y defendibles.

No existe un procedimiento estándar establecido para realizar un análisis forense en un dispositivo móvil. Sin embargo, se han desarrollado una gran variedad de guías que pueden orientar el proceso, además de proporcionar una visión general de las consideraciones pertinentes para la extracción de evidencia de dispositivos móviles. Entre los modelos más destacados y estudiados se encuentran:

- Modelo según la Norma UNE 71506:2013, de AENOR1.
- Modelo según Francisco Lázaro Domínguez, en el libro “Introducción a la Informática Forense”.
- Modelo según el NIST2, en la *Special Publication 800-86*.
- ISO/IEC 27037:2012, Orientaciones para la identificación, recogida, adquisición y preservación de la evidencia digital (*Guidelines for identification, collection, acquisition and preservation of digital evidence*).

- La RFC 3227, aunque no hace referencia directa a los dispositivos móviles, pero se puede considerar una referencia estándar en el proceso forense de computadoras.
- UNE 197010:2015 contiene criterios generales para la elaboración de informes y conjeturas periciales sobre Tecnologías de la Información y las Comunicaciones (TIC). Esta norma tiene por objeto establecer requisitos formales que deben tener los informes y dictámenes periciales en el área de las TIC.

El proceso de análisis forense consiste en el seguimiento, de forma ordenada y sistemática, de un conjunto de técnicas que permiten el estudio e investigación de evidencias en un incidente de seguridad, mediante la implementación de herramientas forenses.

Un buen proceso investigativo debe cumplir con dos requisitos principales:

- **Repetitividad:** consiste en la capacidad de replicar resultados con exactitud, partiendo de las mismas condiciones iniciales y usando los mismos métodos y herramientas. El procedimiento de repetitividad se lleva a cabo, en el supuesto de que, al repetirse una prueba, se debe llegar a las mismas conclusiones encontradas en el informe.
- **Reproducibilidad:** se trata de la posibilidad de obtener los mismos resultados bajo las mismas condiciones iniciales, utilizando el mismo procedimiento, pero con diferentes medios, es decir, implementando otras herramientas o técnicas forenses.

Se dice que un proceso de análisis forense es “*forensically sound*”, si se garantiza que la evidencia no ha sido alterada o destruida. Es decir, si el proceso de recolección, manejo, resguardo y análisis de las pruebas puede asegurar que no han sido modificadas o alteradas mientras se realiza el proceso.

## **5.1 Fases fundamentales de una investigación forense**

Con el paso del tiempo se han desarrollado diversos modelos de estudio forense digital con distintas fases o etapas, con el fin de apoyar a los investigadores en el proceso de análisis de información y evidencias.

Cada modelo cuenta con características diferentes, sin embargo, la mayoría abarca etapas muy similares entre sí. El criterio de elección del método a seguir dependerá del tipo de incidente a investigar. En este sentido, a continuación, se detallan las cuatro fases primordiales que se deben considerar para implementar un proceso de análisis forense digital.

### **5.1.1 Fase de identificación de la escena**

En esta fase se involucran dos procesos importantes para cualquier tipo de investigación forense: la identificación y recolección de evidencias.

Es fundamental que el investigador elabore la documentación donde se registren los datos relevantes del incidente y toda la información de interés, para luego dar inicio al proceso de análisis. Una vez iniciado el proceso de investigación y de identificación de los elementos implicados en el incidente, se comienza otra parte importante, que consiste en la búsqueda y recolección de evidencia. La evidencia obtenida debe ser debidamente extraída para facilitar su manipulación en las siguientes fases.

### **5.1.2 Fase de preservación de la evidencia**

En esta fase es necesario tener una documentación de los métodos que se utilizarán para la preservación de la evidencia, es decir, el almacenamiento y etiquetado de la misma. Este proceso de resguardo de las pruebas debe realizarse de forma rigurosa debido a que la información manejada será utilizada en las siguientes fases. Es de gran importancia realizar copias de todos los dispositivos que contengan datos clasificados como evidencia y además mantener la correcta documentación en la cadena de custodia, pues la evidencia debe estar intacta para su conservación.

### **5.1.3 Fase de análisis de la evidencia**

Para comenzar con la fase de análisis, se requiere las autorizaciones correspondientes al caso, además de las herramientas y procesos adecuados para manipular la evidencia.

Esta etapa tiene como objetivo el restablecimiento de los hechos del incidente, desde su inicio hasta el momento del hallazgo, con el fin de descubrir cómo se produjo el incidente o delito, quién lo ejecutó, bajo qué condiciones se llevó a cabo y sabiendo además con qué objetivo y cuáles consecuencias tuvo. Una vez concretada esta información, se dará por concluida la fase de análisis.

### **5.1.4 Fase de documentación del incidente**

Es importante tener un registro de información para documentar cada una de las actividades que se realizan durante el proceso de investigación, desde el momento en que se descubre el incidente hasta terminar con la etapa de análisis de la evidencia. La documentación generada en las fases previas permitirá realizar un informe final donde se detallarán los resultados de la investigación y los hechos más importantes de lo ocurrido.

## **5.2 Desarrollo de la metodología**

Luego de comprender que los modelos que presentan metodologías para la investigación forense no son absolutos y que cada uno tiene características que los hacen particulares según sea el caso a investigar, es posible realizar una aproximación metodológica, con lineamientos generales apropiados, que permita reducir errores, asegurar el uso de herramientas y garantizar que los procedimientos a seguir sean los adecuados y puedan reproducirse logrando los mismos resultados.

En esta sección se presenta la propuesta de una metodología para el análisis forense de dispositivos móviles, basada en el estudio y comprensión de los conceptos y modelos de análisis. Se propone un método general, considerando aquellos conocimientos y métodos estándares existentes en el área de investigación forense

física y digital. Esta propuesta tiene como intención optimizar procedimientos previamente analizados, que permitan obtener una guía práctica y sencilla de implementar, enfocado en los dispositivos móviles.

La metodología propuesta cuenta con un modelo compuesto de cinco etapas, a saber:



Figura 5.01: Etapas de la metodología propuesta

### 5.2.1 Fase de preparación



Figura 5.02: Etapa de preparación

Esta fase abarca todos los procedimientos necesarios para generar el entorno de pruebas preciso y de esta manera llevar a cabo la inspección de las pruebas y la recuperación de la información.

Inicialmente se clasifican los elementos físicos que se van a examinar y luego se realiza la descripción de la evidencia encontrada en cada uno de ellos. En ocasiones, esta tarea se realiza paralelamente con la incautación y aislamiento de la evidencia.

Es importante actuar ágilmente para dar una respuesta rápida al incidente y a su vez evitar la eliminación o pérdida de información. Por ejemplo, en el transcurso de la confiscación de un dispositivo móvil, la primera tarea que se debe realizar es la

preservación de la evidencia utilizando una “jaula de Faraday”, para así aislar el equipo de señales externas que pudiesen perturbar los datos.

En caso de no disponer de una jaula de Faraday, el aislamiento se puede lograr con otros métodos también efectivos. Una alternativa es, introducir el dispositivo móvil en un envase metálico que obstaculice el paso de las ondas de radio.

En esta etapa también se contempla todo lo relacionado con crear actividades y medidas que preserven el lugar de los hechos a investigar. Para mantener una apropiada protección de la escena, evitar la contaminación, pérdida, alteración y sustracción de evidencia, es necesario tener en cuenta lo siguiente:

- Conservar el lugar de los hechos en su forma original.
- Establecer un perímetro dentro del cual se supone existe la mayor cantidad de evidencia.
- Proteger la escena de manera constante durante el allanamiento del lugar y mientras los investigadores realizan su labor. La protección del área finaliza cuando las autoridades correspondientes dispongan de lo contrario.
- Delimitar áreas de libre acceso que no afecten a la evidencia, ni alteren el lugar de los hechos.

### 5.2.2 Fase de identificación



Figura 5.03: Etapa de identificación

En la fase de identificación se recolecta información referente a dónde y cómo se encuentra el lugar de los hechos. Tras la identificación de estos datos es posible tomar decisiones sobre las acciones y procedimientos necesarios para continuar con el análisis

forense. Esta etapa pretende ubicar información clave de los involucrados, tanto del dueño del dispositivo como de los posibles sospechosos involucrados en el incidente de seguridad.

Para una adecuada identificación de la escena se debe tener en cuenta lo siguiente:

1. Registro del estado inicial.

Con el levantamiento de información inicial, se podrá recolectar información sustancial que podría ser de utilidad en el ámbito legal, por lo que debe ser documentada con detalle. La documentación del estado inicial debe contener:

- Lugar del hecho: se debe llevar un registro del lugar en que se suscitó el incidente o delito, utilizando como recursos, fotografías y videos de cómo se encuentra el lugar de los hechos. Esto debe realizarse antes de iniciar con cualquier tipo de actividad, sea de recolección o análisis de evidencia. Por otro lado, también es necesario el control y registro de datos mediante un documento, para que haya constancia de todo tipo de la información que describe el delito. Este documento debe incluir la siguiente información:

1. Fecha del suceso.
2. Código del caso.
3. Detalles del suceso.
4. Nombre y apellidos del investigador asignado.
5. Fotografías y videos de la escena.

- Dispositivos: se debe tener un soporte en el que se lleve el registro mediante fotografías y videos que muestran el estado del dispositivo que será incautado. En este caso la investigación se encuentra orientada a los teléfonos celulares. Sin embargo, es necesario también documentar todos los dispositivos (computadoras, laptops, etc.) que se encuentren en el lugar de los hechos y sean considerados parte de la evidencia.



## 2. Identificación del dispositivo.

Cada uno de los dispositivos implicados en el suceso debe ser debidamente identificado y etiquetado. Para realizar esta actividad, es necesario tener en cuenta tanto el estado y características del teléfono celular, como la documentación existente del dispositivo. Para realizar una identificación apropiada es importante considerar:

- Estado y características del dispositivo: para llevar un mejor control del dispositivo incautado, todo se debe justificar y documentar adecuadamente, por tanto, el registro debe contar con la siguiente información:
  1. Estado del dispositivo: Encendido/Apagado.
  2. Protegido por clave: Sí/No.
  3. Tipo de protección.
  4. Marca del teléfono.
  5. Modelo del teléfono.
  6. Número de teléfono.
  7. Operadora del servicio.
  8. Número Serial (IMEI).

### 5.2.3 Fase de adquisición



Figura 5.01: Etapa de adquisición

Esta fase contempla toda actividad relacionada con la reproducción exacta de la información digital alojada en el dispositivo incautado. En el mejor de los casos, la adquisición de información de un dispositivo no debería modificar el estado físico ni lógico del equipo. No obstante, resulta difícil mantener la información intacta y esto

dependerá del tipo de recuperación de los datos y las herramientas utilizadas. En tal caso se verán afectados:

- Fecha y hora de acceso a archivos.
- Eliminación o creación de archivos.
- Alteración de la memoria del dispositivo.

Para que la integridad del análisis no se vea afectada es de fundamental importancia documentar todos los tipos de adquisición realizada y los efectos sobre el dispositivo. También es conveniente destacar que durante el proceso de adquisición de datos en un dispositivo móvil se debe proceder, de forma general, del medio más volátil al medio menos volátil.

En la etapa de adquisición se puede encontrar, tanto evidencia física como lógica, relacionada con el dispositivo móvil a investigar. Como se mencionó anteriormente, es importante manipular esta información con extremo cuidado, para así garantizar la preservación de la integridad de los datos y que esta sea admisible como evidencia. Para lograrlo se trabaja bajo el esquema de una cadena de custodia.

Durante este proceso también se debe seleccionar una herramienta de *software* que se adecue a las características del caso de estudio para la recolección de evidencia. Esta herramienta permitirá la recolección de pruebas, que luego será clasificada de acuerdo a un orden de prioridad.

- Cadena de custodia: se define como: “el mecanismo que garantiza la autenticidad de los elementos de prueba recolectados y examinados, esto es, que las pruebas correspondan al caso investigado, sin que dé lugar a confusión, adulteración, ni sustracción alguna.” (Fuertes Rocañín, Cabrera Forneiro, & Fuertes Iglesias, 2007).

La aplicación de la cadena de custodia es de relevante importancia ya que brinda un valor altamente significativo a la investigación. De esta manera se garantiza que el procedimiento empleado ha sido exitoso y

que la evidencia recolectada no ha sufrido ninguna alteración, por lo que puede ser utilizada y presentada ante un tribunal civil o penal.

En cuanto a la evidencia dentro de la escena y el tratamiento de ésta en el proceso investigativo, es importante tener en cuenta lo siguiente:

- Los elementos de prueba encontrados dentro del lugar de los hechos deben tener un trato adecuado en la recolección de los mismos.
  - Los elementos de prueba deben tener un mantenimiento adecuado para su conservación durante el proceso investigativo.
  - La entrega de los elementos de prueba debe ser debidamente fiscalizada.
- Identificación de la herramienta de *software* para la recolección de evidencia: esto es muy importante para el análisis forense de teléfonos celulares, y debe permitir la extracción completa de la información del dispositivo que contenga datos relacionados con el caso.

Para elegir una herramienta adecuada se debe considerar:

- Preseleccionar las posibles herramientas a ser utilizadas en el caso, con una descripción que determine las más adecuadas y compatibles con el modelo y características del teléfono celular.
  - Establecer una comparación de funcionalidades entre las herramientas previamente seleccionadas, de forma que se determine las más apropiadas para el caso según las características del dispositivo a investigar. El costo es un factor importante a considerar.
- Recolección de evidencia: el tipo de adquisición de evidencia que se lleve a cabo sobre un equipo móvil dependerá de las características del mismo y de los puntos relevantes de la investigación. Se intentará dar respuesta a los puntos clave del incidente o delito usando los métodos menos invasivos posibles.

- Inspección y priorización de la evidencia: una vez realizada la recolección de la evidencia se recomienda realizar una inspección y priorización de la misma. Este procedimiento es pertinente realizarlo antes de dar inicio a la etapa de análisis de evidencia para así dar continuidad al control y seguimiento de la cadena de custodia. Para una inspección y priorización adecuada es importante:
  - Realizar un recuento breve del tipo de caso que se está investigando y buscar la evidencia que se encuentra más relacionada con el incidente o delito.
  - Ordenar la evidencia encontrada según el grado de importancia.

### **1.-Adquisición manual**

Este método de adquisición de información sólo es realizable si el teléfono se encuentra desbloqueado y es el más sencillo de todos los métodos, ya que consiste en usar el teclado o la interfaz táctil para navegar a través del dispositivo. En la adquisición manual hay que clasificar todas las aplicaciones existentes y registrar fotográficamente la información encontrada de los elementos que se consideren relevantes para el caso a investigar. El proceso de extracción es relativamente sencillo, pues no se requieren herramientas o técnicas especiales, pero consume tiempo y es propenso a errores humanos. Por ejemplo, es posible que se escapen ciertos datos que no son visibles a través de la interfaz de usuario o debido a la falta de familiaridad con el equipo. Además, con la adquisición manual no es posible recuperar datos borrados, ni extraer la totalidad de la información. Un último recurso a utilizar en este proceso es la conexión del equipo a Internet, pero hay que tener en cuenta que el dispositivo podría ser bloqueado remotamente.

### **2.-Adquisición lógica**

La extracción lógica permite obtener datos del dispositivo mediante el acceso al sistema de archivos. Esta adquisición de evidencias se suele realizar con herramientas que se comunican con el sistema operativo. Permite obtener datos como registros de

llamadas, mensajes, contactos, imágenes, vídeos, archivos de audio, etc. Sin embargo, estos datos se pueden recuperar siempre y cuando no hayan sido borrados.

### 3.-Adquisición física

El método de adquisición física es uno de los más completos a la hora de extraer datos, ya que se accede directamente al sistema de almacenamiento interno y externo. Esta técnica permite realizar una copia *bit a bit* de toda la información guardada en el dispositivo y además amplía las posibilidades de recuperar la mayor cantidad de datos, tanto los datos eliminados como los datos ocultos. Mediante este método se pueden recolectar datos como contraseñas, aplicaciones, información de ubicación, imágenes, videos, correos electrónicos, etc.

Las técnicas de extracción física pueden ser por *hardware* o *software*:

- Extracción física por *hardware*: Se lleva a cabo con el uso de métodos que conectan un *hardware* al dispositivo o que extraen los componentes del dispositivo móvil físicamente.

La extracción mediante *Chip-off* es un método agresivo que consiste en extraer físicamente el circuito de memoria NAND de la placa base del equipo. Tiene como principal ventaja poder analizar equipos dañados y evadir cualquier bloqueo de seguridad. Sin embargo, si el dispositivo se encuentra cifrado, este método no será tan útil para extraer los datos de la memoria.

Otro proceso de extracción por *hardware* es el JTAG (*Joint Test Action Group*). Este método consiste en acceder a un determinado *chip* mediante conexiones eléctricas con los pines del circuito. Con este método se puede acceder a funciones de lectura y escritura de los elementos contenidos en un *chip* de memoria, sin extraerlo de la placa donde se encuentra conectado. La extracción de información por JTAG es complicada debido a las variaciones de *hardware* entre fabricantes, por lo que se debe contar con equipos y personal especializado en circuitos electrónicos. Además, existe el riesgo de producir daños en el *chip* por aplicar voltajes incorrectos o por el mal uso de las

soldaduras, lo que podría generar pérdidas irrecuperables de datos almacenados en el dispositivo.

El método de extracción física por *hardware* también permite registrar un código de programación en el dispositivo, con el fin de saltar el bloqueo e instalar el código en la memoria RAM. Esto servirá para leer la información contenida en la memoria *flash* y finalmente transferirla al equipo forense para su análisis.

- Extracción física por *software*: se realiza con la ejecución de programas en el equipo, con acceso *root* y con la finalidad de obtener una imagen física de todas las particiones de datos.

Este proceso de extracción requiere acceso al dispositivo como usuario *root*, esto ofrece un control privilegiado del sistema operativo y es análogo a como se realiza en el Linux para privilegios de *superuser*. Sin embargo, al cambiar los privilegios de acceso, se generan modificaciones al equipo, por lo tanto resulta ser una técnica con muchos obstáculos para el investigador. Este procedimiento de acceso como usuario *root* varía según el fabricante y la versión de *Android*.

#### 5.2.4 Fase de análisis



Figura 5.02: Etapa de análisis

La fase de análisis de la evidencia es una etapa en que se trabaja con mucho detalle durante la investigación, ya que tiene como objetivo obtener respuestas sobre el incidente de seguridad que dio inicio a la investigación. Durante esta fase se genera la mayor cantidad de información que será anexada al informe de la etapa final. Para

adquirir esta información se requiere aplicar ciertos procesos, métodos y técnicas a la evidencia recolectada, de tal forma que se pueda reconstruir de la mejor manera posible los hechos ocurridos en el incidente. Para esto es importante considerar:

1. Identificación de la herramienta de *software* para el análisis de la evidencia: es importante elegir una herramienta apropiada que permita realizar un análisis minucioso de la evidencia colectada.
2. Análisis de la evidencia digital: se debe examinar todo tipo de información presuntamente relacionada con el incidente y con el dispositivo incautado. Para esto se debe tomar en cuenta lo siguiente:
  - Análisis de información almacenada.
  - Recuperación de archivos borrados.
  - Identificación de aplicaciones instaladas.
  - Análisis de archivos sospechosos.
  - Identificación de archivos involucrados en el caso.
  - Construcción de la línea de tiempo.

### 5.2.5 Fase de presentación



Figura 5.03: Etapa de presentación

La última fase del proceso forense es la presentación de los resultados del caso y es importante elaborar un informe final que contemple la información recolectada en el proceso de adquisición que fue llevado a cabo en la investigación, dónde se justifiquen y describan los hallazgos obtenidos, acciones y hechos durante el proceso de investigación.

El informe final debe ser redactado de forma clara y concisa, tal que sea de fácil comprensión para todos los involucrados, a nivel técnico y legal.

La estructura del informe final debe contar con lo siguiente:

- Periodo de investigación con la fecha de inicio y fecha de cierre de la investigación.
- Nombre del investigador forense o emisor del informe.
- Asunto.
- Resumen: identificación de la escena, recolección de la información y descripción de la evidencia.
- Resultados del análisis de la evidencia.
- Conclusiones.
- Archivos y datos relevantes adjuntos.

### **5.3 Recomendaciones para la implementación de la metodología**

La metodología descrita anteriormente puede ser utilizada como una guía para la realización de una investigación forense digital de dispositivos móviles.

Es importante destacar que se deben implementar los procedimientos y métodos de la guía en el orden propuesto, para que de esta manera se pueda garantizar que la evidencia no sufra alteraciones durante la investigación y que se pueda llevar a cabo un análisis forense íntegro y estructurado.



## CAPÍTULO VI

### INVESTIGACIÓN FORENSE EN DISPOSITIVOS MÓVILES

La finalidad de la investigación forense digital radica en la aplicación de un conjunto de métodos y técnicas con el fin de extraer y analizar información valiosa de las tarjetas de almacenamiento de elementos informáticos que se encuentren involucrados en incidentes de seguridad, sin que esta información sufra modificación alguna durante el proceso. De esta forma se obtiene la evidencia digital que podría ser presentada ante un proceso judicial, si lo requiere el caso.

A continuación, se presentarán diferentes técnicas de extracción y análisis de información en dispositivos móviles con sistema operativo *Android*.

#### 6.1 Adquisición de datos

##### 6.1.1 Adquisición manual de datos

La adquisición manual de datos es una forma rápida y relativamente sencilla de descubrir información a través de la interfaz de usuario de un dispositivo *Android*. El investigador puede encontrar datos accediendo al registro de llamadas y mensajes de texto, examinando las fotografías, explorando el historial del navegador web y clasificando los datos en aplicaciones de terceros.

De esta forma se pueden analizar los datos accesibles en el instante de la revisión. Sin embargo, es un método propenso a errores, ya que los investigadores corren con el riesgo de alterar accidentalmente los datos o comprometer la integridad del dispositivo y su contenido.

Otro factor importante a considerar con este método, es que no es posible recuperar datos eliminados, ni extraer la totalidad de la información. Una forma rápida de realizar la extracción manual de información de un dispositivo *Android*, es mediante un explorador de archivos, que facilite la búsqueda y visualización de datos contenidos en el equipo, el cual puede observarse en la Figura 6.01:

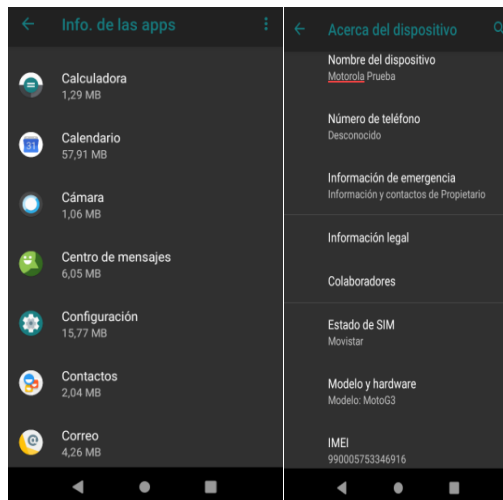


Figura 6.01: Administrador de dispositivos en un sistema *Android*

Es común que los dispositivos móviles dispongan de un administrador de archivos instalado de forma predeterminada, sin embargo, se puede reemplazar por un gestor más avanzado y de mayor alcance que permita acceder de forma sencilla al *file system*, como por ejemplo *FS File Explorer*, tal como se muestra en la Figura 6.02, el cual permite visualizar archivos ocultos:

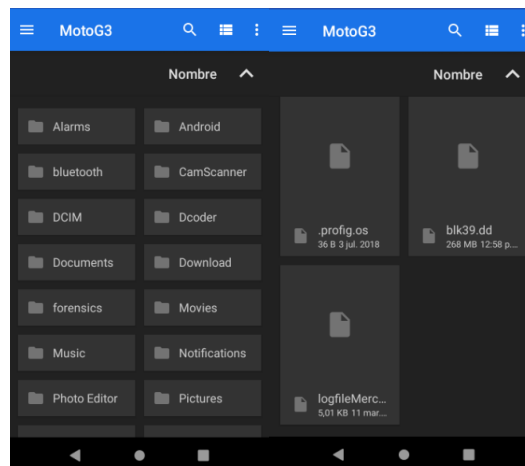


Figura 6.02: Sistema de administración de archivos del Motorola G3

### 6.1.2 Adquisición lógica de datos mediante MTP y conexión USB

La adquisición lógica de información utilizando MTP y conexión USB consiste en extraer los archivos que se encuentran almacenados en una partición lógica del sistema. Este proceso se lleva a cabo al conectar el dispositivo móvil al equipo de investigación forense (laptop o PC) mediante conexión USB o *Bluetooth*. Una vez se establece la comunicación entre los equipos, se ejecutan comandos para copiar los directorios a una tarjeta SD externa o de forma directa al equipo de investigación, para ser analizados posteriormente.

Para que exista comunicación entre un dispositivo móvil y una computadora mediante conexión USB es imprescindible que ciertos *drivers* se encuentren instalados en la computadora. Dado que *Android* es un sistema de *software* libre, es decir, puede ser modificado y personalizado por los fabricantes, no existe un controlador genérico que funcione correctamente para todos los equipos con este sistema operativo.

Cada fabricante tiene *drivers* específicos y por lo general son distribuidos junto con el dispositivo. Por otro lado, *Windows* cumple la función de instalar de forma automática los controladores al momento de conectar el dispositivo a la computadora vía USB, tal como se muestra en la Figura 6.03:

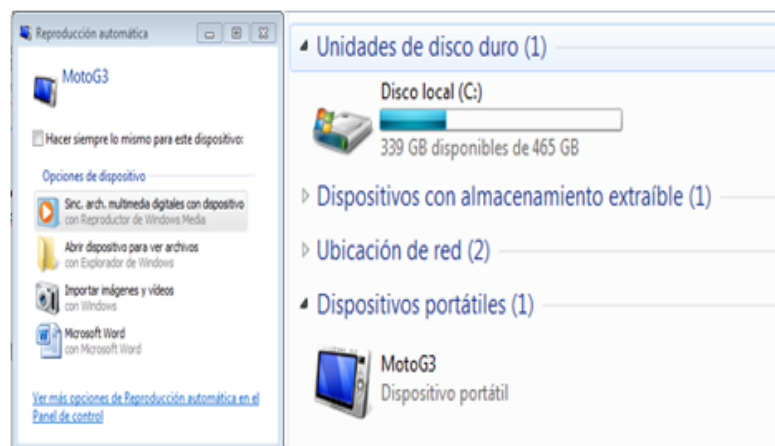


Figura 6.03: Detección automática de un dispositivo en sistema *Windows*

Los dispositivos, al ser conectados a la computadora, solicitarán permisos de transferencia de archivos para establecer la comunicación entre los equipos. Por tal razón se selecciona la opción *Media Transfer Protocol* (MTP), tal como muestra la Figura 6.04:

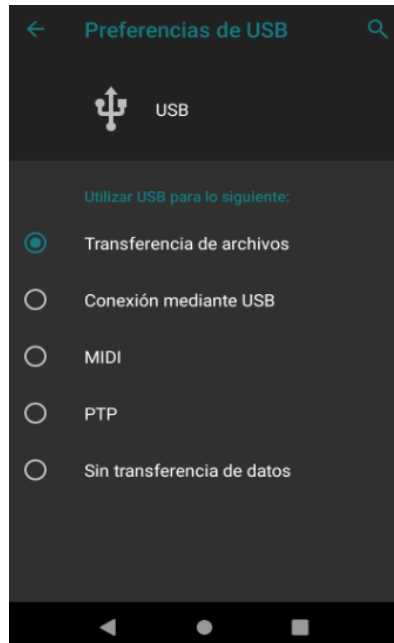


Figura 6.04: Ejemplo de *Media Transfer Protocol* (MTP)

Si se realiza la detección del equipo de forma exitosa, se podrá observar el reconocimiento de una unidad de almacenamiento, a la cual se podrá acceder y realizar copia de las carpetas y los archivos. De esta manera se alcanza un acceso básico al *file system* del dispositivo, tal como se muestra en la Figura 6.05:

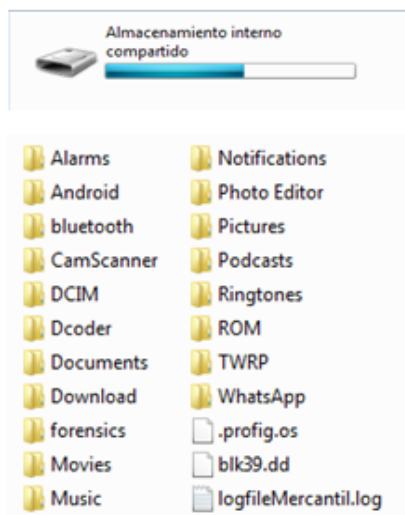


Figura 6.05: Ejemplo de acceso al sistema de carpetas internas de un dispositivo móvil desde el sistema *Windows*

### 6.1.3 Extracción lógica de datos mediante conexión USB y ADB

La herramienta *Android Debug Bridge* (ADB) forma parte de *Android SDK* (*Software Development Kit*) y es uno de los métodos más utilizados en el análisis forense de dispositivos móviles.

Para poder trabajar con el aplicativo ADB, se requiere activar la opción “Depuración por USB” que se encuentra en la ruta Ajustes | Opciones del programador.

En versiones recientes de *Android* esta función está oculta de forma predeterminada. Para habilitarla, se debe seguir la ruta Ajustes | Acerca del dispositivo y tocar 7 veces la opción Número de compilación. Al completarse la activación, se abrirá una pantalla como la mostrada en la Figura 6.06:

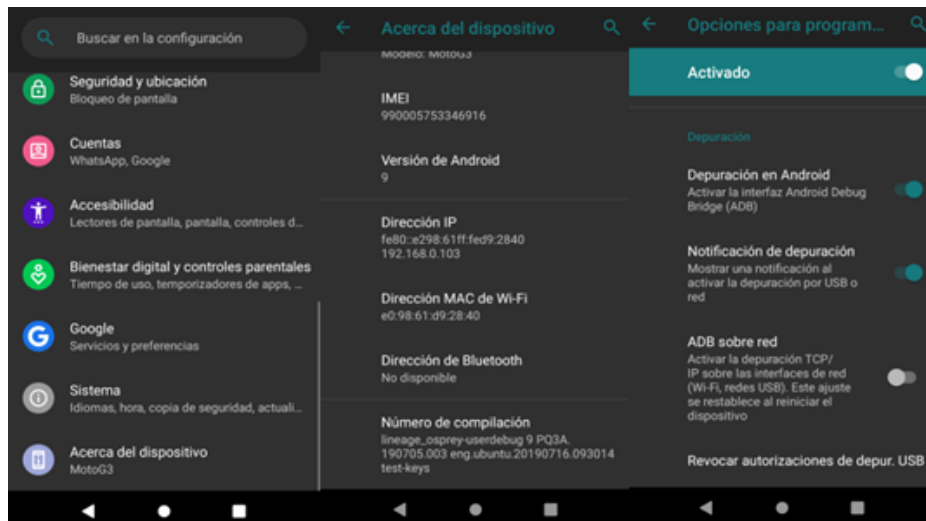


Figura 6.06: Activación de la depuración por USB en un dispositivo *Android*

Una vez activada la “Depuración por USB”, se debe conectar el dispositivo móvil a la computadora y en ese instante el *driver* del aplicativo ADB será instalado automáticamente por *Windows*.

Para verificar que la instalación se realizó correctamente es suficiente con acceder al administrador de dispositivos y comprobar que aparezca el árbol mostrado en la Figura 6.07:

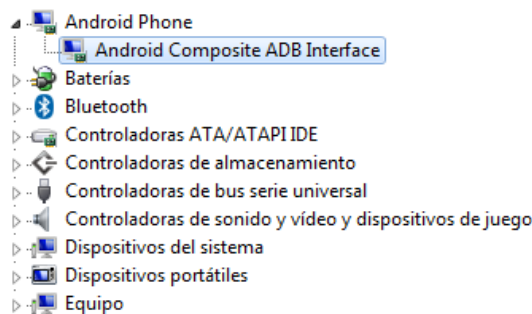


Figura 6.07: Resultado de la correcta instalación de los *drivers* de un dispositivo

Son muchos los casos en que el sistema *Windows* no dispone del *driver* y muestra un error. En caso de que esto suceda, se solventa haciendo clic derecho sobre el ícono que muestra advertencia y seleccionar “Buscar automáticamente *software* de controlador actualizado”. Este procedimiento se puede observar en la Figura 6.08:

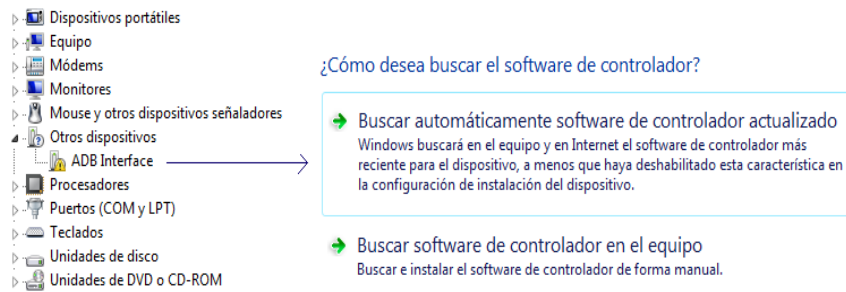


Figura 6.08: Resultado de la instalación fallida de un *driver* en *Windows*

En el peor de los casos, en el que *Windows* no acierte en la búsqueda del controlador, es posible realizar la descarga vía Internet de un *driver* universal. El paquete *Android SDK* y algunas otras herramientas forenses cuentan con los controladores más utilizados por los fabricantes, y en muchas ocasiones no funcionan con todos los modelos de dispositivos móviles.

Cuando el *driver* se instala correctamente, al conectar el equipo móvil al puerto USB, aparecerá una alerta de seguridad, que podría representar un obstáculo para continuar con la investigación. La alerta y su correspondiente información puede observarse en la Figura 6.09:

#### ¿Permitir depuración USB?

La depuración USB solo está indicada para actividades de desarrollo. Puedes utilizarla para intercambiar datos entre el ordenador y el dispositivo, para instalar aplicaciones en el dispositivo sin recibir notificaciones y para leer datos de registro.

CANCELAR ACEPTAR

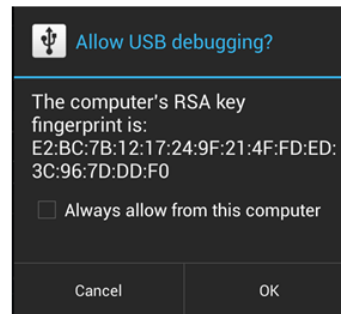


Figura 6.09: Pantalla para la habilitación de permisos de depuración USB

Luego de habilitar los permisos que autoricen la conexión, el sistema *Android* ejecutará el aplicativo *ADB Daemon* (ADB) en segundo plano y buscará una conexión USB. En el equipo de investigación forense (*host*) se debe ejecutar el cliente *adb.exe*, el cual comprobará en primera instancia si existe un servidor local que ya se esté ejecutando.

En caso de no ser así, se comienza un nuevo proceso de iniciación. El ADB *Daemon* y el servidor se comunican a través de los puertos 5555 a 5585. El cliente ADB se comunica con el servidor local a través del puerto 5037.

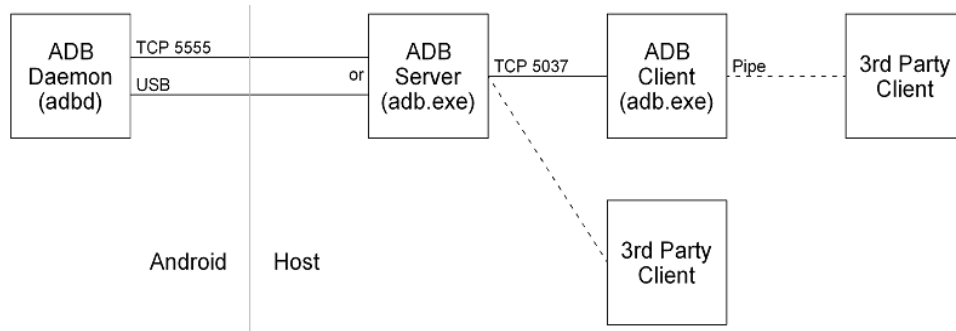


Figura 6.10: Proceso de comunicación del aplicativo ADB *Daemon* con el dispositivo en prueba

A continuación, se debe abrir una ventana de comandos cmd (*command*), tal como se muestra en la Figura 6.11, para dar inicio al proceso de exploración de archivos.

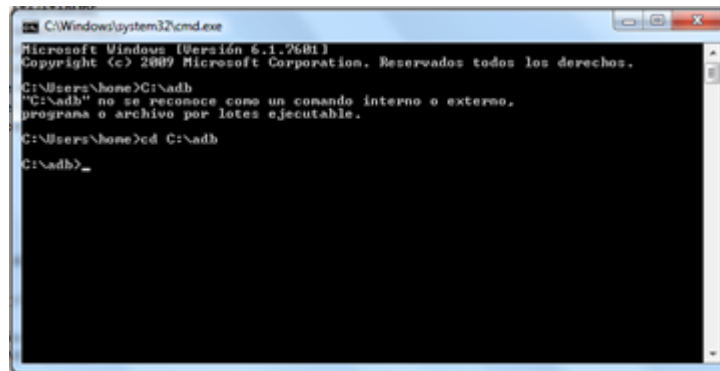


Figura 6.11: Activación de la pantalla CMD para inicio del intercambio de datos

Luego se ingresa el comando *adb devices* que permite saber si hay comunicación vía ADB entre los equipos.

**adb devices**



Si el resultado es exitoso, aparece la respuesta mostrada en la Figura 6.12 y se mostrará la siguiente información del dispositivo:



```
C:\Windows\system32\cmd.exe - adb shell
C:\adb>adb devices
List of devices attached
ZY22342SL8    device
```

Figura 6.12: Resultado exitoso de la aplicación del comando *devices*

Es posible que el servidor ADB no responda a un comando y deba ser reiniciado. Para detener los servicios de ADB se utiliza el siguiente comando:

**adb kill-server**

Mediante ADB se puede obtener un *shell* remoto, en el que se pueden ejecutar comandos internos del propio sistema operativo *Android*. Entonces se debe escribir:

**adb shell**

Después de ejecutar el comando anterior, se puede observar el símbolo de *shell* en la pantalla. Este símbolo aparecerá reflejado con los caracteres \$ o #. En sistemas *Linux*, el símbolo # hace referencia a que el usuario es *root*, mientras que el símbolo \$ indica que el usuario no es *root*.

Si aparece \$, se puede ejecutar el comando SU (superusuario) para así pasar a usuario *root*. Esta acción solo funcionará si el *root* se encuentra instalado en el dispositivo. Para un investigador forense es importante determinar si el dispositivo está "rootado" y saber cómo "rootearlo" a fin de poder extraer la mayor cantidad de datos contenida en el equipo.



```
C:\adb>adb shell
osprey:/ # ls -l
total 1826
```

Figura 6.13: Activación de la pantalla para utilizar el comando *shell*

Un ejemplo de un comando interno, puede ser:

**adb shell ls -l**

Con este comando se obtiene la lista de los archivos del sistema, tal como se puede observar en la Figura 6.14, para así poder ubicar aquellos que puedan ser relevantes para el caso investigado:

```
C:\adb>adb shell
ospreg:/ # ls -l
total 1826
drwxr-xr-x 104 root root      0 1970-05-17 21:13 acct
lrwxrwxrwx  1 root root      50 1969-12-31 20:00 bugreports -> /data/user_d
e/0/com.android.shell/files/bugreports
drwxrwx---  6 system cache 4096 1970-04-09 04:07 cache
lrwxrwxrwx  1 root root      13 1969-12-31 20:00 charger -> /sbin/charger
drwxr-xr-x  3 root root      0 1969-12-31 20:00 config
lrwxrwxrwx  1 root root      17 1969-12-31 20:00 d -> /sys/kernel/debug
drwxrwx--- 51 system system 4096 2018-12-04 23:13 data
-rw-----  1 root root     1641 1969-12-31 20:00 default.prop
drwxr-xr-x 18 root root     5160 2019-01-12 20:41 dev
lrwxrwxrwx  1 root root      11 1969-12-31 20:00 etc -> /system/etc
drwxr-xr-x  4 root root     4096 1969-12-31 20:00 firmware
drwxr-xr-x  2 root root     2048 1969-12-31 20:00 fsg
-rwxr-x---  1 root root    1067440 1969-12-31 20:00 init
-rwxr-x---  1 root root     1138 1969-12-31 20:00 init.environ.rc
-rwxr-x---  1 root root    28517 1969-12-31 20:00 init.rc
-rwxr-x---  1 root root     7874 1969-12-31 20:00 init.usb.configfs.rc
```

Figura 6.14: Ejemplo del contenido de archivos de un sistema típico

Un comando que resulta importante para la investigación forense es *ps* (*process status*):

**adb shell ps**

Este comando despliega una lista del estado (status) de los procesos del sistema y de las aplicaciones que se encuentran corriendo, tal como se muestra en la Figura 6.15:

Ejemplo de resultado:

```
C:\adb>adb shell ps
USER      PID  PPID  USZ  RSS  WCHAN  ADDR S NAME
root      4714 9685 13628 1580 0      aafe3a64 R ps
```

Figura 6.15: Ejemplo de la aplicación del comando *adb*

Otro comando importante en un caso de investigación es: *df* (*disk free*).

**adb shell df**

Este comando muestra información del espacio utilizado y libre que existe en el sistema. Un ejemplo de resultado se puede observar en la Figura 6.16:

```
C:\adb>adb shell df
Filesystem            1K-blocks    Used Available Use% Mounted on
tmpfs                 447868      704    447164   1% /dev
/dev/block/mmcblk0p40 2301196    917328  1383868  40% /system
tmpfs                 447868      0    447868   0% /mnt
/dev/block/mmcblk0p41 4765568   3710776  1054772  78% /data
/dev/block/mmcblk0p39 253928     168    253760   1% /cache
/dev/block/mmcblk0p23 2017       2015     2    100% /fsq
/dev/block/mmcblk0p1 36000     32192   3888    90% /firmware
/dev/block/mmcblk0p29 3952      300     3652    8% /persist
data/media           4765568   3710776  1054772  78% /mnt/runtime/default/emu1
ated
```

Figura 6.16: Uso del comando *df*

Luego de explorar los directorios y encontrar información que resulte relevante para el caso, se puede realizar la extracción mediante el comando *pull* de ADB, de la siguiente manera:

```
adb pull <remoto><local>
```

En el comando anterior, <remoto> hace referencia a la ruta en el dispositivo *Android* y <local> a la ruta en la que será almacenada la información en el equipo de investigación forense. Entonces se puede ejecutar la siguiente línea de comando:

```
adb pull /system/app/Calendar/Calendar.apk C:\Users\home\Desktop
```

Un ejemplo del resultado es el que puede observarse en la 6.17:

```
C:\adb>adb pull /system/app/Calendar/Calendar.apk C:\Users\home\Desktop
2175 KB/s (2334933 bytes in 1.048s)
C:\adb>_
```

Figura 6.17: Resultado de la aplicación del comando *pull*

Es importante saber dónde y cómo se almacenan los datos. Generalmente, todos los datos importantes relacionados con las aplicaciones instaladas residen en la carpeta */data/data* tal como se muestra en la Figura 6.18:

DATOS	RUTA DE UBICACIÓN
Contacts	/data/data/com.android.providers.contacts/
Calendar	/data/data/com.android.providers.calendar/
SMS & MMS	/data/data/com.android.providers.telephony/
Downloads	/data/data/com.android.providers.downloads/
Browser	/data/data/com.android.providers.browser/
Gmail	/data/data/com.google.android.providers.gmail/
Location	/data/data/com.google.android.location/

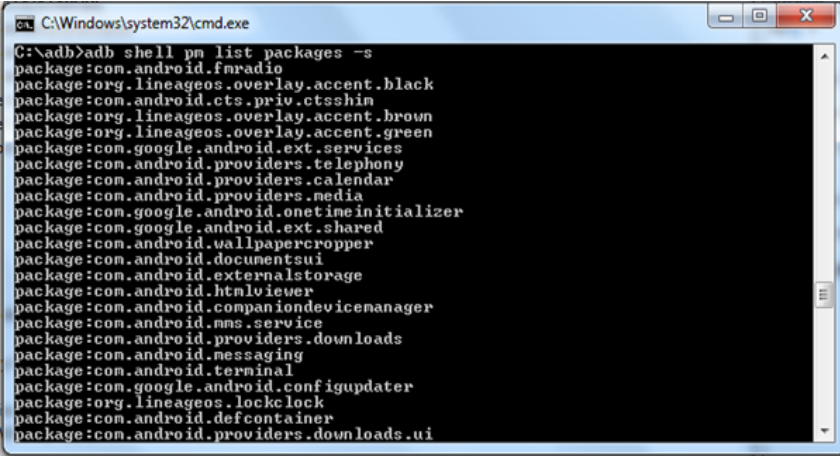
Figura 6.18: Ejemplo de la distribución de datos de un dispositivo

Sin embargo, normalmente no será posible realizar la descarga de estos archivos mediante el comando *pull* por las características de seguridad impuestas por el sistema operativo. En versiones más recientes de *Android* no es posible realizar la descarga aunque el dispositivo se encuentre “rooteado”. Esta situación conlleva a realizar una adquisición de forma física.

Para listar solo los paquetes instalados por terceros y realizar su evaluación se ejecuta el siguiente comando:

```
adb shell pm list packages -3
```

El resultado tras la ejecución puede observarse en la Figura 6.19:



```
C:\Windows\system32\cmd.exe
C:\>adb>adb shell pm list packages -s
package:com.android.fmradio
package:org.lineageos.overlay.accent.black
package:com.android.cts.priv.ctsshim
package:org.lineageos.overlay.accent.brown
package:org.lineageos.overlay.accent.green
package:com.google.android.ext.services
package:com.android.providers.telephony
package:com.android.providers.calendar
package:com.android.providers.media
package:com.google.android.onetimeinitializer
package:com.google.android.ext.shared
package:com.android.wallpapercropper
package:com.android.documentsui
package:com.android.externalstorage
package:com.android.htmlviewer
package:com.android.companiondevicemanager
package:com.android.mms.service
package:com.android.providers.downloads
package:com.android.messaging
package:com.android.terminal
package:com.google.android.configupdater
package:org.lineageos.lockclock
package:com.android.defcontainer
package:com.android.providers.downloads.ui
```

Figura 6.19: Ejemplo del listado de paquetes instalados por terceros

#### 6.1.4 Adquisición lógica de Datos mediante *MOBILedit Forensic Express PRO*

Para hacer uso de este popular *software*, lo primero es descargarlo directamente desde el sitio web <https://www.MOBILedit.com/>

Una vez iniciada la instalación, como puede observarse en la Figura 6.20, se abre la opción de descargar en *ClockworkMod*<sup>1</sup> los *drivers* de la mayoría de los dispositivos móviles del mercado; se recomienda hacerlo si la conexión al equipo se va a llevar a cabo vía USB. Sin embargo, *MOBILedit* también permite conexión por *Wi-Fi* y *Bluetooth*.

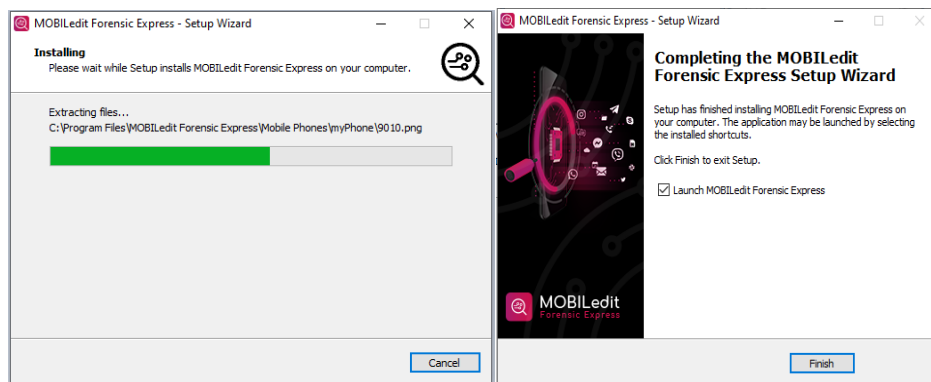


Figura 6.20: Proceso de instalación de la herramienta *MOBILedit*

Una vez descargado *MOBILedit Forensic Express*, se ejecuta el programa. Luego éste comenzará a buscar todos los dispositivos conectados por cable. Es importante que el USB *debugging* (depuración por USB) esté habilitado, tal como puede ser observado en la Figura 6.21:

---

<sup>1</sup> *ClockworkMod* es un *software* de la compañía Koushik "Koush" Dutta, la cual desarrolla varios productos para los *Smartphones* y *tablets* de *Android*. Es ampliamente conocida por los usuarios su servicio de recuperación personalizada de imagen.



Figura 6.21: Pantalla principal de la herramienta

Se selecciona el equipo y se hace clic para avanzar al siguiente paso.

Luego *MOBILedit* preguntará si se desea efectuar la adquisición de todos los datos. Se deberá instalar el conector de la aplicación en el equipo.

En esta parte se solicitarán todos los datos necesarios para comenzar la conexión interna entre el dispositivo y el *software*.

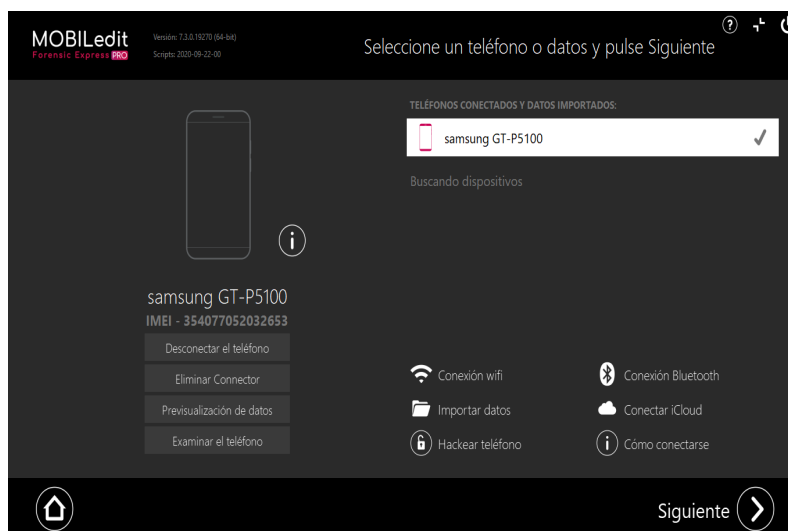


Figura 6.22: Selección del dispositivo a diagnosticar

En las Figuras 6.22 y 6.23 se puede observar el proceso de identificación de dispositivo y la petición de permisos para pre-visualizar los datos.

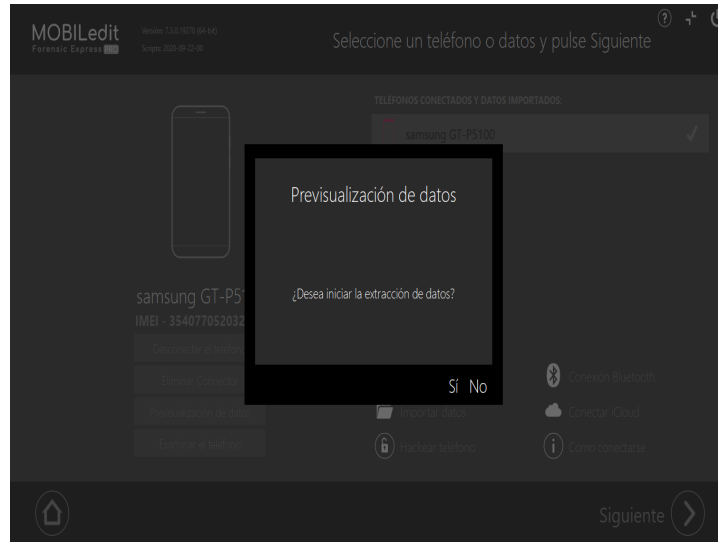


Figura 6.23: Solicitud de pre-visualización de datos

*MOBILedit* permite pre-visualizar los datos. Si se marca esta opción, se muestra un resumen de los datos encontrados en el teléfono y además se abrirá un panel de opciones sobre la información a la que se puede acceder. Allí se muestra el directorio telefónico, los mensajes, las llamadas y otros eventos, tal como muestra la Figura 6.24:

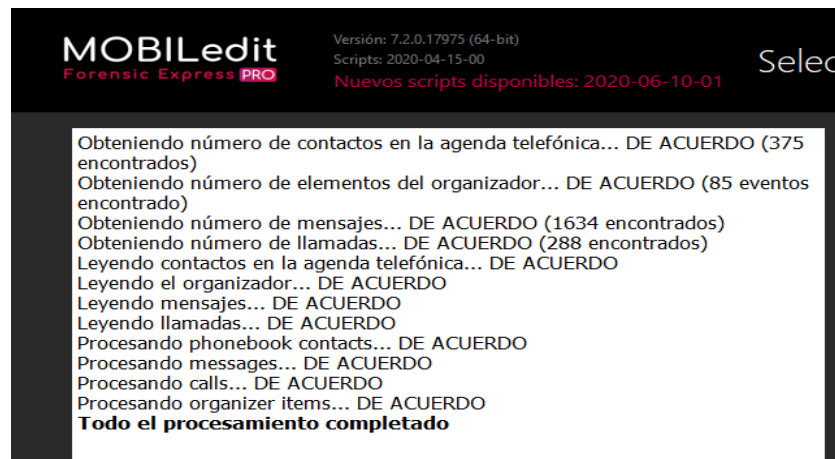


Figura 6.24: Obtención de la información contenida en el dispositivo

En la Figura 6.25 se pueden observar los datos del directorio telefónico.

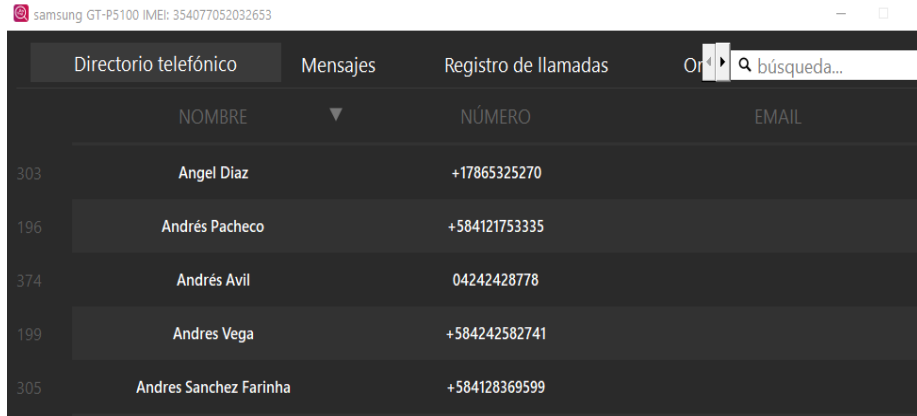


Figura 6.25: Ejemplo de como se muestra el directorio telefónico

En la Figura 6.26 se puede observar un ejemplo de la visualización de los mensajes SMS.



Figura 6.26: Ejemplo de la obtención de los datos de mensajes

En la Figura 6.27 se muestra un ejemplo de la visualización del registro de llamadas telefónicas.



	TIPO	NÚMERO	ETIQUETA	DURACIÓN	COMIENZO	FIN	ZONA HORARIA
20	Recibido	04142159430	Simone Bermudez	07:40	2019-02-22 12:07:58	2019-02-22 12:15:38	UTC-4
21	Recibido	04142159430	Simone Bermudez	01:10	2019-02-22 13:37:44	2019-02-22 13:38:54	UTC-4
26	Recibido	04241671434	Katherin Chacon	02:02	2019-02-26 12:07:45	2019-02-26 12:09:47	UTC-4
29	Recibido	04142159430	Simone Bermudez	01:17	2019-02-28 12:21:30	2019-02-28 12:22:47	UTC-4
38	Recibido	04169350041	Celestina Marquez	00:02	2019-03-04 19:31:27	2019-03-04 19:31:29	UTC-4

Figura 6.27: Ejemplo de la obtención del registro de llamadas

En la Figura 6.28 se puede observar el resultado de la visualización de la información de otros eventos.

Una vez que se cierra esta ventana y se marca “Terminar”, se vuelve al menú inicial. Allí se marca la opción “siguiente” para comenzar a recolectar la información del dispositivo. Luego se muestra un cuadro de diálogo donde se informa el estado del rooteo del teléfono, como se puede ver en la figura 6.29:

	TIPO	RESUMEN	DESCRIPCIÓN	COMIENZO	FIN	ZONA HORARIA
49	Evento	Vuelo a Venice (IB 3262)	<p>Este evento se ha creado a partir de un correo que recibiste en Gmail. <a href="https://mail.google.com/mail?extsrc=cal&amp;plid=A...cYdqIXuD2z7Cc">https://mail.google.com/mail?extsrc=cal&amp;plid=A...cYdqIXuD2z7Cc</a></p> <p>Si quieres ver información detallada sobre los eventos creados automáticamente como este, utiliza la aplicación oficial de Google Calendar. <a href="https://g.co/calendar">https://g.co/calendar</a></p>	2018-08-10 06:20:00	2018-08-10 08:45:00	UTC-4
50	Evento	Vuelo a Madrid (IB 3249)	<p>Este evento se ha...</p> <p>Si quieres ver información detallada sobre los eventos creados automáticamente como este, utiliza la aplicación oficial de Google Calendar. <a href="https://g.co/calendar">https://g.co/calendar</a></p>	2018-08-23 01:55:00	2018-08-23 04:35:00	UTC-4

Figura 6.28: Obtención de la información de otros eventos

Es importante tener claro que es necesario el rooteo si el propósito es obtener el máximo de información, incluyendo aplicaciones y datos eliminados como, por ejemplo, *WhatsApp* o mensajes *Facebook*.



Figura 6.29: Pantalla donde se indica que el dispositivo móvil no es *root*

Para la selección específica de los datos a recopilar, se puede elegir entre: todo el contenido, análisis de aplicaciones, sólo datos eliminados, sólo información del dispositivo o *parental check* (una opción optimizada para que los padres puedan extraer información del teléfono de los hijos). Esto se elige de acuerdo al propósito del caso.

Para fines prácticos, se selecciona todos los datos, y se marca “siguiente”. Si se requiere hacer una selección específica, allí se puede hacer la configuración del reporte y elegir los ítems que sean de interés para la investigación, tal como muestra la Figura 6.30:



Figura 6.30: Ejemplo de cómo seleccionar la data a extraer

Luego de hacer la selección e ir al siguiente paso, se llenan los espacios con los detalles del caso, tal como se muestra en la Figura 6.31:

AJUSTES DEL INFORME:	
Zona horaria:	Zona horaria del equipo (America/K ▼)
Idioma:	español de España ▼
Formato de hora:	ISO (yyyy-MM-dd hh:mm:ss) ▼
Mostrar fuentes de datos:	<input checked="" type="radio"/> Sí <input type="radio"/> No
Filtrado clutter:	<input type="radio"/> Sí <input checked="" type="radio"/> No

DETALLES DEL CASO:	
Etiqueta:	Dispositivo de prueba 2
Número de prueba:	Prueba 2
Detalles:	
Notas:	
<input checked="" type="button" value="Borrar los detalles del caso"/>	

DETALLES DEL TELEFONO:	
Etiqueta:	Dispositivo de prueba 2
Nombre:	samsung GT-P5100
ID:	
Número de prueba:	2
Nombre del propietario:	Miriam Cedeño
Número de teléfono:	+584146873131
Notas:	

DETALLES DEL INVESTIGADOR:	
Nombre:	Simone Bermúdez
Designación:	Investigadora
Email:	simone.jbermudez@gmail.com
Número de teléfono:	+584142150430
Documento de permiso:	
Logo:	Ningún archivo seleccionado ...

Figura 6.31: Pantalla donde se especifican los detalles del informe solicitado

En el siguiente paso, Figura 6.32, se eligen los detalles sobre el formato del reporte y se genera el archivo para hacer la exportación.



Figura 6.32: Pantalla donde se seleccionan los detalles del formato del reporte

Se selecciona el nombre y la dirección del reporte, figura 6.33, y se espera a que se complete la exportación y el análisis de los datos.

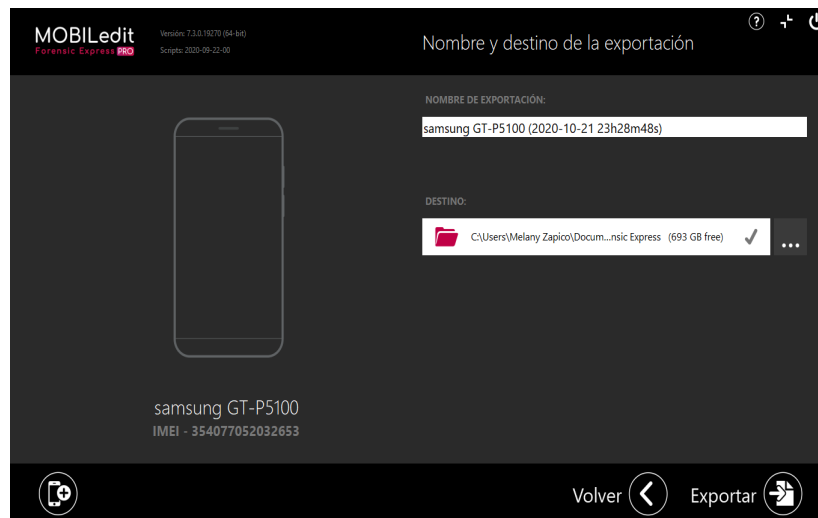


Figura 6.33: Pantalla indicativa del nombre y dirección del reporte

Una vez que esto se haya completado, se puede acceder a la carpeta del reporte y ver los resultados, ver Figura 6.34:

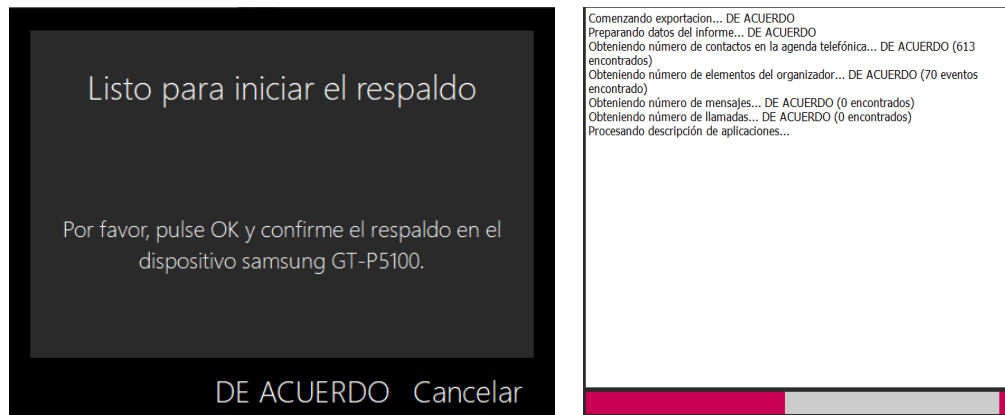


Figura 6.34: Pantalla indicativa de que comienza el respaldo de la información

### 6.1.5 Rooting de un equipo *Android*

Hacer *rooting* a un teléfono es una práctica que cada vez se ha vuelto más común y que consiste en romper las limitaciones que normalmente se tienen para los usuarios *Android*.

Ser usuario *root* en el sistema de *Android* es equivalente a ser un superusuario, por lo tanto, es tener acceso total y general del dispositivo en el que se habilitan ciertas opciones que se encuentran inaccesibles para los usuarios normales, es decir, se obtienen permisos que antes no se tenían para realizar modificaciones a las aplicaciones y al sistema.

Al ser usuario *root* se tienen muchos más permisos que en general no están disponibles para los usuarios. Sin embargo, esta práctica tiene sus riesgos y desventajas.

Existen muchas maneras para hacer el *rooting* de un dispositivo, pero para fines prácticos se hará uso de una herramienta bastante popular, *KingRoot*, la cual fue desarrollada por *KingRoot Studio*.

*KingRoot* es al igual que *KingoRoot* (desarrollada por *Kingsoft Technology Limited*), una de las herramientas más populares y fáciles de usar ya que evita hacer procesos que pongan en riesgo al dispositivo. Es un *software* que se encuentra en constante actualización, por lo que es compatible con una gran variedad de dispositivos.

Efectuar el proceso de rooteo es muy fácil con esta herramienta. Si se quiere rootear un equipo y éste ya estaba rooteado, la aplicación lo informará. Además, es posible realizar o eliminar de manera muy rápida el *root* cuando el usuario lo desee.

Con *KingRoot* es posible hacer un rooteo de los equipos *Android* en sólo segundos y es compatible con sistemas operativos *Android* que estén dentro de las actualizaciones *Android* 4.2.2 y 5.1. Por su fácil manejo y rapidez, está catalogada como una herramienta del tipo “*one click*”, que al español se traduce como “un sólo clic”.

Para comenzar, se realiza la descarga directa desde el sitio web oficial de *KingRoot* (<https://king-root.net/>), allí se bajará un ejecutable tipo .apk si la descarga se lleva a cabo desde un equipo móvil o como un ejecutable tipo .exe si es desde una computadora. La descarga realizada desde un dispositivo móvil se puede observar en la Figura 6.35:

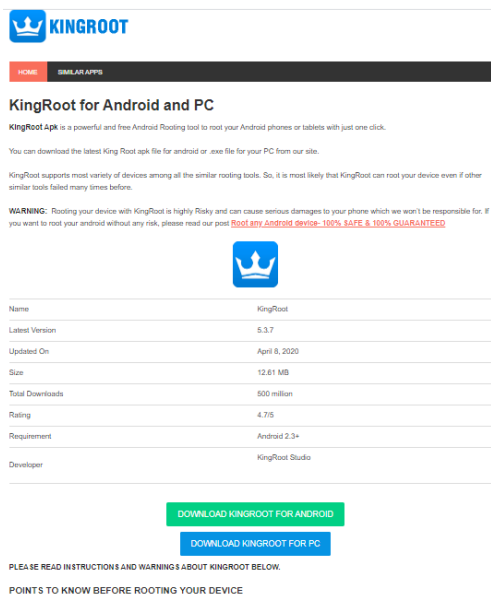


Figura 6.35: Pantalla principal de *KingRoot*

Si se realiza desde el dispositivo móvil, luego de la descarga del apk sólo se necesita correr *KingRoot*. Se mostrará en pantalla el tipo de equipo y se comenzará a evaluar el entorno para el *root*. Este proceso se puede observar en la Figura 6.36:



Figura 6.36: La herramienta *KingRoot* realizando la evaluación del equipo

Luego de que se culmina el paso anterior, se elige la opción “Optimizar” y se puede ver como se comienzan a conceder los permisos de superusuario, tal como se muestra en la Figura 6.37:

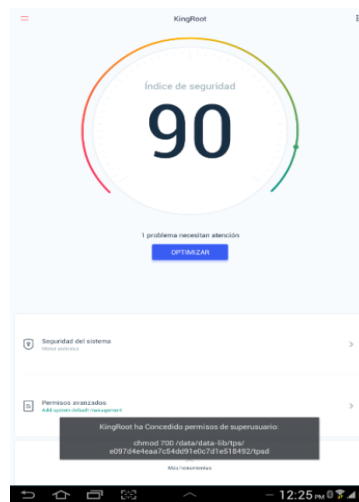


Figura 6.37: Pantalla indicativa de que se están concediendo los permisos de superusuario

Seguidamente se ubica el menú de *root*. Allí se mostrará al detalle la información del dispositivo y en la parte superior se mostrará la opción “Probar *Root*”, tal como se muestra en la Figura 6.38:

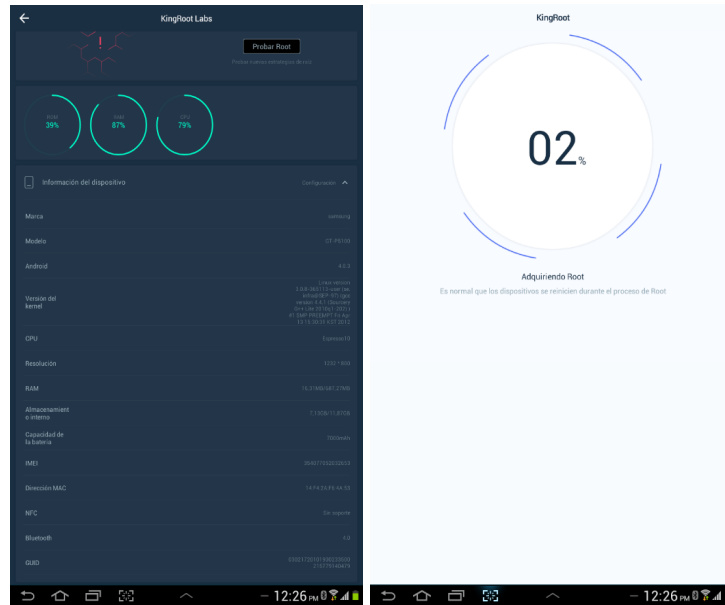


Figura 6.38: Pantalla indicativa del estado del dispositivo

Luego de que finalice el proceso de *rooting*, se mostrará el siguiente mensaje y se sabrá si el equipo se ha rooteado exitosamente.



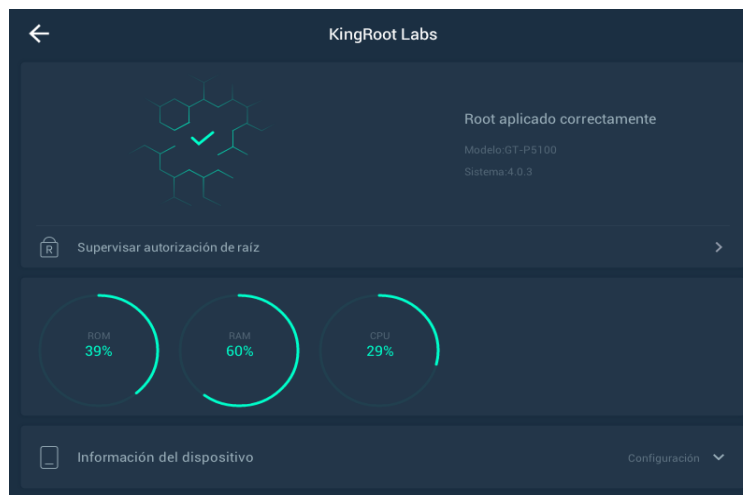


Figura 6.39: Pantalla indicativa que el *root* fue aplicado correctamente

### 6.1.6 Adquisición física de datos mediante *dd*.

Para un análisis forense más completo y detallado de un dispositivo móvil, la extracción física es el método más idóneo, ya que consiste en obtener una copia bit a bit del espacio asignado y no asignado que se almacena en la memoria física del equipo. Su mayor ventaja es que permite encontrar archivos borrados (o sus restos).

La extracción física es la que presenta más obstáculos a la hora de realizarla, pues el dispositivo cuenta con protección contra la lectura arbitraria de la memoria. Muchas veces la forma de lograrlo es teniendo privilegios de *root*.

Para tener éxito con este método de extracción es necesario conocer el sistema de archivos y su funcionamiento interno. El *filesystem* en *Android* se divide en particiones denominadas *data*, *cache*, *boot*, *system*, *recovery*, etc. y que se asignan a elementos de bloque como `/dev/block/mmcblk0` o `/dev/block/mtdblk1`. Esta asignación varía según la marca, el modelo y el tipo de memoria:

Para entender la estructura de las particiones en el dispositivo, se requiere disponer del número y el nombre de los bloques en el mismo, información que se encuentra en la ruta `/proc/partitions`.

```
adb shell cat /proc/partitions
```

El resultado podría ser algo como lo mostrado en la Figura 6.40:

```
C:\Users\Usuario>
C:\Users\Usuario>adb shell cat /proc/partitions
major minor #blocks name
254      0    524288 zram0
179      0   7651328 mmcblk0
179      1    40832 mmcblk0p1
179      2     512 mmcblk0p2
179      3     128 mmcblk0p3
179      4    1100 mmcblk0p4
179      5     250 mmcblk0p5
179      6     560 mmcblk0p6
179      7     128 mmcblk0p7
179      8     512 mmcblk0p8
179      9     512 mmcblk0p9
179     10    3516 mmcblk0p10
179     11    1100 mmcblk0p11
179     12     250 mmcblk0p12
179     13     560 mmcblk0p13
179     14     128 mmcblk0p14
179     15     512 mmcblk0p15
179     16    2048 mmcblk0p16
179     17     512 mmcblk0p17
179     17     512 mmcblk0p17
179     18    2236 mmcblk0p18
179     19    1536 mmcblk0p19
179     20    1536 mmcblk0p20
179     21     488 mmcblk0p21
179     22      32 mmcblk0p22
179     23    3072 mmcblk0p23
179     24      1 mmcblk0p24
179     25     128 mmcblk0p25
179     26     512 mmcblk0p26
179     27    4096 mmcblk0p27
179     28    4096 mmcblk0p28
179     29    8192 mmcblk0p29
179     30    8192 mmcblk0p30
179     31   16384 mmcblk0p31
259      0   16484 mmcblk0p32
259      1      8 mmcblk0p33
259      2    8696 mmcblk0p34
259      3    8192 mmcblk0p35
259      4    8192 mmcblk0p36
259      5   32768 mmcblk0p37
259      6   32768 mmcblk0p38
259      7  262144 mmcblk0p39
259      8  2375680 mmcblk0p40
259      9  4767616 mmcblk0p41
179     32    2048 mmcblk0rpb
179     64  7761920 mmcblk1
179     65  7757824 mmcblk1p1
```

Figura 6.40: Particiones típicas de un dispositivo móvil

En el ejemplo anterior, mmcblk0 corresponde a la memoria interna de 8 GB, mientras que mmcblk1 corresponde a la memoria externa SD de 8GB.

Otro comando útil es *df*, el cual arroja la información del espacio utilizado y libre en el sistema:

```
adb shell df
```

Y el ejemplo del resultado puede observarse en la Figura 6.41:

```
dd: /sdcardfs/blk39.dd: No such file or directory
|josprey_cdma:/ # df
Filesystem            1K-blocks    Used Available Use% Mounted on
tmpfs                 447612      644   446968    1% /dev
tmpfs                 447612        0   447612    0% /mnt
/dev/block/mmcblk0p40 2338316 1310216  1028100   57% /system
/dev/block/mmcblk0p39 253920     208   253712    1% /cache
/dev/block/mmcblk0p23  2017      2015      2 100% /fsg
/dev/block/mmcblk0p1  36080     32192   3888    90% /firmware
/dev/block/mmcblk0p29  3952       312    3640     8% /persist
/dev/block/mmcblk0p41 4765568 2700584 2064984   57% /data
/data/media           4765568 2700584 2064984   57% /mnt/runtime/default/emulated
/dev/block/vold/public:179,65 7753728 185984 7567744    3% /mnt/media_rw/3137-6135
/mnt/media_rw/3137-6135 7753728 185984 7567744    3% /mnt/runtime/default/3137-6135
josprey_cdma:/ #
```

Figura 6.41: Pantalla que muestra la utilización del espacio de memoria dentro del dispositivo

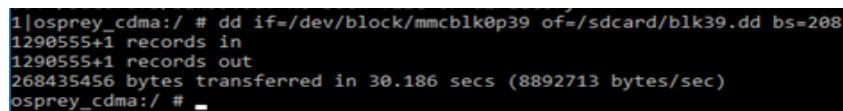
Luego de realizar la revisión de los directorios del dispositivo, se procede a la extracción física mediante *dd* (*dataset definition*). Esta herramienta permite convertir y copiar archivos, pero se utiliza con frecuencia para crear imágenes de particiones o

de unidades enteras. Como *dd* está incluido en las distribuciones basadas en *Linux*, generalmente suele estar incluido en plataformas *Android*.

Para utilizar *dd* con el fin de volcar una partición del almacenamiento del equipo, se debe ejecutar un comando como el siguiente desde el usuario *root*:

```
dd if=/dev/block/mtdblock39 of=/sdcard/blk39.dd bs=208
```

De la aplicación de dicho comando se obtiene el resultado mostrado en la Figura 6.42:



```
1|osprey_cdma:/ # dd if=/dev/block/mmcblk0p39 of=/sdcard/blk39.dd bs=208
1290555+1 records in
1290555+1 records out
268435456 bytes transferred in 30.186 secs (8892713 bytes/sec)
osprey_cdma:/ #
```

Figura 6.42: Pantalla que muestra el resultado de copia de una partición

Ese comando, de resultar exitoso, realiza una copia de una partición entera y la almacena en la tarjeta SD externa, por lo que no es tan práctico. Una mejor solución es copiar la partición a la computadora utilizando *Netcat* o *nc*, una herramienta para redes que posee muchas funcionalidades de comunicación.

*Netcat* no es una aplicación que se encuentre preinstalada en el sistema *Android*, pero forma parte de *BusyBox*, un popular aplicativo que contiene un conjunto de comandos del sistema *Linux* que por lo general se instala automáticamente al rootear un equipo *Android* o se puede instalar independientemente, tras la descarga desde *Google Play* o como un APK desde una página de confianza.

*Netcat* se suele utilizar para transferir archivos abriendo un canal inverso de comunicación mediante *sockets*. Para tal fin se coloca un *Netcat* para enviar el archivo desde un puerto TCP y otro *Netcat* en escucha en ese mismo puerto para recibir el archivo. El procedimiento es el siguiente:

Luego de descargar *Netcat* para *Windows* (*nc.exe* o *ncat.exe*), este archivo se coloca en la misma carpeta donde se encuentra *adb.exe*.

Seguidamente se realiza la evaluación de las particiones y se ubica el bloque a transferir. En este ejemplo será el que corresponde a la caché, señalado como `mmcblk0p39`.

```

/dev/block/mmcblk0p40      2338316 1310216 1028100 57% /system
/dev/block/mmcblk0p39      253920  208    253712  1% /cache
/dev/block/mmcblk0p23      2017    2015    2    100% /fsg
/dev/block/mmcblk0p1       36000   32192   3888   90% /firmware
/dev/block/mmcblk0p29      3952    312     3640   8% /persist
/dev/block/mmcblk0p41     4765568 2700584 2064984 57% /data

```

Figura 6.43: Ubicación del bloque de datos a transferir `mmcblk0p39`

Es posible que el comando no funcione por ser una versión antigua del sistema *Android*. Pero si afortunadamente no hay problemas, se debe ejecutar el siguiente comando y el resultado sería el mostrado en la Figura 6.44:

```
netcat 127.0.0.1 9999 > blk39.dd
```

```
C:\Users\Usuario\Desktop\Forensica>NetCat 127.0.0.1 9999 > blk39.dd
```

Figura 6.44: Pantalla que muestra el volcado con el comando *Netcat*

Las ventanas se congelarán y no se permitirán más comandos porque están ocupadas transfiriendo datos, lo cual puede tomar su tiempo, dependiendo del tamaño del archivo a transferir. Si el tamaño del archivo `dd` está aumentando en la carpeta donde se está guardando la imagen, significa que se está efectuando la transferencia con éxito. Al finalizar, volverá al símbolo del sistema y se mostrará información sobre la transferencia.

En la Figura 6.45, se puede observar un resultado típico:

xprueba	16/10/2020 10:23 p. m.	Carpeta de archivos	
blk39.dd	1/2/2020 12:58 p. m.	Archivo DD	262.144 KB

Figura 6.45: Resultados del proceso de transferencia

## 6.2 Análisis de datos.

En el proceso de análisis de una imagen del sistema operativo *Android*, que se llevará a cabo a continuación, se examinará la imagen obtenida en el proceso de adquisición física de datos mediante *dd*, utilizando la herramienta *Autopsy*, una aplicación gratuita que es la interfaz gráfica para *The Sleuth Kit* (TSK).

Una vez en *Autopsy*, aparecerá una ventana con tres opciones a elegir. Para crear un nuevo se elige la opción *Create New Case*, tal como se muestra en la Figura 6.46:



Figura 6.46: Pantalla principal de la herramienta *Autopsy*

Se introduce la información sobre el caso, tal como se señala en la Figura 6.47. Los resultados serán guardados en una carpeta en el *Base Directory*.

**Case Information**

Case Name: [Revisión de Memoria Cache]

Base Directory: [D:\Forense en Móviles\Evidencia\] [Browse]

Case Type:  Single-user  Multi-user

Case data will be stored in the following directory: [D:\Forense en Móviles\Evidencia\Revisión de Memoria Cache]

< Back Next > Finish Cancel Help

**Optional Information**

Case

Number: [001]

Examiner

Name: [Minam]

Phone: [04126873131]

Email: [xurmar@gmail.com]

Notes: [ ]

Organization

Organization analysis is being done for: [ ] [Manage Organizations]

< Back Next > Finish Cancel Help

Figura 6.47: Pantalla para la introducción de los datos del caso

Seguidamente se debe seleccionar la fuente de datos, como se muestra en la Figura 6.48:

Revision de Memoria Cache - Autopsy 4.15.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline File Discovery Generate Report Close Keyword Lists Keyword Search

**Add Data Source**

**Steps**

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

**Select Data Source**

Path: [D:\Forense en Móviles\Evidencia\001\01.dd] [Browse]

Ignore orphan files in FAT file systems

Time zone: [(GMT-4:00) America/Caracas]

Sector size: [Auto Detect]

Figura 6.48: Pantalla para la selección de la fuente de datos

Se selecciona la zona horaria que corresponda al caso, ya que así se establecen correctamente los tiempos en que ocurrieron los hechos que se están analizando.

El siguiente paso es seleccionar los *Ingest Modules*, estos son los módulos que serán procesados tal y como se muestra en la Figura 6.49:

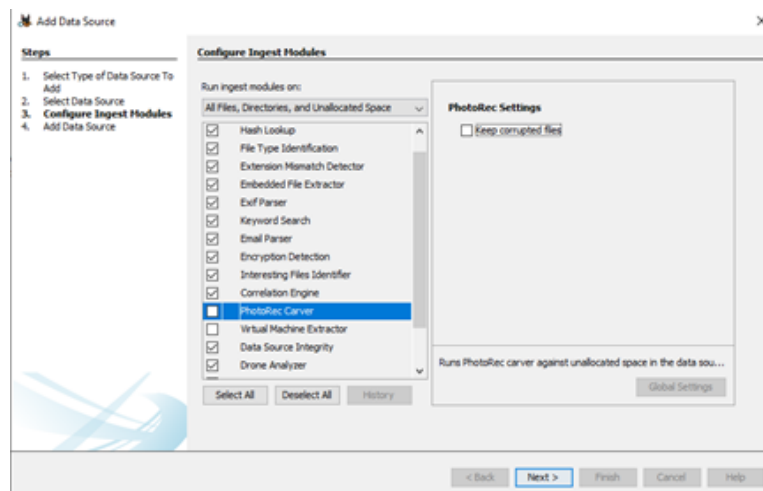


Figura 6.49: Selección de los módulos a procesar

Una vez añadida la fuente de datos, se pulsa *Finish* y *Autopsy* pasará de una vez al análisis.

Los resultados se extraerán e irán apareciendo paulatinamente en la vista del árbol que se encuentra a la izquierda. En la barra inferior se muestra el porcentaje de avance, (ver Figura 6.50) y es un proceso que puede llevar tiempo en completarse.



Figura 6.50: Muestra del avance del proceso de análisis

Al finalizar la carga de la evidencia, se mostrará la interfaz de *Autopsy*, en la que se podrá examinar de manera exhaustiva la información contenida en la imagen procesada (ver Figura 51).

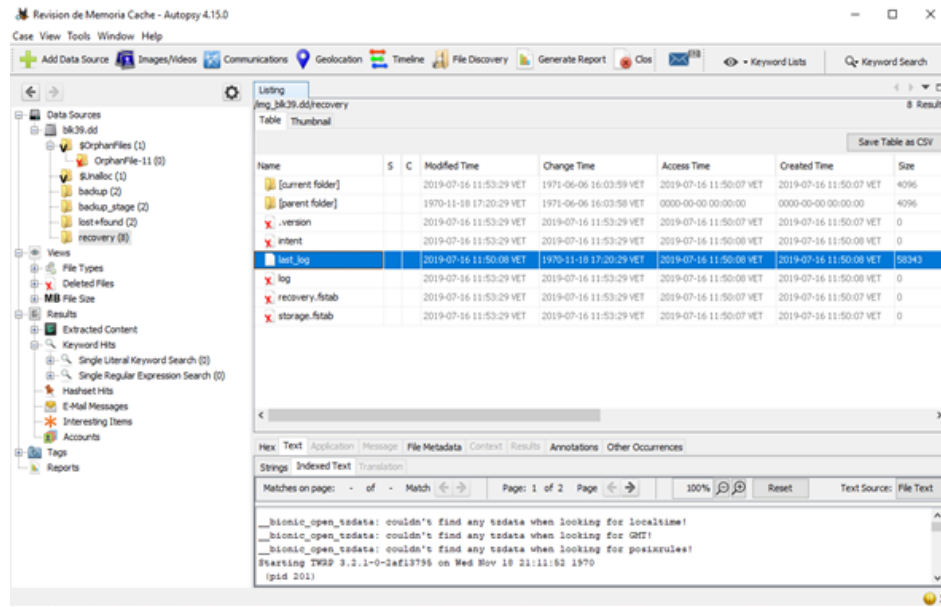


Figura 6.51: Pantalla que muestra los resultados del proceso de análisis de la imagen

Dado que la imagen analizada en este ejemplo no presenta información relevante que pueda ser considerada como evidencia para este ejemplo, se realizará el examen de otra imagen la cual sí posee información sustancial para el caso, tal como se muestra en la Figura 6.52:



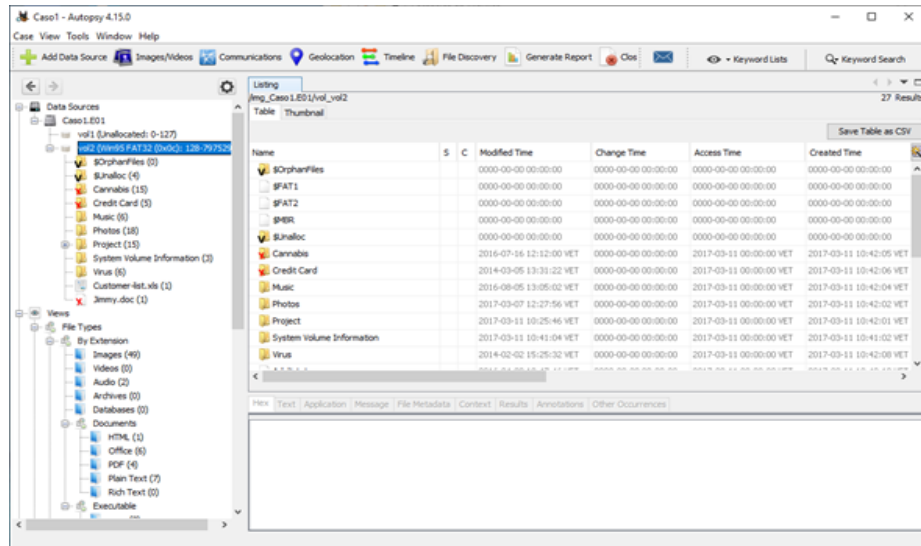


Figura 6.52: Muestra del árbol de directorios de una partición con datos para el análisis

Luego de que *Autopsy* reconoce la imagen cargada, se mostrará un árbol de directorios, en el que se podrá navegar por los distintos archivos que componen la evidencia, tal como muestra la Figura 6.53:

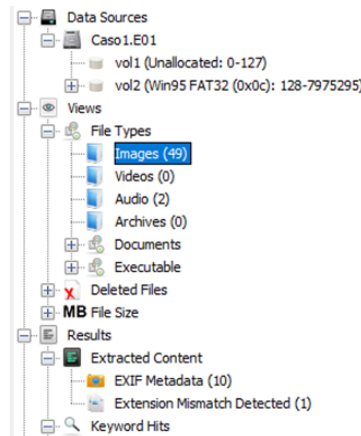


Figura 6.53: Ejemplo de árbol de directorios obtenido con *Autopsy*

En la sección *Data Source* se muestran los archivos del sistema. En este módulo es posible visualizar los archivos y carpetas eliminados, que fueron recuperados

directamente del sistema de archivos (*file system*). Este resultado puede visualizarse en la Figura 6.54.

En la sección *Views* se agrupan los archivos por categorías, con el fin de poder identificar rápida y fácilmente las imágenes, audio o documentos presentes en el sistema de archivos, según su extensión.

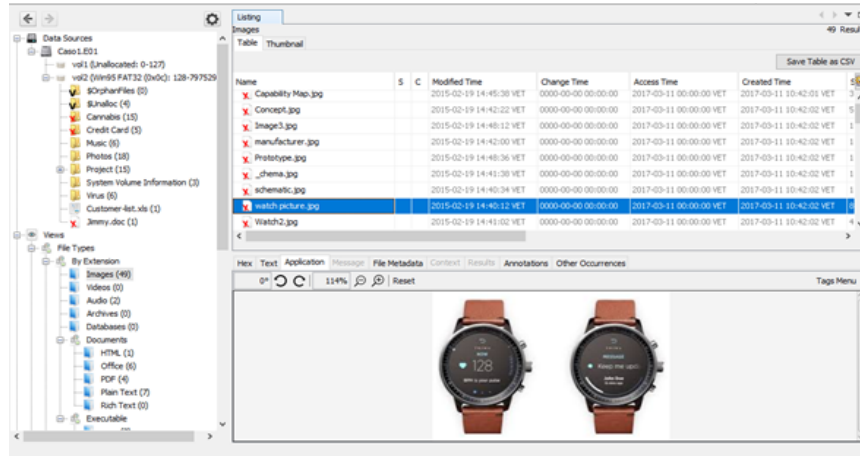


Figura 6.54: Pantalla que muestra la visualización con la opción *Views*.

En la sección *Results*, pantalla de la Figura 6.55, se encuentran los resultados obtenidos tras el uso de complementos para *Autopsy* que optimizan el análisis de la evidencia. Estos complementos agregan nuevas características a la aplicación para facilitar el manejo de la evidencia.

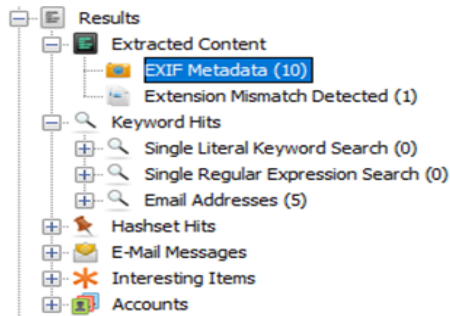


Figura 6.55: Pantalla que muestra los resultados de la aplicación complementos del *software*

Además de poder visualizar los resultados obtenidos en el árbol de directorios, en la ventana principal de *Autopsy* aparecen una sección que permite la examinación de la evidencia con más detalles:

La opción *Listing*, Figura 6.56, muestra los archivos relevantes según el complemento instalado para el estudio del caso y muestra con detalles los datos encontrados.

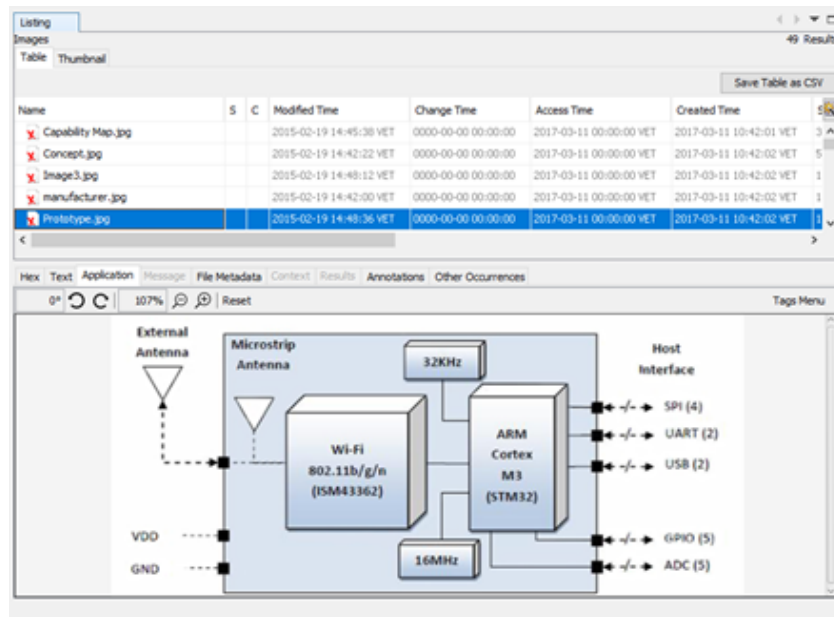


Figura 6.56: Pantalla con los resultados de la opción *Listing*

Es importante mencionar que los resultados obtenidos pueden ser exportados en formato HTML, entre otros disponibles, para que sea posible acceder desde cualquier otro equipo que no cuente con *Autopsy* a la información encontrada.

### 6.3 Detección de spyware

Un *spyware* es un tipo de *software* malicioso que recopila distintos tipos de datos alojados en un dispositivo y los envía a un tercero sin consentimiento del usuario.

### 6.3.1 *Free Android Spy*

*Free Android Spy* es una herramienta de monitoreo gratuita e invisible que permite espiar a celulares y tabletas *Android*.

Una vez que se instala esta aplicación en un dispositivo, es posible hacer seguimiento del registro de llamadas, las locaciones, espiar en los mensajes de texto, en la galería de fotos y vídeos, aplicaciones instaladas, entre otras opciones. Para las opciones más sofisticadas, como registro de mensajes de *WhatsApp*, *Snapchat* u otras aplicaciones, es necesario realizar un pago. Sin embargo, la opción gratuita brinda información bastante amplia y detallada del dispositivo y sus datos.

### 6.3.2 Proceso de descarga y uso

Antes de iniciar la descarga es necesario apagar el *Scan* de seguridad de *Google Play Protect*, tal como se muestra en la Figura 6.57:

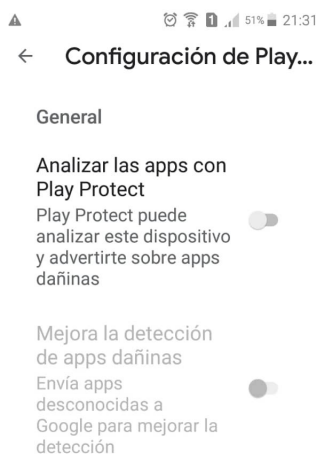


Figura 6.57: Desconexión del *Scan* de seguridad de *Google Play Protect*

Luego se habilitan los permisos para poder descargar aplicaciones de orígenes desconocidos, tal como se muestra en la Figura 6.58:

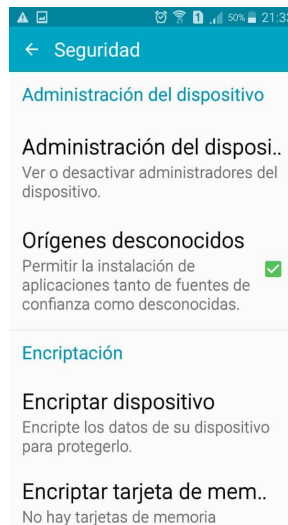


Figura 6.58: Habilitación de los permisos para instalar aplicaciones desconocidas

*Free Android Spy* se puede descargar de <http://www.spyssetup.com>. Una vez descargado el apk, se tendrá guardado un archivo con el nombre “*imusic.apk*” y éste es el archivo a ejecutar. Se trata de un archivo que tendrá acceso a toda la información del teléfono y además de orígenes desconocidos para el equipo, en caso de que haya algún antivirus, este enviará una notificación de alerta sobre el programa. Este proceso se puede visualizar en la Figura 6.59:

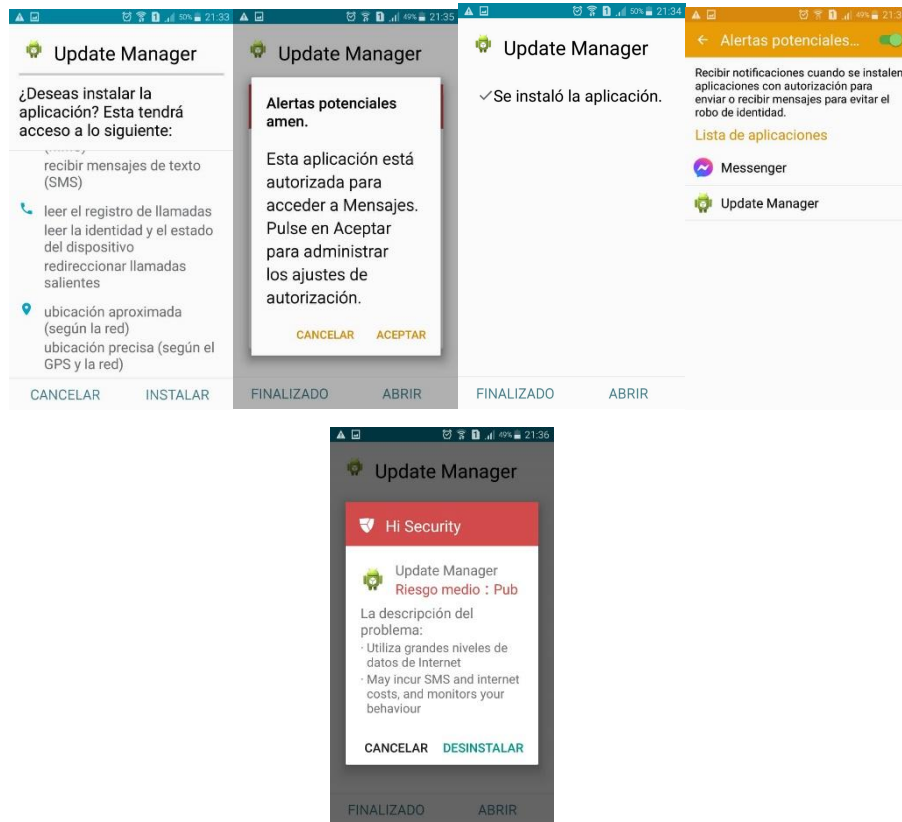


Figura 6.59: Proceso de instalación de *Free Android Spy*

Una vez finalizada la instalación en el dispositivo, se ingresa el correo al que luego se enviará una contraseña. Ver Figura 6.60:

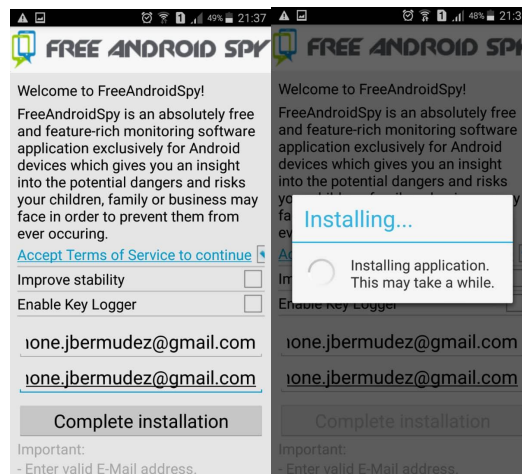


Figura 6.60: Instalación de la herramienta *Anti Spy*

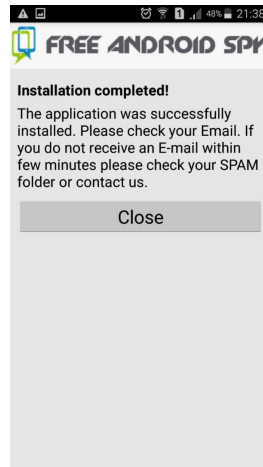


Figura 6.61: Pantalla que indica que la instalación se completó adecuadamente

Se chequea el *e-mail* para recibir la información de *login*. Ver Figura 6.62:

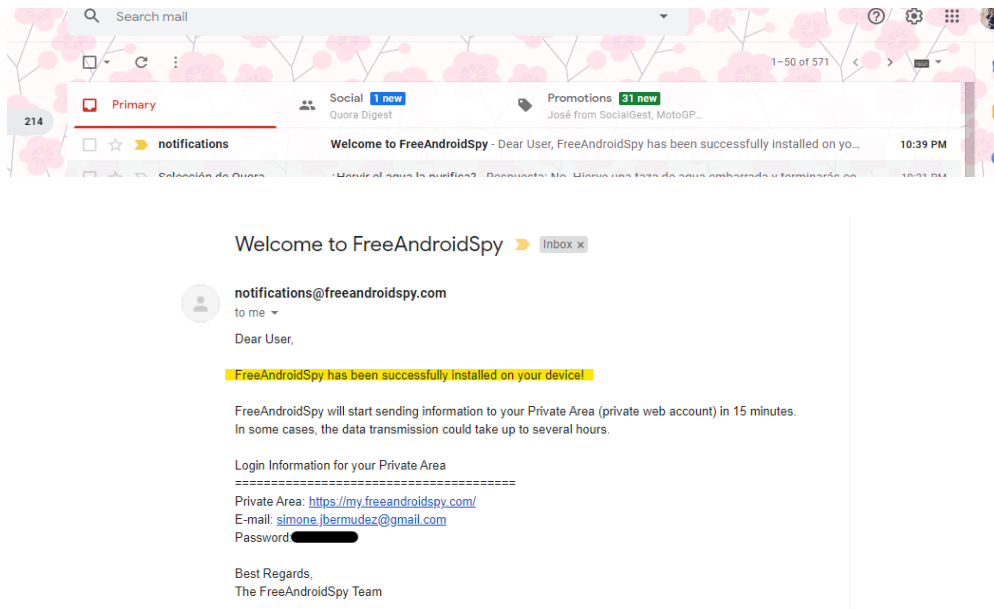


Figura 6.62: Recibiendo el *mail* con el *password* para operar la herramienta

Finalmente se abre el área privada y allí se requiere completar el *login* para comenzar a monitorear el equipo. Este proceso se muestra en la Figura 6.63:

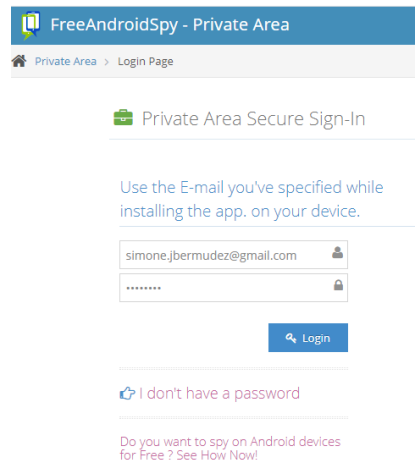


Figura 6.63: Accediendo al área privada de la herramienta

Una vez que se abre el área privada, es posible tener acceso a la información básica del equipo, tales como modelo del equipo, sistema operativo, memoria, espacio libre, IMEO, serial de la SIM, operadora y un pequeño resumen de las historias de llamadas, mensajes, agenda, recursos multimedia. Tal como se muestra en la Figura 6.64:



Figura 6.64: Pantalla que muestra la información del equipo en prueba

En las figuras 6.65, 6.66, 6.67, 6.68 y 6.69 se muestra el resultado de la información contenida en las diversas carpetas del dispositivo.



Type	Person	Number	Duration	At
[Incoming]	-	0414 [redacted]	3 min. 32 sec.	3h 30m ago
[Incoming]	-	0424 [redacted]	35 sec.	10h 46m ago
[Incoming]	-	0414 [redacted]	13 sec.	16 Oct 2020 18:45
[Incoming]	-	0414 [redacted]	0 sec.	16 Oct 2020 18:44
[Incoming]	-	0414 [redacted]	0 sec.	16 Oct 2020 18:44
[Incoming]	-	0424 [redacted]	1 min. 8 sec.	16 Oct 2020 18:19
[Incoming]	-	0414 [redacted]	44 sec.	16 Oct 2020 18:18
[Incoming]	-	0414 [redacted]	0 sec.	16 Oct 2020 18:11
[Incoming]	-	0424 [redacted]	0 sec.	16 Oct 2020 17:55
[Incoming]	-	+58414 [redacted]	5 min. 23 sec.	16 Oct 2020 17:46

Figura 6.65: Información de llamadas entrantes y salientes

Type	Person	To/From	Content	At
[Incoming]	-	0424 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:49
[Incoming]	-	0424 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:48
[Incoming]	-	0414 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:47
[Incoming]	-	0416 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:45
[Incoming]	-	0416 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:45
[Incoming]	-	041 [redacted]	Muy buenos días, la reunión de las 3 pm se suspende hasta nuevo aviso. Gracias	20 Jan 2020 09:45
[Outgoing]	-	0414 [redacted]	Ok copiado muchas gracias	19 Jan 2020 16:38
[Outgoing]	-	0416 [redacted]	Ok, en cuenta. Buenas tardes	19 Jan 2020 16:20
[Incoming]	-	0414 [redacted]	Buenas tardes [redacted]	19 Jan 2020 16:20
[Incoming]	-	0416 [redacted]	Buenas tardes [redacted]	19 Jan 2020 16:19

Figura 6.66: Detalle de la información de los mensajes de texto

Display name	Phone	calls	SMS
Corpoelec Ing Mantilla	[redacted]	N/A	N/A
Francisco Suarez	[redacted]	N/A	N/A
Alcides Colmenares	[redacted]	N/A	N/A
Seguridad Raul Medina	[redacted]	N/A	N/A
Ronald Marcella	[redacted]	N/A	N/A
Boris	[redacted]	N/A	N/A
Sra Ari	[redacted]	N/A	N/A
Maribic Gonzalez	[redacted]	N/A	N/A
Arturo Suarez	[redacted]	N/A	N/A
Patricia	[redacted]	N/A	N/A

Showing 31 to 40 of total 200 contacts

Figura 6.67: Detalle de la agenda de contactos del dispositivo

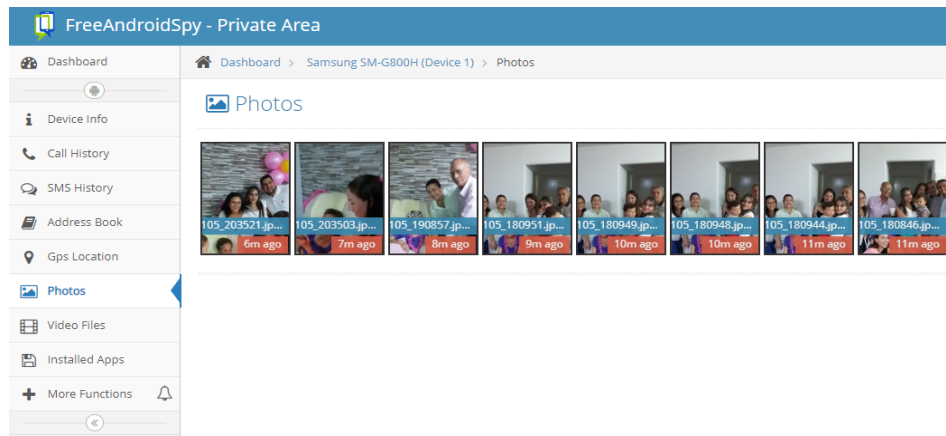


Figura 6.68: Muestra de las fotos contenidas en el dispositivo en prueba

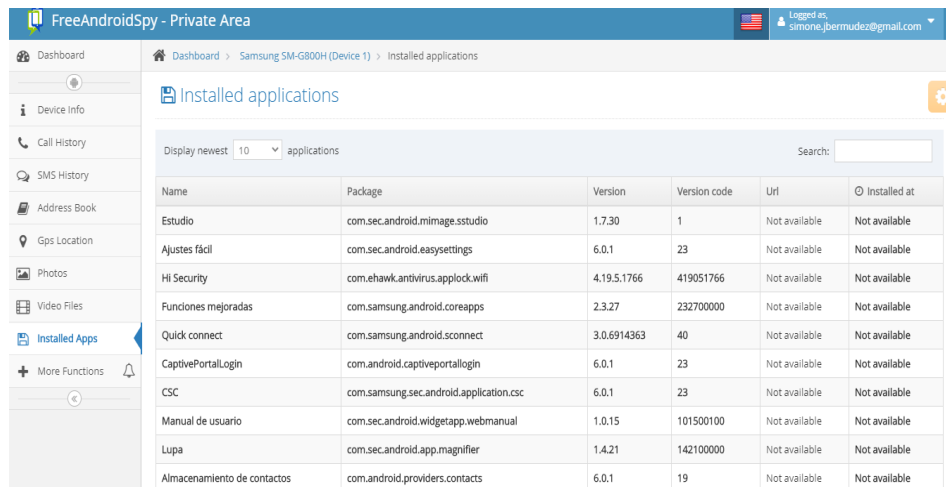


Figura 6.69: Reporte de las aplicaciones instaladas en el dispositivo

### 6.3.3 Detección y eliminación de un *spyware*

Detectar un *spyware* en un dispositivo no es tarea fácil. A diferencia de otros *softwares* maliciosos, éste es sigiloso, suele ocultarse y se ejecuta en segundo plano.

Sin embargo, existen varios indicios que pueden levantar la sospecha sobre un *spyware* dentro del dispositivo. Varias señales de *software* maliciosos son:

- Falta de memoria.
- Consumo de los datos.
- Ralentización del dispositivo.

- Pueden aparecer ventanas emergentes cuando no se está navegando en Internet.
- Aplicaciones o herramientas nuevas que no se han descargado.

Un recurso útil para descargar en caso de que se sospeche que existe un programa espía en el equipo, es *GlassWire*, un *software* gratuito disponible en *Play Store*, creado por *SecureMix LLC*. Permite descubrir aplicaciones que gasten datos sin el consentimiento del usuario. Es decir, con esta aplicación es muy fácil monitorear la red y ver el movimiento de la misma para detectar si hay alguna aplicación consumiendo datos de manera inesperada. En la Figura 6.70 se puede observar el resultado de un diagnóstico con esta herramienta.



Figura 6.70: Pantalla principal de *GlassWire*

En caso de descubrir un *spyware* en el dispositivo, existen varias maneras de eliminarlo, como se explica a continuación

#### 6.3.4 Desinstalación mediante *Google Protect*

Para equipos *Android* es posible visitar en *Google Play* la opción de *Play Protect* cuando se despliega el menú. Esta es una opción de *Google Play* que al activarse ayuda en la verificación de la seguridad de las apps descargadas en el dispositivo.

Analiza la actividad del dispositivo para detectar apps potencialmente dañinas de otras fuentes, conocidas como *software* malicioso, advierte sobre cualquier app potencialmente dañina que haya encontrado y la quita del dispositivo, envía alertas de privacidad acerca de las apps que pueden obtener permisos de los usuarios para acceder a información personal, lo que constituye un incumplimiento de la Política para Desarrolladores.

De esta manera se puede verificar si en el dispositivo hay un *spyware* descargado con esta herramienta. Para ello, basta con ir a *Google Play*, abrir el panel y seleccionar la opción de *Play Protect*, tal como se muestra en la Figura 6.71:

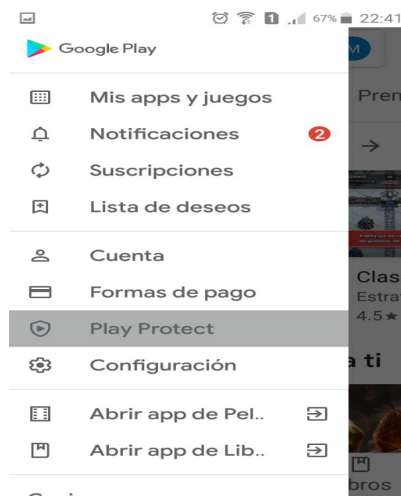


Figura 6.71: Ubicación de *Play Protect* en *Google Play*

Allí se puede verificar el estado del dispositivo y obtener mayor información. En caso de encontrarse alguna app que se considere potencialmente dañina, se mostrará un mensaje similar a este en el que se incluye el nombre de la app.

Finalmente, se puede eliminar el *spyware* con marcar la opción de “Desinstalar”, tal como se puede ver en la Figura 6.72:

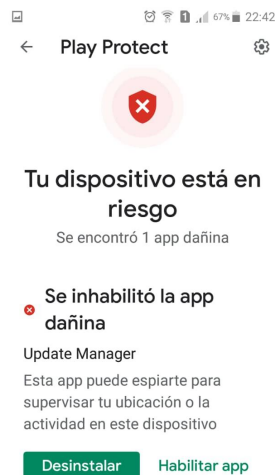


Figura 6.72: Pantalla de alarma en caso de detectar *spyware*

### 6.3.5 Desinstalación mediante aplicación *anti-spy*

Una segunda opción para detectar un *spyware*, es por medio de una aplicación alterna, un *software anti-spy*. En este caso, se realizará la experiencia con *Escáner Anti-spy y spyware*, la cual es una app creada por *Protectstar*, una empresa alemana fundada en 2004. Se puede visualizar en el *Play Store* en la Figura 6.73:



Figura 6.73: Escáner *Anti-Spy* en *Google Play*

*Escáner Anti-Spy y spyware* está disponible en *Play Store*, ambos en versiones gratuitas y pagas. En este caso, para hacer un pequeño escaneo del teléfono, es suficiente con la versión gratuita. El proceso de revisión y detección puede observarse en la Figura 6.74:

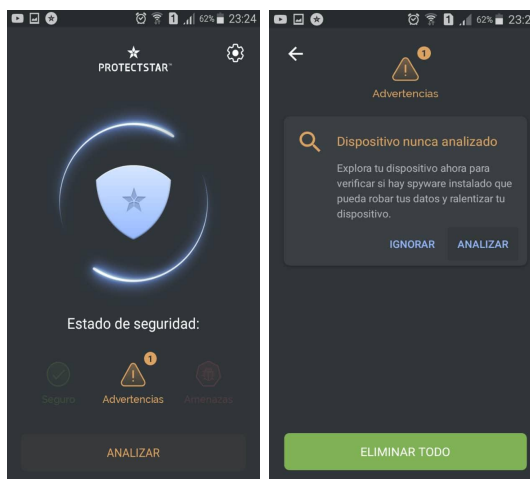


Figura 6.74: Proceso de análisis con *Escáner Anti-Spy y spyware*

Una vez completada la revisión del dispositivo, se mostrará en pantalla la cantidad de amenazas encontradas. Se puede ver que el *Free Android Spy* se encuentra oculto bajo el nombre de *Update Manager*, así que para eliminarlo del dispositivo basta con darle a la opción de eliminar, como se observa en la Figura 6.75:

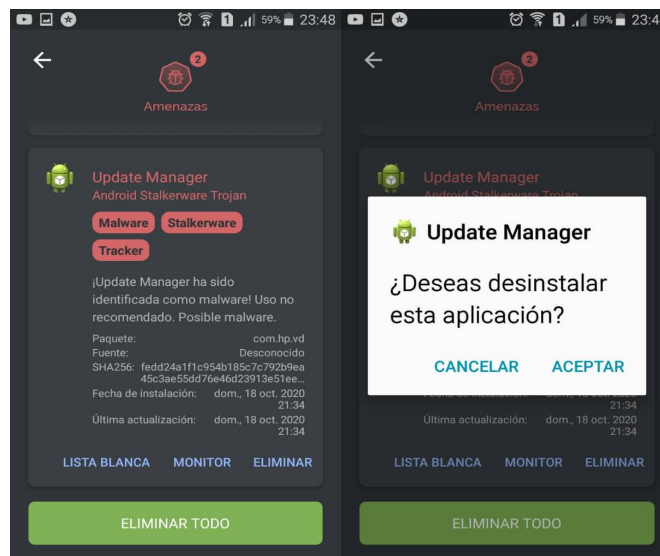


Figura 6.75: Proceso de detección y anulación de un programa malicioso

Al eliminarse con éxito el *spyware* del dispositivo, se rompe la comunicación desde el *Free Android Spy* y este ya no enviará más información al perfil.

Finalmente, en el perfil dentro del sitio web de *Free Android Spy*, saldrá reflejada la última conexión, junto con un mensaje que explica que el *software* ha sido desinstalado y que esto puede deberse a un bloqueo por el *Play Protect* o algún antivirus.

En el ejemplo se logra impedir el envío de datos de la aplicación *Free Android Spy*, tal como se observa en la Figura 6.76:

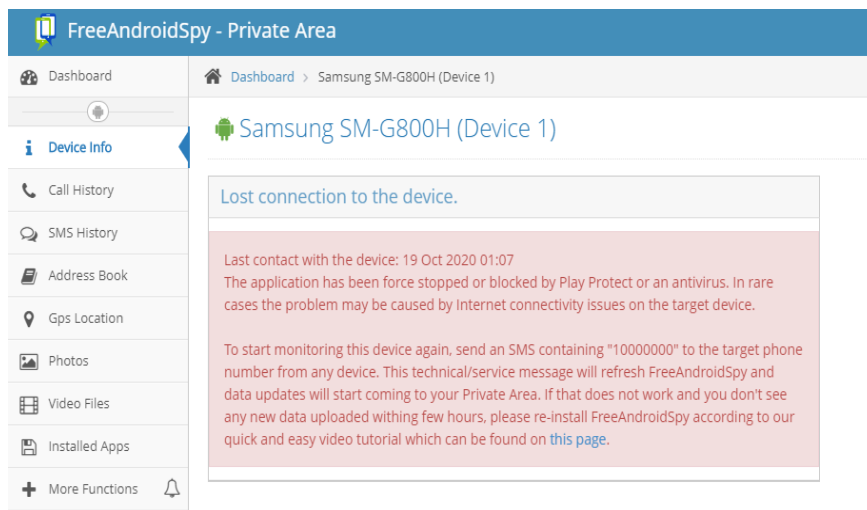


Figura 6.76: Pantalla de notificación de ruptura del envío de datos



## CAPÍTULO VII

### IMPLEMENTACIÓN Y DESARROLLO DE METODOLOGÍA

A continuación, se aplica la metodología propuesta en los capítulos anteriores, con el fin de mostrar la importancia y eficiencia que tiene cumplir con un procedimiento adecuado de análisis forense de datos.

#### 7.1 Descripción del caso práctico de prueba

El caso práctico de prueba para ejemplificar y simular la implementación y ejecución de la metodología para un procedimiento de análisis forense de datos de dispositivos móviles, es el siguiente:

*Una prestigiosa empresa dedicada a la comercialización de equipos tecnológicos, solicita la realización de una revisión exhaustiva a los dispositivos móviles entregados a su personal para uso laboral. Esta investigación es solicitada tras las constantes quejas de sus clientes por la falta de respuesta inmediata en la atención que brindan. Los dispositivos fueron entregados para el uso exclusivo de funciones relacionadas con la empresa. Finalmente, la empresa desea conocer qué tipo de información es manejada en el equipo celular que pueda estar interfiriendo en las actividades diarias de su personal.*

##### 7.1.1 Características del dispositivo

El dispositivo que se utilizará como objeto de pruebas en el siguiente caso práctico, tiene las siguientes especificaciones:

- Tableta *Samsung* con sistema operativo *Android*.
- *Android* versión 4.4.2.

##### 7.1.2 Descripción de herramientas

La herramienta a utilizar en la metodología de investigación forense propuesta y que se implementará en el caso práctico, en la etapa de adquisición y análisis de la evidencia, es la siguiente:

- ***MOBILedit! Forensic Express PRO***

La herramienta *MOBILedit! Forensic Express PRO* es una edición diseñada para los usuarios que buscan funciones avanzadas en el campo de la informática forense. Esta herramienta entra en el orden del tipo comercial y el precio del plan de pago depende de la edición. En este caso, se trabaja con una licencia de 30 días proporcionada por el agente autorizado de Compelson en Latinoamérica como apoyo a la investigación que se lleva a cabo y cuya utilización debe ser con fines exclusivamente académicos.

El precio de esta herramienta no se encuentra publicado de manera oficial en el sitio web de Compelson porque varía de acuerdo a los requerimientos del cliente y a esto se le suma que existe un tema de negociación, pero a lo sumo puede llegar a costar \$7000 la licencia con todos los requerimientos.

## **7.2 Implementación de la metodología**

### **7.2.1 Preparación e Identificación:**

A continuación, se recauda toda la información involucrada en la escena del suceso, para realizar la documentación de la misma.

Para la investigación que se está llevando a cabo, tomando en cuenta que es de índole académica y se presenta un escenario hipotético, las medidas de mayor rigor consideradas en la fase de preparación serán las siguientes:

- Resguardar de forma adecuada los dispositivos incautados que serán calificados como evidencia para el caso.
- Preservar la integridad de la información contenida en el dispositivo durante todo el proceso de identificación.

El resultado de esta etapa o fase se puede visualizar en la Tabla 1 que se muestra a continuación.

CONDICIONES DEL DISPOSITIVO MÓVIL				
ESTADO DEL DISPOSITIVO	ENCENDIDO	X	APAGADO	
PROTECCIÓN	SI	X	NO	
TIPO DE PROTECCIÓN DEL DISPOSITIVO				
CONTRASEÑA	N/A			
PIN	N/A			
PATRÓN	N/A			
HUELLA DACTILAR	N/A			
RECONOCIMIENTO FACIAL	N/A			
OTRO	DESLIZAR			
CARACTERÍSTICAS DEL DISPOSITIVO				
MARCA	SAMSUNG			
MODELO	GT-P5100			
NÚMERO TELEFÓNICO	0414-119-1205			
OPERADORA DE SERVICIO	MOVISTAR			
SERIAL IMEI	354077052032653			
ELEMENTOS DEL DISPOSITIVO				
MEMORIA EXTRAIBLE	SI		NO	
CARGADOR	SI		NO	
FACTURAS	SI		NO	
DISPOSITIVO				

Tabla 7.2 Condiciones de entrega del dispositivo en estudio.

En esta fase es necesario presentar una documentación del estado inicial de la escena y del dispositivo incautado, con el fin de llevar un registro de las actividades de identificación del suceso y su evidencia.

### 7.2.2 Adquisición de la evidencia

El proceso de adquisición de la evidencia lógica del caso de estudio se realizó utilizando la herramienta de análisis forense *MOBILedit! Forensic Express PRO*, de la siguiente manera:

Se ejecuta la aplicación de forma habitual seleccionando la opción “Comienzo” y se muestra la pantalla de la Figura 7.01:



Figura 7.01: Pantalla principal de la herramienta *MOBILedit*

Luego de conectar el dispositivo al equipo de análisis con el modo depuración por USB activo, se instala y se ejecuta de forma automática el *Android Forensic Connector*, este es una aplicación de *Android* que permite el acceso a los datos del teléfono desde el *software MOBILedit Forensic* tal como se muestra en la Figura 7.02:

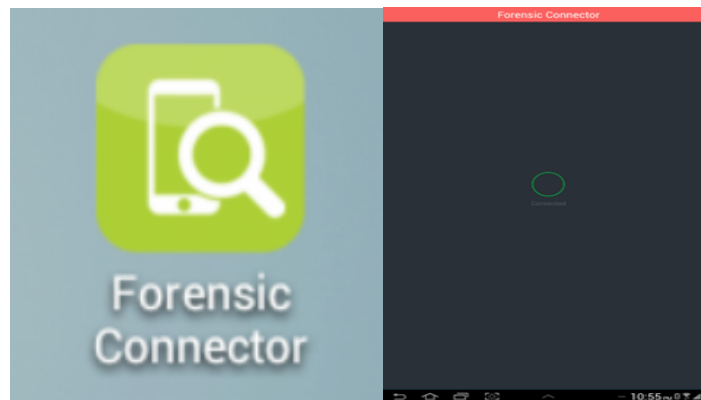


Figura 7.02: Pantalla de reconocimiento de dispositivo de *Forensic Connector*

En la Figura 7.03 se muestra como la herramienta informática muestra que reconoció el dispositivo en prueba.

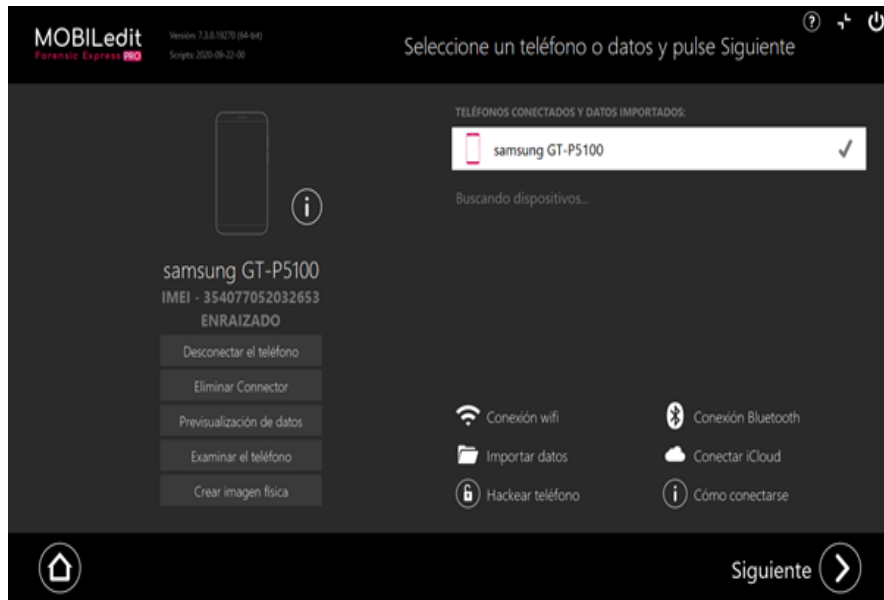


Figura 7.03: Pantalla donde *MOBILedit* reconoce el dispositivo conectado

Para continuar con la adquisición, se selecciona la opción Siguiente y se sabrá si el dispositivo se encuentra rooteado, tal como se muestra en la Figura 7.04:



Figura 7.04: Reconocimiento de que el dispositivo está rooteado

Luego se elige el análisis de aplicaciones, Figura 7.05, debido a que el principal interés en el estudio del caso es verificar si el empleado está haciendo uso del dispositivo para asuntos ajenos a la empresa.



Figura 7.05: Selección de análisis de aplicaciones

Se observa que hay aplicaciones de juegos y de redes sociales, Figura 7.06, lo cual representa una falta a las políticas de uso del dispositivo móvil perteneciente a la empresa. Se marca “Seleccionar todo” para así extraer las 201 aplicaciones disponibles en el dispositivo.



Figura 7.06: Selección de las aplicaciones que se extraerán del dispositivo

Luego se completan los detalles del informe, tal como se muestra en la Figura 7.07. Este dispositivo es el número 1 de la empresa y se encuentra asignado al gerente general.



Figura 7.07: Selección del formato de salida del informe final

Seguidamente se ajusta el formato de salida del informe final, como se muestra en la Figura 7.08 y se selecciona la opción “Siguiente”.

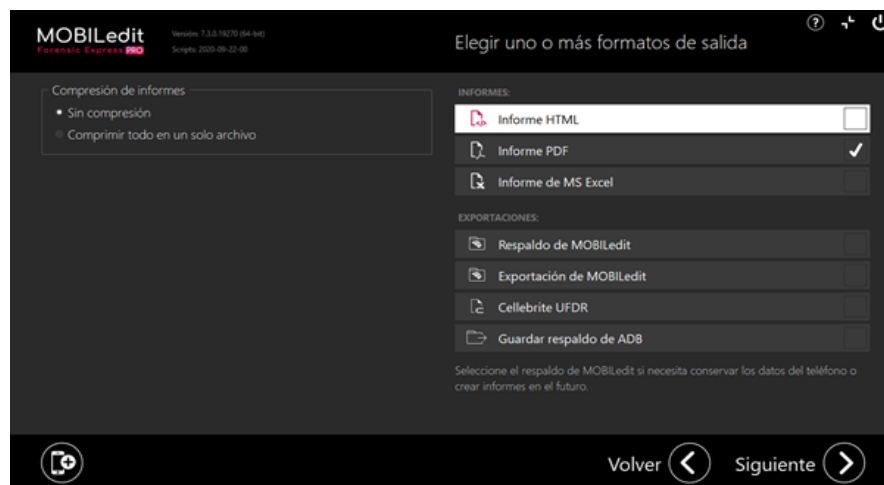


Figura 7.08: Selección del formato de visualización del informe final

Comienza la extracción de los datos para unificarlos en el informe, Figura 7.09:



Figura 7.09: Pantalla que muestra el inicio de la extracción de los datos

Una vez finalizada la exportación, como se observa en la Figura 7.10, del informe se observa la pantalla que se muestra a continuación.

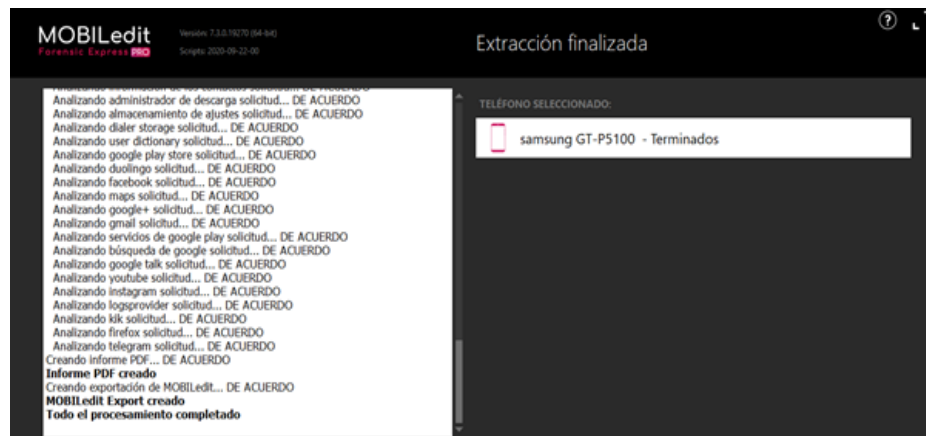


Figura 7.10: Pantalla que indica que el proceso de extracción se completó con éxito

En la Figura 7.11 se puede observar un resumen de los datos del equipo y la información aportada por la herramienta utilizada para la extracción de la información.



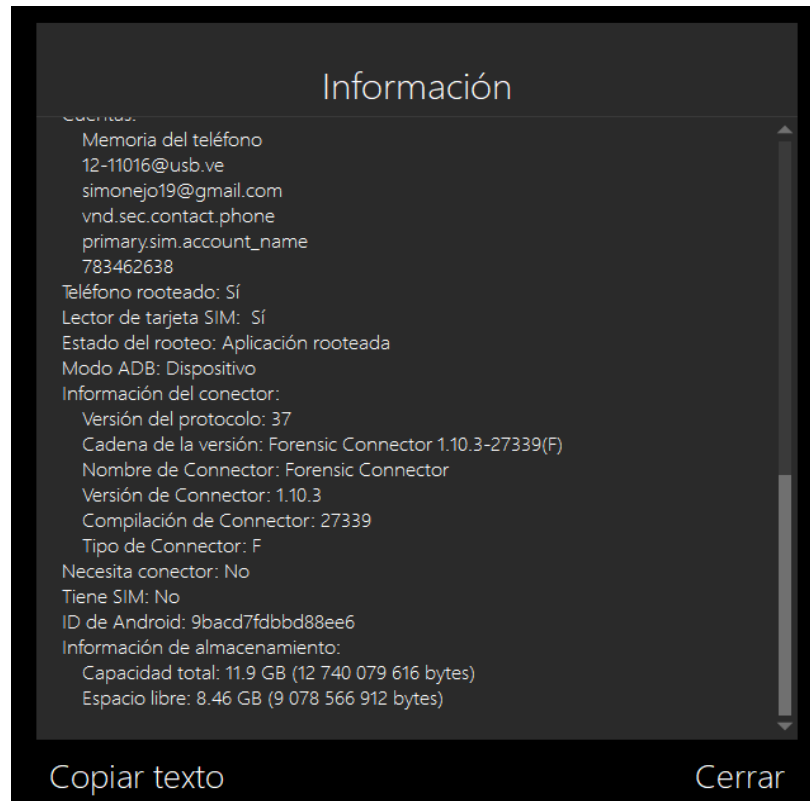


Figura 7.11: Resumen de los datos del equipo y el sistema de extracción

Por último, en la Figura 7.12 se observa el informe final que se genera luego de finalizado el proceso de extracción y las diversas configuraciones realizadas en el programa correspondiente.



REPORTE DE CONTENIDO DE FORENSIC EXPRESS

Dispositivo 1 EMPRESA - Gerente

Número de evidencia del caso: Prueba 1 - Apps



Fabricante **samsung**  
 Producto **GT-P5100**  
 Revisión de HW **IML74K**  
 Plataforma **Android**  
 Revisión SW **4.0.3 (15)**  
 Número de serie **RV1CB57F2AR**  
 IMEI **354077052032653**  
 Enraizado **Si**  
 Tarjeta SIM **Si**  
 Operador **Movistar, MCC: 734, MNC: 4**

Información del caso

Etiqueta de caso	Dispositivo 1 EMPRESA - Gerente
Número de evidencia del caso	Prueba 1 - Apps
Detalles de evidencia del caso	Extracción de aplicaciones en dispositivo corporativo

Información de dispositivo

Etiqueta del dispositivo	
Nombre del dispositivo	samsung GT-P5100
ID del dispositivo	
Número de evidencia del dispositivo	
Nombre del dueño	
Número de teléfono del propietario	
Notas telefónicas	

Información

Nombre	
Designación	
Email	
Número de teléfono	
Documento de permiso	

Información de extracción

La extracción de datos comenzó	2020-10-25 22:28:44 (UTC-4)
Extracción de datos finalizada	2020-10-25 23:01:44 (UTC-4)
Extraído por	MOBILedit Forensic Express PRO 7.3.0.19270
Informe generado por	MOBILedit Forensic Express PRO 7.3.0.19270
Aplicación del cliente	Forensic Connector 1.10.3-27339(F)

Paquetes

Scripts de la aplicación	2020-09-22-00
Degradación de la aplicación	No instalado
Base de datos de torres de antenas de telefonía celular	No instalado
EDL	No instalado
Face Matcher	No instalado
Photo Recognizer	No instalado
Traducciones	2020-09-22-00
Malware	No instalado
Imágenes de recuperación	No instalado
Soporte de captura de pantalla de iOS	No instalado
Lista de archivos excluidos	No instalado

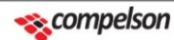


Figura 7.12: Informe de resultados

### 7.2.3 Análisis de los resultados

Una vez recolectada la información, se procede a realizar el análisis de la misma utilizando el reporte generado por la herramienta *MOBILedit*.

- Información básica del dispositivo. En la Figura 7.13 se puede visualizar la información básica del dispositivo.

The screenshot displays the MOBILedit Forensic Express interface. At the top, the logo and title 'MOBILedit Forensic Express' are visible. Below this, a header reads 'REPORTE DE CONTENIDO DE FORENSIC EXPRESS'. The main title of the report is 'Dispositivo 1 EMPRESA - Gerente', with the case number 'Número de evidencia del caso: Prueba 1 - Apps'. On the left, there is a graphic of a smartphone. To its right, a list of device specifications is provided:

Fabricante	samsung
Producto	GT-P5100
Revisión de HW	IML74K
Plataforma	Android
Revisión SW	4.0.3 (15)
Número de serie	RV1CB57F2AR
IMEI	354077052032653
Enraizado	Sí
Tarjeta SIM	No
Operador	MCC: 734, MNC: 2

On the right side, there is a section titled 'Información del caso' with a table of case details:

Etiqueta de caso	Dispositivo 1 EMPRESA - Gerente
Número de evidencia del caso	Prueba 1 - Apps
Detalles de evidencia del caso	Extracción de aplicaciones en dispositivo corporativo

Figura 7.13: Indicador de información básica del dispositivo

- Directorio telefónico. En la Figura 7.14 se observa la información obtenida del registro de contactos del dispositivo.

Se encontró un total de 261 contactos con sus nombres y números de teléfonos registrados.



Figura 7.14: Ejemplo de los datos del directorio telefónico

- Registro de llamadas: En la Figura 7.15, se visualiza el reporte de llamadas del dispositivo.

Se recuperó un total de 288 llamadas. Se puede observar el nombre del contacto, número telefónico, fecha, hora y duración de cada llamada.

Llamadas (288)  
 Todos los teléfonos llamadas, ordenado A tiempo en ascendiendo orden  
 \* Las entradas marcadas con un asterisco tienen referencias cruzadas de los contactos del teléfono

Legenda:

- Llamada marcada
- Llamada recibida
- Llamada perdida
- Llamada rechazada
- Mensaje de voz

Etiqueta	Desde / A	Hora	Duración
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	13/02/2019 15:49:01 (UTC-4)	00:00:00
☑️	Desde: 02122639630	15/02/2019 17:33:19 (UTC-4)	00:00:00
☑️	Desde: 02122639630	15/02/2019 18:59:45 (UTC-4)	00:00:00
☑️ Carlos Cedeño	Desde: 04165178769 (Carlos Cedeño)*, Carlos Cedeño	17/02/2019 18:59:54 (UTC-4)	00:00:00
☑️ Carlos Cedeño	Desde: 04165178769 (Carlos Cedeño)*, Carlos Cedeño	17/02/2019 20:16:16 (UTC-4)	00:00:00
☑️ Simone Bermudez	A: 02125421914	18/02/2019 10:16:41 (UTC-4)	00:02:41
☑️ Simone Bermudez	A: +584142159430 (Simone Bermudez)*, Simone Bermudez	18/02/2019 11:16:34 (UTC-4)	00:00:04
☑️ Simone Bermudez	A: 02125421914	18/02/2019 11:20:16 (UTC-4)	00:00:10
☑️ Simone Bermudez	A: +584142159430 (Simone Bermudez)*, Simone Bermudez	18/02/2019 11:39:35 (UTC-4)	00:00:05
☑️ Angel Lopez	A: 04168794002 (Angel Lopez)*, Angel Lopez	19/02/2019 10:11:45 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	20/02/2019 11:57:35 (UTC-4)	00:00:00
☑️ Simone Bermudez	A: 04142159430, Simone Bermudez	20/02/2019 11:58:23 (UTC-4)	00:00:51
☑️ Katherin Chacon	Desde: 04241671434 (Katherin Chacon)*, Katherin Chacon	20/02/2019 15:39:32 (UTC-4)	00:00:00
☑️ Katherin Chacon	Desde: 04241671434 (Katherin Chacon)*, Katherin Chacon	20/02/2019 15:40:35 (UTC-4)	00:00:00
☑️ Katherin Chacon	Desde: 04241671434 (Katherin Chacon)*, Katherin Chacon	20/02/2019 15:41:09 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	22/02/2019 08:45:27 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	22/02/2019 09:16:50 (UTC-4)	00:00:00
☑️ Carmen Carrasquel	A: 04142830187 (Carmen Carrasquel, Carmen Carrasquel)*, Carmen Carrasquel	22/02/2019 11:26:04 (UTC-4)	00:00:10
☑️ Simone Bermudez	A: 04142159430, Simone Bermudez	22/02/2019 12:03:23 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	22/02/2019 12:07:58 (UTC-4)	00:07:40
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	22/02/2019 13:37:44 (UTC-4)	00:01:10
☑️ Simone Bermudez	A: 02126389296	23/02/2019 21:22:26 (UTC-4)	00:33:54
☑️ Simone Bermudez	A: 04142159430, Simone Bermudez	25/02/2019 11:28:49 (UTC-4)	00:00:02
☑️	A: 123	25/02/2019 13:29:32 (UTC-4)	00:00:05
☑️ Angel Lopez	A: 04168794002 (Angel Lopez)*, Angel Lopez	25/02/2019 17:50:24 (UTC-4)	00:00:15
☑️ Katherin Chacon	Desde: 04241671434 (Katherin Chacon)*, Katherin Chacon	26/02/2019 12:07:45 (UTC-4)	00:02:02
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	27/02/2019 08:42:14 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	27/02/2019 09:11:04 (UTC-4)	00:00:00
☑️ Simone Bermudez	Desde: 04142159430, Simone Bermudez	28/02/2019 12:21:30 (UTC-4)	00:01:17
☑️	A: 02126185794	03/03/2019 18:33:24 (UTC-4)	00:00:44
☑️	A: 02126185794	03/03/2019 18:36:48 (UTC-4)	00:05:11
☑️	A: 02126185794	03/03/2019 19:05:40 (UTC-4)	00:01:16

Figura 7.15: Muestra del informe de registro de llamadas

- Mensajería: En la Figura 7.16 se puede observar el resumen de intercambio de mensajes del dispositivo y en la Figura 7.17 como se observaría al pedir un detalle de cada una de ellas.

Se identificaron un total de 1634 mensajes de 72 conversaciones, mostrando el contenido del mensaje, remitente, fecha y hora de emisión y recepción.

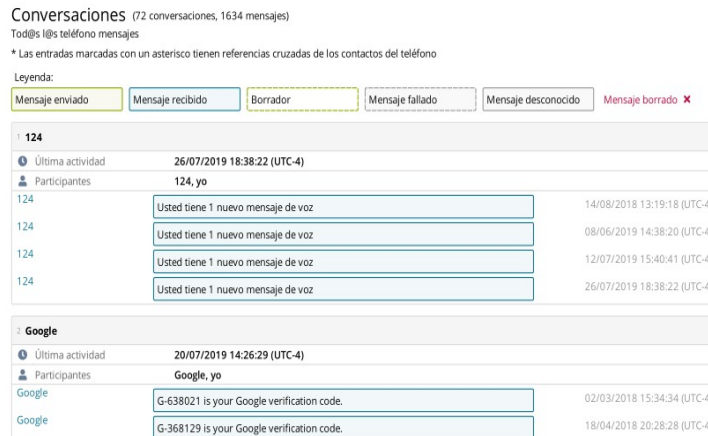


Figura 7.16: Resumen del resumen de mensajería

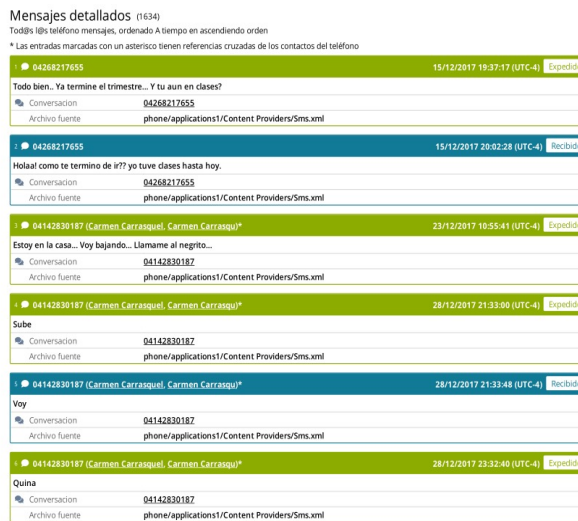


Figura 7.17: Detalle del resumen de mensajería del dispositivo

Aplicaciones: en las Figuras 7.18 y 7.19 se muestran detalles de las aplicaciones instaladas en el dispositivo.

Se encontraron más de 201 aplicaciones en las que se incluyen aplicaciones de juegos y redes sociales.

Etiqueta de caso: Dispositivo 1 EMPRESA - Gerente      Número de evidencia del caso: Prueba 1 - Apps      Etiqueta del dispositivo:

---

**Aplicaciones** (201)  
 Tod@s los Datos de aplicaciones

**501 Free New Escape Games**

Etiqueta	501 Free New Escape Games
Paquete	air.com.HFG.A51EscapeGames
Versión	17.6
tipo de aplicación	Aplicación de usuario
Instalado por	com.android.vending (Google Play Store)
Tamaño de la aplicación	115.4 MB
Tamaño de datos	164.0 KB
Tamaño del caché	0 B
Archivo APK extraído	SI
Verificación de APK exitosa	SI
Verificación del esquema APK	1

Figura 7.18: Reporte de los juegos encontrados en el dispositivo

- Datos de aplicaciones: en la Figura 7.19, se puede observar la forma de mostrar la información detallada de cada una de las aplicaciones instaladas.

<p><b>Clash Royale</b></p> <p>Etiqueta: Clash Royale</p> <p>Paquete: com.supercell.clashroyale</p> <p>Versión: 2.1.7</p> <p>tipo de aplicación: Aplicación de usuario</p> <p>Instalado por: com.android.vending (Google Play Store)</p> <p>Tamaño de la aplicación: 110.1 MB</p> <p>Tamaño de datos: 7.1 MB</p> <p>Tamaño del caché: 0 B</p> <p>Archivo APK extraído: SI</p> <p>Verificación de APK exitosa: SI</p> <p>Verificación del esquema APK: 2</p> <p>Mejor certificado encontrado: Cert-2c76c072014e3f12279e1182a2c0a666, valid from 2016-01-17T08:16:18Z to 2019-10-07T08:16:18Z Subject: CN=, OU=Juegos, L=Helsinki, O=Supercell, OU=Supercell, CN=Supercell, Issuer: CN=, OU=Juegos, L=Helsinki, O=Supercell, OU=Supercell, CN=Supercell</p> <p>Permisos para Android: com.supercell.clashroyale.permission.C2D_MESSAGE, com.google.android.c2dm.permission.RECEIVE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_WIFI_STATE, com.android.vending.BILLING, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE</p> <p>Primera instalación: 2018-02-23 14:26:19 (UTC-4)</p> <p>Última actualización: 2018-02-23 14:26:19 (UTC-4)</p>	<p><b>Dominó</b></p> <p>Etiqueta: Dominó</p> <p>Paquete: air.com.jogatina.dominio.android</p> <p>Versión: 2.1.1</p> <p>tipo de aplicación: Aplicación de usuario</p> <p>Instalado por: com.android.vending (Google Play Store)</p> <p>Tamaño de la aplicación: 66.3 MB</p> <p>Tamaño de datos: 356.0 KB</p> <p>Tamaño del caché: 0 B</p> <p>Archivo APK extraído: SI</p> <p>Verificación de APK exitosa: SI</p> <p>Verificación del esquema APK: 1</p> <p>Mejor certificado encontrado: Cert-9eacae5e7576036037be816fac5e6d041546047, valid from 2012-03-15T13:46:39Z to 2042-03-08T13:46:39Z, Subject: C=US, ST=Rio de Janeiro, L=Rio de Janeiro, O=Jogatina, OU=Mobile, CN=Android Games, Issuer: C=US, ST=Rio de Janeiro, L=Rio de Janeiro, O=Jogatina, OU=Mobile, CN=Android Games</p> <p>Permisos para Android: android.permission.INTERNET, com.android.vending.BILLING, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.DISABLE_KEYGUARD, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.GET_ACCOUNTS, air.com.jogatina.dominio.android.permission.C2D_MESSAGE, com.google.android.c2dm.permission.RECEIVE</p> <p>Primera instalación: 2018-02-23 15:17:32 (UTC-4)</p> <p>Última actualización: 2018-02-23 15:17:32 (UTC-4)</p>
--	--

Figura 7.19: Muestra de la visualización de los datos de las aplicaciones

- Media: en la Figura 7.20, se puede observar el reporte de los archivos multimedia del sistema.

<b>3.jpg</b>	
Descripción	Archivo adjunto de Gmail de "Simone Jose Bermudez Perez" <12-11016@usb.ve>
Camino	/mnt/sdcard/Download/3.jpg
Modificado	2020-02-20 09:11:13 (UTC-4)
MIMICA	image/jpeg
URL	<a href="#">non-dwnldmng-download-dont-retry2download</a>
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0x11534 (Mesa: downloads)
<b>parcial 2 de radiocom Guillermo.pdf</b>	
Descripción	Archivo adjunto de Gmail de "Simone Jose Bermudez Perez" <12-11016@usb.ve>
Camino	/mnt/sdcard/Download/parcial 2 de radiocom Guillermo.pdf
Modificado	2020-02-20 09:11:14 (UTC-4)
MIMICA	application/pdf
URL	<a href="#">non-dwnldmng-download-dont-retry2download</a>
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0x11637 (Mesa: downloads)
<b>4.jpg</b>	
Descripción	Archivo adjunto de Gmail de "Simone Jose Bermudez Perez" <12-11016@usb.ve>
Camino	/mnt/sdcard/Download/4.jpg
Modificado	2020-02-20 09:11:14 (UTC-4)
MIMICA	image/jpeg
URL	<a href="#">non-dwnldmng-download-dont-retry2download</a>
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0x11773 (Mesa: downloads)
<b>5.jpg</b>	
Descripción	Archivo adjunto de Gmail de "Simone Jose Bermudez Perez" <12-11016@usb.ve>
Camino	/mnt/sdcard/Download/5.jpg
Modificado	2020-02-20 09:11:20 (UTC-4)
MIMICA	image/jpeg
URL	<a href="#">non-dwnldmng-download-dont-retry2download</a>
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0x11876 (Mesa: downloads)

Otros archivos multimedia

Imágenes (1)

<b>downloadfile.png</b>	
Nombre de archivo	downloadfile.png
Camino	phone/applications0/com.android.providers.downloads/live_data/cache/downloadfile.png
Tamaño	2.73 KB
Modificado	2020-10-25 21:32:59 (UTC-4)
Accedido	2020-10-25 21:32:59 (UTC-4)
Anchura	96 pixel
Altura	96 pixel
Formato	png




Figura 7.20: Ejemplo de visualización de los datos de archivos multimedia

- Archivos varios: en la Figura 7.21, se muestra cómo se reportan otras informaciones de aplicaciones y opciones del sistema operativo, en este caso es específico del gestor de descargas.

### Administrador de descarga

Etiqueta	Administrador de descarga
Paquete	com.android.providers.downloads
Versión	4.0.3-P5100UBALD4
tipo de aplicacion	Aplicación del sistema
Tamaño de la aplicación	149.7 KB
Tamaño de datos	188.0 KB
Tamaño del caché	4.0 KB
Primera instalación	2012-04-13 02:27:39 (UTC-4:30)
Última actualización	2012-04-13 02:27:39 (UTC-4:30)

### Archivos descargados (114 total, 10 eliminado)

1 d=160763374551973 <span style="float: right;">✖ Eliminado</span>	
Camino	tps://android.clients.google.com/proxy/gmail/a/usb.ve/g/?version=25
Modificado	1973-05-24 15:05:03 (UTC-4)
MÍMICA	&clientVersion=
Paquete	nyVersion=1&view=att&
URL	ht
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0x7065 (Mesa: downloads)
2 =165906136220497348&partId <span style="float: right;">✖ Eliminado</span>	
Camino	tps://android.clients.google.com/proxy/gmail/a/usb.ve/g/?version=25&
Modificado	1973-10-11 14:43:02 (UTC-4)
MÍMICA	clientVersion=2
Paquete	yVersion=1&view=att&m
URL	ht
Archivo fuente	phone/applications0/com.android.providers.downloads/live_data/databases/downloads.db : 0xf4d1 (Mesa: downloads)

Figura 7.21: Reporte de otros archivos encontrados en el dispositivo



## Cadena de custodia





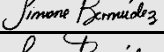


CADENA DE CUSTODIA					
INFORMACIÓN GENERAL					
<b>INCRIMINADO</b>	Miriam Viviana Cedeño Carrasquel				
<b>LUGAR DEL DELITO</b>	Calle La California, Caracas 1071, Distrito Capital. Venezuela.		<b>HORA</b>	9:12AM	
<b>TIPO DE DELITO</b>	Rastreo de actividades en dispositivo móvil.		<b>FECHA</b>	22/10/2020	
DATOS DE LA EVIDENCIA					
<b>EVIDENCIA</b>	Smartphone / Tablet	<b>NÚM. SERIAL</b>	RV1CB57F2 AR	<b>IMEI</b>	35748605030251 2
<b>MARCA</b>	SAMSUNG			<b>MODELO</b>	GT-P5100
<b>SISTEMA OPERATIVO</b>	ANDROID			<b>VERSIÓN</b>	4.0.3 (15)
<b>ESTADO</b>	<b>BUENO</b>	X	<b>REGULAR</b>	<b>MALO</b>	
<b>COLOR</b>	Plateado			<b>TAMAÑO</b>	256.6 x 175.3 x 9.7 mm
<b>DIMENSIONES</b>	76.1*150.2*9.4 mm			<b>PESO</b>	588 gr
<b>DETERIORO</b>	Ninguno			<b>OTRO</b>	N/A
<b>FECHA</b>	<b>HORA</b>	<b>OBSERVACIÓN</b>	<b>RESPONSABLE</b>	<b>FIRMA</b>	
22/10/2020	11:00 a. m.	Preservación de evidencia	Simone José Bermúdez Pérez		
23/10/2020	8:00 a. m.	Identificación de evidencia	Simone José Bermúdez Pérez		
24/10/2020	9:00 a. m.	Extracción de evidencia	Simone José Bermúdez Pérez		
25/10/2020	18:30 p.m.	Extracción de evidencia	Simone José Bermúdez Pérez		
26/10/2020	8:30 a. m.	Análisis de evidencia	Simone José Bermúdez Pérez		
27/10/2020	16:30 p.m.	Análisis de evidencia	Simone José Bermúdez Pérez		
30/10/2020	11:00 a. m.	Presentación de informe	Simone José Bermúdez Pérez		

Tabla 7.3: Resumen de la cadena de custodia

### **7.2.4 Presentación**

Como último paso en la investigación del caso práctico, se debe realizar un informe con las evidencias encontradas y las conclusiones a las que se ha llegado tras la realización del análisis.

#### **Informe de la investigación**

Periodo de investigación: 22 de octubre de 2020 – 30 de octubre de 2020.

Nombre del investigador y emisor del informe: Simone José Bermúdez Pérez.

Asunto: Rastreo de actividades en equipos móviles corporativos.

#### Resumen:

La presente investigación forense fue solicitada por la siguiente razón:

*La empresa hizo la entrega de dispositivos móviles a sus empleados para el uso exclusivo de funciones relacionadas con la empresa, no obstante, debido a las constantes quejas de sus clientes por la falta de respuesta inmediata en la atención que ofrecen, la empresa desea conocer qué tipo de información es manejada en el dispositivo que pueda estar interfiriendo en las actividades diarias de su personal.*

#### **Evidencias**

Los dispositivos incautados como objeto de prueba cuentan con las siguientes especificaciones:

- Marca de los equipos: LG.
- Modelo de los equipos: E988.
- Operadora: Digitel.
- Dispositivos: encendidos.

Además, se entregó documentación extra, perteneciente a estos dispositivos, tales como:

- Memorias extraíbles.
- Cargadores.

### **Resultados del análisis de la evidencia**

Se obtuvo los siguientes resultados de la evidencia recolectada de 1 de 5 de los dispositivos que se analizaron:

- Información básica del dispositivo (marca, modelo, IMEI, número de serie, operadora del servicio, plataforma, versión del sistema operativo entre otros).
- 261 contactos con nombres de registro y números telefónicos.
- 288 llamadas registradas (perdidas, realizadas, recibidas).
- 1634 mensajes de texto de 72 conversaciones.
- Ningún registro en el calendario.
- 201 aplicaciones (aplicaciones del sistema y de usuario).
- 1845 fotografías.
- 84 videos.
- Información básica de la tarjeta SIM.

### **Conclusiones**

El análisis de las pruebas extraídas de los dispositivos indica que la posible causa de la poca atención que brindan los empleados de la empresa a sus clientes se debe al uso excesivo de aplicaciones de redes sociales, tales como *Instagram*, *Facebook*, *Twitter* y *WhatsApp*.

La aplicación *WhatsApp* es utilizada como el medio de comunicación con los clientes y los empleados de la empresa, sin embargo, también es posible que sea usada para entablar

conversaciones con familiares, amigos, etc., que generen un tipo de distracción a los empleados.

### **Archivos adjuntos**

Anexo se encontrarán los siguientes detalles del caso:

- Reportes generados por las herramientas de *software* (reporte demasiado extenso).

## CAPITULO VIII

### CONCLUSIONES Y RECOMENDACIONES

#### Conclusiones

La investigación forense orientada al análisis de dispositivos móviles es uno de los campos de la informática forense que cada día requiere más estudio, ya que es una tecnología que se encuentra en constante actualización. Los innumerables beneficios de los *smartphones*, junto a Internet no sólo se han convertido en herramientas de uso común, sino en una necesidad para el hombre contemporáneo.

Los dispositivos móviles a pesar de tener tantos beneficios, también se han pasado a formar parte del portafolio de herramientas para delinquir y son innumerables los casos en los que se prestan para infringir en algún incidente de seguridad y/o actividad ilícita. Por otro lado, tenemos que *Android* es uno de los sistemas operativos más populares de la actualidad y además posee una gran comunidad de desarrolladores, es por ellos que son cada vez más los dispositivos móviles *Android* envueltos en incidentes y delitos informáticos.

Cuando se trata de incidentes de seguridad y delitos de carácter tecnológico y digital, aparece una figura de suma importancia, el perito digital. Estos son profesionales que intervienen cuando se requiere iniciar una investigación y se necesita recolectar información procedente de teléfonos, *tablets*, computadores, unidades de almacenamiento de datos, y redes o sistemas de datos. El perito informático es un profesional que aplica sus conocimientos en informática, telemática y electrónica para recolectar y traducir en un lenguaje claro y conciso, la información extraída de los dispositivos incautados.

El investigador forense unifica los puntos de interés del caso en un solo informe que contiene información importante para tratar los puntos litigiosos. Este no sólo se

encarga de redactar en un lenguaje más simple la información obtenida para la resolución de un caso, sino que además informa sobre en qué puede beneficiar y/o perjudicar a los involucrados del incidente.

Son diversos los métodos que un investigador forense puede aplicar para extraer y analizar los datos de un dispositivo móvil. Sin embargo, mientras los fabricantes de estos equipos continúen actualizando estas tecnologías, se presentarán nuevos obstáculos para el análisis forense. Uno de los desafíos que se tienen durante cualquier investigación forense y, especialmente, durante el desarrollo del análisis llevado a cabo en este trabajo, es el implementar técnicas que generen el mínimo de impacto en los datos y en el dispositivo.

Antes de realizar el levantamiento de la información contenida en un dispositivo móvil Android, es necesario y gran importancia comprender a fondo el funcionamiento y las características de este sistema operativo, especialmente porque está en constante actualización y es cada vez más robusto.

También se debe tener presente que al existir distintos métodos de extracción y análisis de datos, no basta con elegir cualquiera, sino que es necesario evaluar las consideraciones y las necesidades del caso, por ejemplo, se debe evaluar el tipo de caso, dispositivo, presupuesto y herramientas disponibles. En condiciones ideales, durante un caso investigativo, el analista podría tener la libertad de elegir una herramienta u otra según su criterio y tipo de caso a investigar, pero el análisis forense es un campo muy costoso que requiere equipos robustos y herramientas muy sofisticadas de precios muy elevados. De esta manera, la elección del procedimiento en muchos casos se ve limitado al presupuesto y a los recursos disponibles del laboratorio forense.

Con una base sustancial de conocimientos sobre el análisis forense en equipos móviles y sobre el sistema operativo *Android*, se desarrolló una metodología que permite la extracción, análisis y clasificación de datos de forma adecuada y organizada. Es importante aclarar que con este método se puede obtener y tener a disposición

información confidencial y que debe utilizado con ética profesional por las personas que desean aplicarlo y/o continuar esta investigación.

Durante la selección del método investigativo se debe tener en cuenta que existen varias maneras de proceder y que los métodos forenses son distintos entre sí, pero coinciden en puntos en varios en común. Para esta investigación, la metodología propuesta detalla una serie de pasos a seguir (centrada en los puntos en común de las metodologías ya existentes) sobre cómo llevar el procedimiento de investigación forense. Esta consta de 5 etapas las cuales son: preparación, identificación, adquisición, análisis y presentación. Es importante mencionar que, sin importar el tipo de caso, las nuevas actualizaciones en la tecnología y cuál sea el tipo de herramienta forense a usar, esta metodología puede ser adaptada a cada caso particular y que basta con seguir las etapas ya antes descritas.

En lo que a efectividad respecta, no es posible comparar un método sobre otro puesto a que esto depende del criterio del perito y de la forma en la que se sienta más a gusto para proseguir en la investigación. De igual manera, durante la implementación del método, cada fase puede cambiarse, modificarse y/o repetirse según las necesidades del caso y del investigador a cargo, teniendo presente que es de suprema importancia ejecutar cada fase correctamente para evitar que la evidencia sea descartada y no tenga validez jurídica.

Para la aplicación de la guía metodológica, se trabajó bajo un escenario ficticio y se simuló el procedimiento completo a partir de la incautación del equipo móvil con sistema operativo *Android*, hasta la fase final de presentación donde se elabora el informe pericial. Con este caso se buscaba evaluar y poner en práctica cada etapa dentro la metodología planteada, incluyendo su efectividad sobre recolección de evidencia con las herramientas propuestas, reportes presentados, viabilidad y limitantes de aplicación.

Luego de culminar la investigación, se puede concluir que:

- El área de la informática forense orientada a dispositivos móviles es una rama de las ciencias forenses que es relativamente nueva y se encuentra aún en desarrollo, por lo requiere aportes continuos y que los profesionales especializados en esta área se mantengan actualizados constantemente.
- Es fundamental disponer de distintos materiales bibliográficos que permitan sustentar las bases de la investigación, y así sintetizar distintas metodologías en una sola, como es la metodología propuesta en este trabajo.
- La extracción y examinación de evidencias en dispositivos móviles fue uno de los más puntos más importantes antes del análisis de resultados. Debido a la complejidad y delicadeza con la que se deben manejar los datos, es necesario que se desarrollen e implementen otros métodos que permitan hacer adquisiciones más completas y menos invasivas a fin de extraer datos de interés sobre el incidente o delito.
- Al final del proceso de ejecución de la guía propuesta, se pudo concluir que cumple su efectividad ante un proceso de peritaje informático. Es viable llevar a cabo su aplicación.
- Aunque la guía metodológica está orientada a dispositivos móviles con sistemas operativos *Android*, no representaría ningún problema aplicar la metodología en dispositivos móviles con otro sistema operativo.

### **Recomendaciones**

Con el objetivo de dar continuidad a la investigación, se pueden afinar las técnicas de extracción de la información almacenada en el dispositivo móvil mediante el desarrollo de procedimientos aún más complejos y/o con otro tipo de herramientas más sofisticadas que permitan adquirir la mayor cantidad de datos para el momento. Es importante adaptar los métodos de extracción y adquisición de datos a las nuevas actualizaciones del sistema operativo y de las herramientas forenses.

También se recomienda realizar un análisis más profundo de aplicaciones maliciosas que se encuentren disponibles en el mercado para el sistema operativo



*Android*, y esto representa un aporte importante para el área forense digital orientado a dispositivos móviles. Se recomienda implementar la metodología planteada para buscar las aplicaciones instaladas en el dispositivo, analizarlas y de encontrar aplicaciones maliciosas o que filtren información, así como evaluar su comportamiento.

Finamente, a las personas que deseen continuar con la investigación y/o aplicar el método, se les recomienda explorar otras herramientas de análisis forense además de las presentadas. E investigar un poco más para mejorar o hacer una expansión de la metodología ya presentada.

## BIBLIOGRAFÍA

- [1] Andalucía ES Digital. (2020). <https://www.seguridad.andaluciaesdigital.es>.  
<https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/seguridad+apps+m%C3%B3viles/1dcc78b6-7fc1-4d49-9348-6e59d3133dd3>
- [2] ANDROULIDAKIS, I. (2012). *Mobile Phone Security and Forensics: A Practical Approach*. Springer.
- [3] BAIR J. (2018). *Seeking the Truth from Mobile Evidence*. Elsevier Inc.
- [4] BENDINELL, I. (2013). Análisis forense de dispositivos móviles con sistema operativo Android. Buenos Aires, Argentina: Tesis de grado.
- [5] Criminalística | Ciencias Forenses. (2021). Consultado el 14 de junio de 2020 en, <http://criminalistica.mp.gob.ve/division-de-ciencias-forenses/>
- [6] Documento institucional de Welivesecurity. Consultado el 20 de mayo de 2020. Disponible en, <https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/>
- [7] EPIFANI, M. y PASQUALE STIRPARO. (2016). *Learning iOS Forensics*,. Packt Publishing.
- [8] EUROPA, C. D. (2001). *Explanatory Report to the Convention on Cybercrime*. Disponible en, <https://rm.coe.int/16800cce5b>
- [9] GRONLI, M. HANSEN, J. GHINEA, G Y YOUNAS M. (2014). *Mobile Application platform heterogeneity: Android vs Windows phone vs iOS vs Firefox OS*. IEEE.
- [10] HOOG, A. (2011). *Android Forensics - Investigation, Analysis, and Mobile Security*. Elsevier, Inc

- [11] ISO/IEC 27037:2012 - *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. [En línea]. Disponible: <https://www.iso.org/standard/44381.html>
- [12] KIPPER, G. (2007). *Wireless Crime and Forensic Investigation*. Auerbach Publications.
- [13] NILLES, G. (2017). Adquisición de dispositivos móviles con sistema operativo *Android*. Consultado en enero del 2020. Disponible en, <http://www.clei2017-46jaiio.sadio.org.ar/sites/default/files/Mem/SID/sid-09.pdf>
- [14] T.-M. Gronli, J. Hansen, G. Ghinea, y M. Younas, “Mobile application platform heterogeneity: *Android* vs *Windows* phone vs *iOS* vs *Firefox OS*,” IEEE, 2014
- [15] Lab Kaspersky (2020). Los tipos de *malware*. Consultado en agosto del 2020. Disponible en, <https://latam.Kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>
- [16] Lab Kaspersky (2020). Información sobre el *malware* y cómo proteger todos tus dispositivos. Consultado en agosto del 2020. Disponible en, <https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>
- [17] M., H. (2016). *Mobile Incident Response for Android and iOS*. NowSecure.
- [18] MORRISSEY, S. (2010). *IOS Forensic Analysis for iPhone, iPad, and iPod Touch*. A Press.
- [19] J. CANO, J. & MARTÍNEZ, J. (2016). *Computación forense*. México DF: Alfaomega.
- [20] OLEG, S. D. (2018). *Learning Android Forensics*. Packt Publishing.

- [21] Perito informático colegiado (2016). Consultado en noviembre 2020. Disponible en, <https://peritoinformaticocolegiado.es/blog//los-acusados-del-caso-anonymous-absultos-gracias-a-un-peritaje-informatico>
- [22] REIBER, L. (2019). *Mobile Forensic Investigations*. McGraw-Hil.
- [23] ROHIT, T. O. (2018). *Practical Mobile Forensics*. Packt Publishing.
- [24] SONG M, X. W. (2010). *Research on architecture of multimedia and its design based on Android*. IEEE.
- [25] T.-M. GRONLI, J. HANSEN, G. GHINEA, Y M. YOUNAS. *Mobile application platform heterogeneity: Android vs Windows phone vs iOS vs Firefox OS*. IEEE, 2014.
- [26] VASILEIOS, S. (2014). *Android Forensics*. Atenas, Grecia: Tesis de Grado.
- [27] ZDZIARSKI, J. (2008). *iPhone Forensics*. O'Reilly Media, Inc.
- [28] Developers (2020). Descripción general del almacenamiento de archivos y datos. Consultado en 24 marzo 2021, en <https://developer.Android.com/guide/topics/data/data-storage?hl=es>
- [29] MENDILLO, V. Cursos Mendillo. Consultado el 26 de marzo de 2021, en <https://mendillo.info/cursos/CursosMendillo.htm>

## ANEXO 1



**30 de octubre del 2020**

Abogado Vincenzo Mendillo

Despacho

Junta directiva empresa Soluciones iCOM C.A.

Extracción de la información del dispositivo móvil asignado a Miriam Viviana Cedeño Carrasquel.

### INFORME PERICIAL

#### 1.1 DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

<b>TRIBUNAL/JUZGADO/FISCALÍA</b>	Universidad Simón Bolívar
<b>No. De proceso</b>	00001
<b>Nombre y apellido del perito/a</b>	Simone José Bermúdez Pérez
<b>Profesión, oficio, arte o actividad</b>	Ingeniero de Telecomunicaciones
<b>Dirección de contacto</b>	Valle de Sartenejas, Municipio Baruta. Caracas, Estado Miranda, Venezuela
<b>Teléfono principal</b>	0414-000-0000
<b>Teléfono secundario</b>	0212-910-0000
<b>Dirección de correo</b>	12-11016@usb.ve

Tabla A1.1: Datos del tribunal de la causa.

## 1.2 ANTECEDENTES

A pedido de la parte interesada, quien solicita los servicios profesionales de un Perito Informático Forense para que: “Proceda a la extracción de la información del dispositivo móvil, Marca: *Samsung*, Color: Plateado, Modelo: GT-P5100, Serial No: RV1CB57F2AR”.

### 1.21 ELEMENTOS RECIBIDOS

Una tablet, marca *Samsung*, color plateado. Modelo GT-P5100, con serial No. RV1CB57F2AR, con batería original, con su cargador original y con las siguientes especificaciones técnicas.

DISPOSITIVO MÓVIL – <i>GALAXY TAB 2 10.1</i>	
<b>Marca</b>	<i>Samsung</i>
<b>Serie</b>	RV1CB57F2AR
<b>Puertos</b>	Pin de carga. MicroSD hasta 32GB Puerto de tarjeta SIM.

Tabla A1.2: Identificación del dispositivo.



Figura A1.1: Vista trasera y delantera del dispositivo utilizado en el estudio

## **2.1 FUNDAMENTOS TÉCNICOS**

### **2.1 APP (Aplicaciones).**

Programas que se instalan en los dispositivos con el fin de realizar una función específica que mejora o amplía las características del equipo.

### **2.2 *HARDWARE***

Conjunto de elementos físicos que componen un dispositivo.

### **2.3 IMAGEN FORENSE**

Es una copia exacta bit a bit de un dispositivo de almacenamiento.

### **2.4 *ROOTEО/ROOTING***

Proceso que permite al usuario manejar todos los privilegios de acceso a los archivos del dispositivo.

### **2.5 *SCREENSHOT***

Imagen capturada por un equipo informático que muestra los elementos vistos en la pantalla del dispositivo.

### **2.6 SISTEMA OPERATIVO**

Programa que coordina y dirige los servicios y aplicaciones que utiliza el usuario en un dispositivo informático.

### **2.7 *SOFTWARE:***

Programa que genera instrucciones que hacen posible el funcionamiento de un dispositivo.

## **3.1 TRABAJOS REALIZADOS**

Con la intención de cumplir con la experiencia forense digital, se realizaron los siguientes trabajos:

Para la identificación técnica y profunda del dispositivo se procedió a hacer el registro de las especificaciones del equipo, así como también de los complementos adquiridos.

Luego se procedió a realizarle un proceso de *rooting*, con la intención de poder escarbar con permisos de superusuario en los datos del equipo. Además, se hizo el levantamiento de información con el uso de una herramienta para análisis forense en dispositivos móviles. Las especificaciones del equipo se pueden observar en la Tabla A1-3.

DISPOSITIVO MÓVIL – GALAXY TAB 2 10.1	
Marca	<i>Samsung</i>
Serie	RV1CB57F2AR
Sistema operativo	<i>Android 4.0.3</i>
Capacidad	16Gb

Tabla A1.3: Características técnicas del dispositivo en prueba.

## 4.1 ELEMENTOS ADQUIRIDOS

### 4.1.1 HERRAMIENTA DE VOLCADO DE DATOS

Para el volcado de datos mediante la herramienta de *software MOBILedit Forensic Express PRO 7.3.0.19270*, se ha cumplido las normas de seguridad del *hardware* y *software* del dispositivo móvil.

Se tiene un dispositivo roteado, con sistema operativo *Android 4.0.3* (15), al que se le aplicó el levantamiento de información de forma lógica, garantizando la integridad, confiabilidad y disponibilidad de los datos contenidos en el equipo.

### 4.1.2 RESULTADOS DEL VOLCADO DE DATOS DESCRIPCIÓN DE LOS ELEMENTOS ADQUIRIDOS

Se obtienen alrededor de 10 aplicaciones de juegos instaladas, actualizadas y utilizadas durante el tiempo que estuvo designado el dispositivo móvil (tablet) a Miriam Viviana Cedeño Carrasquel.



Además, se encuentra en el historial que se realizaron visitas e interacciones a sitios web

En el proceso de volcado de información para la adquisición física de la evidencia digital del dispositivo se cumplió con los protocolos de seguridad que garantizan la adquisición, preservación e integridad de los datos.

Con esta herramienta no se sufren daños de ningún tipo. Con el *MOBILedit* se obtiene una auditoría del equipo en que se muestran eventos, datos y procesos desarrollados con el dispositivo.

Dentro de los protocolos de análisis forense se siguió el siguiente procedimiento metodológico: identificación, adquisición, preservación, análisis y presentación de resultados.

Con esto se permite mantener dentro del protocolo de trabajo además de conservar la cadena de procesos y a su vez de la información de recreación y a redes sociales.

## **5.1 ANÁLISIS FORENSE**

### **5.1.1 DETALLES DE LOS DATOS OBTENIDOS EN EL *MOBILEDIT FORENSIC EXPRESS PRO***

**Aplicaciones instaladas:** aquí se verifica si las aplicaciones que existen en el equipo deben estar instaladas o no son apropiadas para mantener el uso corporativo del dispositivo.

**Archivos descargados y recuperados eliminados:** registro de todos los archivos descargados que estén dentro del dispositivo o que hayan sido eliminados.

**Calendario:** en este apartado se obtienen todos los eventos existentes en el calendario. No se encontró evidencia del mal uso de la aplicación.

**Contactos:** se pueden ver los contactos asociados a la cuenta de Google, alojados en el teléfono y de redes sociales como *WhatsApp* y *Telegram*.

**Contraseñas:** información acerca de las contraseñas insertadas en el dispositivo, que pueden ser utilizadas para justificar el acceso a una aplicación, sitio web.

**Cookies:** de aquí se puede obtener información sobre la navegación del usuario y verificar las páginas más visitadas.

**Cuentas de usuario:** en este apartado se puede sacar información sobre las cuentas de usuario existentes en el dispositivo. Da la impresión de que más de un usuario ha tenido acceso a este equipo.

**Historial de Internet:** acá se verificaron las búsquedas en la web y los sitios más frecuentados. Hay visitas en *Facebook* y otras redes sociales.

**Mensajes y recuperación de correos eliminados:** se obtiene información sobre los mensajes de correos emitidos o recibidos del dispositivo.

**Mensajes de texto:** también se registran mensajes.

**Redes inalámbricas:** con este apartado se puede verificar si el dispositivo se ha conectado a una red *KingRoot*, con eso se puede obtener información extra sobre la presencia del individuo en ese lugar. En muchos casos pudiese ser información de gran importancia.

**Registro de Llamadas:** muestra información sobre los emisores, receptores y duración de llamadas.

**Análisis de actividad:** de aquí se pueden obtener estadísticas sobre el uso del dispositivo especialmente en las redes sociales y en las aplicaciones instaladas.

**Análisis de correos electrónicos:** se obtiene información sobre las cuentas de correo emisoras y receptoras de mensajes de correos electrónicos.

**Análisis de teléfonos:** información sobre los emisores y receptores de llamadas.

**Análisis de *WhatsApp*:** Muestra el registro de los mensajes y contenidos intercambiados con otros usuarios de esa red.

Información de extracción	
La extracción de datos comenzó	2020-10-25 22:28:44 (UTC-4)
Extracción de datos finalizada	2020-10-25 23:01:44 (UTC-4)
Extraído por	MOBILedit Forensic Express PRO 7.3.0.19270
Informe generado por	MOBILedit Forensic Express PRO 7.3.0.19270
Aplicación del cliente	Forensic Connector 1.10.3-27339(F)

Figura A1.2: Información de la extracción realizada con *MOBILedit Forensic*

## 6.1 DETALLES IMPORTANTES PARA EL CASO

El dispositivo incautado forma parte de las herramientas de trabajo y debe ser de uso exclusivo para actividades corporativas.

Efectivamente se obtiene evidencia sobre más de 10 aplicaciones distintas para recreación. Estas son:

- Juego de ajedrez

Primera instalación 2018-02-23 14:32:22 (UTC-4)

Última actualización 2018-02-23 14:32:22 (UTC-4)

- Amazon Kindle

Primera instalación 2020-04-12 00:28:58 (UTC-4)

Última actualización 2020-04-12 00:28:58 (UTC-4)

- *Candy Crush Saga*

Primera instalación 2018-02-23 14:51:15 (UTC-4)

Última actualización 2018-02-23 14:51:15 (UTC-4)

- Apalabrados

Primera instalación 2018-02-23 15:21:55 (UTC-4)

Última actualización 2018-02-23 15:21:55 (UTC-4)

- *Clash Royale*

Primera instalación 2018-02-23 14:26:19 (UTC-4)

Última actualización 2018-02-23 14:26:19 (UTC-4)

- *Day R Survival*

Primera instalación 2020-04-12 00:40:52 (UTC-4)

Última actualización 2020-04-12 00:40:52 (UTC-4)

- *Dead Zombie Shooting Target 3D- Zombie Killer 2019*

Primera instalación 2020-04-18 23:21:19 (UTC-4)

Última actualización 2020-04-18 23:21:19 (UTC-4)

Dominó

Primera instalación 2018-02-23 15:17:32 (UTC-4)

Última actualización 2018-02-23 15:17:32 (UTC-4)

También se encuentran registros de ingreso a redes sociales:

<https://es-la.facebook.com/>

<http://grooveshark.com/>

<https://twitter.com/>

<https://www.directv.com.ve/>

<https://www.inflenster.com/>

Y sitios web de entretenimiento, juegos, compras online,

<https://ww.victoriasssecret.com/>

<https://www.amazon.com/>

<https://www.netflix.com/>

<https://www.shopmissa.com/>

<https://www.spotify.com/>

<https://www.twitch.tv/>

<https://www.walmart.com/>

*Sciences et Avenir - Actualité des sciences et de la recherche - journal d'information*

Virtual Piano Sheets, Virtual Piano Notaları

*Free Printables - Scattered Squirrel*

Aprender francés, verbos y conjugaciones - *C'est facile!*

The Walking Dead en Español: The Walking Dead # 1

*La Valse d'Amelie* | Virtual Piano Music Sheets

Sailor Moon ver online todos los capítulos HD subtítulos español

## **7.1 CONCLUSIONES**

Efectivamente se ha encontrado evidencia consistente con las acusaciones, este dispositivo ha tenido gran actividad en aplicaciones no laborales. En vista que es un dispositivo destinado única y exclusivamente para asuntos relacionados con la empresa, por lo que es claro que hay un incidente.

Por medio de las cookies se registró actividad inusual en sitios web de distracción y esparcimiento tales como, música, juegos, videos, películas, libros, entre otros.

Hay muchas aplicaciones que tienen fecha de última actualización con más de 12 meses respecto a la fecha actual en la que se presenta este informe (30 de octubre del 2020). Sin embargo, es claro que el uso desmesurado e inapropiado del equipo si corresponde con las fechas de asignación a la Gerente Miriam Viviana Cedeño Carrasquel.

Se registra como fecha de entrega el 14 de marzo del 2017, por lo que queda evidencia sobre el uso del dispositivo durante los tiempos de posesión por parte de la gerencia durante el tiempo de uso.

## **8.1 DECLARACIÓN JURADA**

El presente Informe técnico consta de 21 folios, de los cuales 984 son anexos; 1005 páginas en total. El dispositivo móvil, objeto de análisis y motivo del presente informe, fue devuelto a la parte interesada manteniendo la respectiva Cadena de Custodia, en las mismas condiciones en las que se recibió para ser peritado.

Finalmente, yo, SIMONE JOSÉ BERMÚDEZ PÉREZ con C.I: 24.318.590, declaro bajo juramento que mi informe es independiente y corresponde a mi real convicción técnica y profesional, así como también, que toda la información que he proporcionado es verdadera.

Atentamente,

ING. SIMONE BERMÚDEZ.

PERITO INFORMÁTICO ACREDITACIÓN No. 0001