



**INSTITUTO UNIVERSITARIO AERONÁUTICO**  
**FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN**  
**INGENIERÍA DE SISTEMAS**

**PROYECTO DE GRADO**

**“ANÁLISIS DE METODOLOGÍAS, PROTOCOLOS Y USO DE  
HERRAMIENTAS DE FORENSIA INFORMÁTICA PARA PERITAJE DE  
SMARTPHONES EN LA REPÚBLICA ARGENTINA”**

**INTEGRANTES**

**CONSTANZA ÚRSULA GEBHARDT**  
**MAGALÍ NATALIA MALDONADO**

**TUTOR**

**ING. EDUARDO CASANOVAS**

Agradecimientos

A nuestro **tutor**, el Ing. Eduardo Casanovas, por su colaboración y predisposición en la elaboración del presente trabajo, por ser una guía indispensable a lo largo del desarrollo de esta investigación.

Al **Poder Judicial de la Provincia de Córdoba**, en particular al Sr. Fiscal de Instrucción, Dr. Enrique Gavier, al Ing. Arsenio Cardone, al Ing. Gustavo Guayanes y al Ing. Luciano Paquali, por su apertura, tiempo, colaboración y predisposición, ya que sin éstas, hubiera sido imposible concretar este proyecto.

Al **Instituto Universitario Aeronáutico** como institución, al personal administrativo y especialmente a los docentes, por ser piezas fundamentales de nuestro proceso de formación académica y desarrollo profesional.

.....

Constanza Úrsula Gebhardt

.....

Magalí Natalia Maldonado

Dedicatoria

Especialmente a mi **mamá**, por su infinita paciencia y sostén, por su dulzura y su confianza, por su amor incondicional, por siempre creerme capaz de alcanzar lo que yo me proponga.

A mi **papá**, por ser ejemplo de rectitud y de esfuerzo, de predisposición y solidaridad.

A mis **hermanos**, Maximiliano y Willy.

A mi **abuela** Teresa.

A mi **compañero** Mateo.

A **Magalí**, por ser participe necesaria de todo este proceso, por la escucha y el consejo, por el apoyo y la protección de hermana mayor. Por el afecto y la compañía, por ser un bálsamo en los momentos más difíciles.

.....

Constanza Úrsula Gebhardt

### Dedicatoria

Este trabajo de tesis quiero dedicarlo a:

A mi madre, **Dorita**, que sin ella todo esto no podría haber sido. Ella fue y es el pilar fundamental de mi vida, de mis sueños, de mis metas, y esta gran meta es para ella. Por su amor, su apoyo incondicional, su paciencia y su presencia.

A mi padre, **Mario**, quien fue el principal impulsor para que comenzara y terminara mi carrera universitaria; fue quien me alentó a seguir y no abandonar en el camino, demostrándome que sí se puede, y si se quiere, se puede llegar muy lejos.

A mi esposo, **Milton**, mi compañero de años, mi amigo, mi apoyo diario. A él que siempre me escuchó, me aconsejó y me alentó a continuar con esto que generaba en mí estados de ánimos muy cambiantes. A él, quien me enseñó, y de quien aprendo día a día.

A mis hermanos, por sobre todo al mayor de ellos, **Ismael**, porque fue él quien más de una vez ocupó sus horas de ocio para cubrirme en el trabajo para yo poder terminar mis estudios.

A mi hermano menor, **Mauro**, que gracias a la vida me permitió disfrutarlo desde otro lugar, con más años y ganas; él, mi compañero de travesuras.

Y finalmente a mi compañera, mi amiga y hermana del alma **Constanza Gebhardt**. Mi compañera de tesis, de estudio, de aventuras, de experiencias, de momentos difíciles y momentos hermosos. ¡A vos, porque sabés que sin vos el camino hubiera sido mucho más sinuoso! eternamente gracias! Gracias por tomarme la mano y dejar que camine a tu lado.

.....

Magalí Natalia Maldonado



**I**  
**U**  
**A** INSTITUTO  
UNIVERSITARIO  
AERONAUTICO

*FORMULARIO C*

Facultad de Ciencias de la  
Administración

Departamento Desarrollo Profesional

Lugar y fecha: Córdoba, 05/12/2014

INFORME DE ACEPTACIÓN del PROYECTO DE GRADO

**Título del Proyecto de Grado:** Análisis de metodologías, protocolos y uso de herramientas de forensia informática para el peritaje de smartphones en la República Argentina.

**Integrantes:** Constanza Úrsula Gebhardt, Magalí Natalia Maldonado, Ingeniería de Sistemas.

**Profesor Tutor del PG:** Ingeniero Eduardo Casanovas

**Miembros del Tribunal Evaluador:** Ing. Juan Giró, Ing. Brenda Meloni, Ing. Ma. Elena Ciolli.

Resolución del Tribunal Evaluador

- El PG puede aceptarse en su forma actual sin modificaciones.
- El PG puede aceptarse pero el/los alumno/s debería/n considerar las Observaciones sugeridas a continuación.
- Rechazar debido a las Observaciones formuladas a continuación.

Observaciones:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

<b>Índice</b>	<b>Pág.</b>
Índice.....	1
<b>Introducción.....</b>	<b>5</b>
Introducción.....	6
Situación problemática.....	8
Objetivos.....	9
Alcance del trabajo.....	10
Marco teórico.....	10
Metodología de trabajo.....	10
<b>Capítulo 1: Marco Legal.....</b>	<b>12</b>
Concepto de Derecho.....	13
Derecho Penal, Derecho Penal sustantivo y adjetivo.....	13
Normativa Penal vigente.....	15
Delito.....	15
Proceso Judicial.....	17
Roles y Responsabilidades dentro del Proceso Penal.....	20
Labor Pericial.....	21
Principio de Libertad Probatoria.....	25
Ley de Protección de Datos Personales.....	29
Ley de Delitos Informáticos.....	30
Referencias.....	32
<b>Capítulo 2: Nociones de Informática Forense.....</b>	<b>33</b>
Informática Forense.....	34
Principio de Locard.....	37
Metodología y fases de un análisis forense informático.....	37
Fase de extracción de información física.....	40
Fase de extracción de información lógica.....	40
Cadena de Custodia.....	42
Evidencia digital.....	45
Prueba y Evidencia.....	47
Roles y responsabilidades del Perito Informático.....	49
Ciberdelito.....	51
Referencias.....	56

<b>Capítulo 3: Normativa Internacional.....</b>	<b>58</b>
Convenio de Budapest.....	59
Articulación del Convenio de Budapest con la normativa legal argentina.....	63
Guías de Buenas prácticas.....	69
RFC 3227.....	69
Normas ISO / IEC 27037: 2012.....	73
PURI – Proceso Unificado de Recuperación de Información.....	77
Red G8 24/7 para delitos de alta tecnología.....	80
Referencias.....	83
<b>Capítulo 4: Consideraciones básicas sobre smartphones Android.....</b>	<b>84</b>
Introducción.....	85
Características de los dispositivos móviles.....	85
Tarjeta SIM.....	87
Equipo móvil.....	89
Componentes de hardware de un móvil con Android.....	90
Componentes de software de un móvil con Android.....	90
Estructura del sistema de archivos en Android.....	92
Referencias.....	97
<b>Capítulo 5: Aspectos procedimentales del Análisis forense de Smartphones...98</b>	<b>98</b>
Introducción.....	99
Principios rectores durante la recolección de la prueba.....	99
Orden de volatilidad.....	100
Cosas a evitar.....	100
Privacidad.....	101
La prueba informática.....	101
Proceso de recolección.....	102
Cadena de custodia.....	103
Herramientas.....	103
Protocolo de actuación para Pericias Informáticas.....	104
Pericias sobre telefonía móvil en el marco de la informática forense.....	104
Cuestiones procedimentales.....	106
Etiquetas de seguridad para dispositivos informáticos.....	109
Procedimiento aplicable a telefonía móvil.....	110
Recolección en Smartphones Android.....	117

Elementos a recolectar.....	117
Recolección de información de la tarjeta SIM.....	118
Procedimiento para la duplicación de los dispositivos USB de almacenamiento (UMS-USB-Mass Storage) en dispositivos Android.....	119
Procedimientos para la recolección lógica en dispositivos Android.....	120
Procedimientos para la recolección física en dispositivos Android.....	123
Etapa de Análisis de datos.....	125
Referencias.....	127
<b>Capítulo 6: Análisis de Herramientas Forenses Licenciadas.....</b>	<b>128</b>
Introducción.....	129
Tipos de extracción.....	129
Descripción de herramientas.....	131
UFED Touch Ultimate.....	131
XRY Complete.....	134
Oxygen Forensic Suite.....	135
Análisis comparativo.....	136
Referencias.....	139
<b>Capítulo 7: Caso Práctico.....</b>	<b>140</b>
Consideraciones Previas.....	141
Dispositivo a analizar.....	142
Conectividad.....	142
Preparación del dispositivo para la extracción.....	143
Extracción lógica.....	144
Resultados de la extracción lógica.....	149
Conclusiones.....	161
<b>Capítulo 8: Estado del Arte.....</b>	<b>163</b>
Introducción.....	163
Sobre la DACTI.....	163
Sobre protocolos y guías de buenas prácticas.....	165
Sobre el Convenio de Budapest.....	165
El escenario a nivel nacional.....	165
Sobre la cadena de custodia.....	166
Sobre el análisis forense de telefonía móvil.....	166
Sobre el registro fotográfico.....	167



Cuestiones procedimentales.....	167
¿Quién audita los procedimientos?.....	171
Sobre la selección de herramientas.....	172
<b>Capítulo 9: Desnaturalización de la evidencia digital.....</b>	<b>174</b>
Introducción.....	175
Desnaturalización de la evidencia tecnológica.....	175
Características Generales.....	177
Equipamiento.....	184
Borrado seguro de datos para Android.....	185
Consideraciones Jurídicas Legales.....	191
Referencias.....	193
<b>Capítulo 10: Conclusiones.....</b>	<b>194</b>
Conclusiones.....	195

# **INTRODUCCIÓN**

## Introducción

Durante los últimos veinte años tanto Argentina, como el resto del mundo, han asistido al fenómeno global de la democratización de las telecomunicaciones. El boom tecnológico de las comunicaciones se produce en términos de telefonía celular e Internet, realidades que en vez de presentarse separadas se complementan. La combinación de estos planos origina un medio de interacción social que actualmente está presente en todos los ámbitos del entramado sociocultural. En particular y a los fines del presente trabajo, nos enfocaremos en la telefonía móvil, más precisamente en los teléfonos inteligentes.

Un teléfono inteligente (smartphone en inglés) se diferencia de un teléfono celular ordinario principalmente por la posibilidad que ofrece al usuario de correr diversas aplicaciones sobre él, debido a que a diferencia de los celulares comunes posee un sistema operativo móvil. Podemos pensar a los teléfonos inteligentes como computadoras personales en miniatura que además nos permiten efectuar llamadas y enviar/recibir mensajes de texto. Algunas de las características básicas de este tipo de aparatos son el acceso a Internet (Wi-Fi/red 3G), la función multimedia (cámara de fotos/video, reproductor de mp3, etc.), la función de visor de documentos en variedad de formatos (.pdf, .doc, .xls, etc.), entre otras. Existe una diversidad de sistemas operativos específicos para esta clase de dispositivos, los más populares son Android (Google), iOS (Apple), Windows Phone (Microsoft) y BlackBerry OS (BlackBerry).

El crecimiento vertiginoso y asequible de la tecnología móvil ha propiciado el uso fraudulento y criminal de esta por parte de los delincuentes. Como consecuencia de este hecho, la justicia, a su propio ritmo, se vio obligada a incorporar como elemento probatorio en los procesos judiciales a los teléfonos celulares primero, y a los smartphones después. Mientras los delincuentes han perfeccionado maneras cada vez más ingeniosas de infringir la ley, las fuerzas policiales y judiciales han tenido que elaborar formas más eficaces de someterlos a la justicia.

En el proceso penal la práctica de la prueba se concreta a fines de determinar la culpabilidad del imputado. Sucede en muchos de los casos, que la explicación de ciertos hechos relevantes para el proceso judicial requiere de determinados conocimientos técnicos/científicos ajenos al saber específico del magistrado que entiende en la causa. En este escenario surge la necesidad de que el juez sea asistido en la apreciación de los hechos, con el fin de potenciar su capacidad de juzgar, por sujetos con saberes especiales en alguna ciencia, técnica, arte o industria, a los cuales se denominan peritos.

Encuadrando la actividad de los peritos se encuentran las Ciencias Forenses, que según el diccionario implican la aplicación de prácticas científicas dentro del proceso legal. Éstas incluyen todas aquellas ciencias (Derecho, Medicina, Psicología, Biología, Ingeniería, etc.) o especialidades científicas cuyos principios, métodos y técnicas coadyuvan al proceso legal.

Existe una relación de proximidad conceptual y práctica importante entre la criminalística y las ciencias forenses. Adherimos a la definición del Dr. Rafael Moreno González, que la describe como la disciplina que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen de material sensible significativo relacionado con un presunto hecho delictuoso, con el fin de determinar, en auxilio de los órganos de administrar justicia, su existencia, o bien reconstruirlo o bien señalar y precisar la intervención de uno o varios sujetos en el mismo.

Retomando la temática de la ciencia forense, es pertinente a los fines de este proyecto, acercarnos al concepto de cómputo forense, también denominado forensia informática. La forensia informática es la aplicación de técnicas, científicas y analíticas especializadas, a infraestructuras tecnológicas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

El cómputo forense se encarga de analizar diferentes sistemas informáticos en la búsqueda de datos, información y evidencia, potenciales o relevantes, que colaboren con una causa judicial o una negociación extrajudicial. Es de carácter científico ya que utiliza el método científico, el que supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y medible, aplicando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtiene más evidencia.

La metodología aplicada en la forensia informática debe ser conocida, sabida y practicada, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a las mismas conclusiones. Sus resultados deben ser objetivos e imparciales, implicando un alto grado de profesionalidad en el desarrollo de todas las tareas a realizar. Deben explicar de forma clara las relaciones de causa y efecto, eliminar aquellas alternativas que sean estimativas y evitar las conclusiones no falsables.

En síntesis, la forensia informática como una ciencia de análisis, de descubrimiento, de aplicación, etc. deberá permitir responder las preguntas: ¿Cuándo?, ¿Quién?, ¿Cómo?, ¿Dónde?, ¿Para qué? y ¿Por qué?

En cuanto al informático forense, éste debe ser una persona capaz de manejar y hacer uso de la tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos y, poseer una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. Sus conocimientos abarcan desde el software hasta el hardware, de redes, de seguridad, de hacking, de cracking, de recuperación de información, etc.

Cabe destacar que el cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello tenemos la seguridad informática. Con esto queremos destacar que es más que preciso tener en claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática. La seguridad informática, por su parte y en su rol preponderantemente preventivo, se enfoca en salvaguardar la infraestructura de cómputo y todo lo relacionado con ésta, y en particular la información contenida o circulante. La auditoría informática comprende un proceso llevado a cabo por profesionales que consiste en reunir, agrupar y evaluar evidencia para determinar si un sistema informático protege el activo empresarial, conserva la integridad de los datos, cumple eficazmente con los objetivos de la organización, emplea de manera eficiente los recursos disponibles y a su vez, respeta la normativa establecida.

#### *Situación problemática*

A nivel nacional, observamos una ausencia de reglamentación con respecto a herramientas y metodologías de uso en la pericia informática en general y a la relativamente novedosa pericia de smartphones en particular. Consideramos que la existencia y posterior adhesión a unos lineamientos claros en la materia posibilitarían:

- La adecuada delimitación del alcance de los servicios profesionales forenses de este tipo
- Formalizar la actuación pericial en materia de teléfonos inteligentes
- Profundizar el resguardo de la cadena de custodia de la prueba, garantizando la preservación de la evidencia digital

Por otra parte, la República Argentina no está completamente adherida a convenios internacionales sobre cibercriminalidad que contribuyan a la rápida y eficaz cooperación entre naciones. En particular, se encuentra en proceso de adecuarse al Convenio de Budapest (sancionado en el año 2001 por el Comité de Ministros del Consejo de Europa junto a Estados Unidos, Canadá, Japón, Costa Rica, México y Sudáfrica, y en vigencia desde el año 2004), el único que se encarga de la seguridad informática y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos. La Convención de Budapest es prioritaria debido a que provee un marco veloz y seguro, de cooperación y colaboración internacional para garantizar la persecución de delitos transnacionales, por lo que la participar de este acuerdo de forma plena le permitiría a la Argentina tanto ofrecer como recibir asistencia técnico legal en materia de cibercrimen.

Desde la sanción de este acuerdo, nuestro país enfrentó y enfrenta un largo proceso tendiente a minimizar las lagunas jurídicas que existen en el ordenamiento nacional respecto a los delitos producidos a través de las nuevas tecnologías de la información. Si bien se han alcanzado hitos importantes (como la Ley 25.326 de Habeas Data en el año 2000 y la Ley 26.388 de Delitos Informáticos en el año 2008) es bastante todavía el trabajo que debe realizarse en materia de reglamentación, siempre con la intención de unificar y estandarizar criterios.

### Objetivos

A partir del estudio de metodologías, protocolos y herramientas de pericia informática de teléfonos inteligentes, extraer conclusiones que aporten mejoras a los actuales procesos de peritaje ejecutados en el ámbito de la provincia de Córdoba. Los objetivos del proyecto son:

- Analizar teóricamente la normativa a nivel nacional y provincial y su relación con convenios internacionales.
- Investigar una serie de herramientas de forensia de teléfonos móviles inteligentes.
- Realizar el seguimiento de un caso testigo.
- Elaborar propuestas de mejora referidas a la materia.

### Alcance del trabajo

Espacialmente, nos circunscribimos al ámbito de la Provincia de Córdoba, República Argentina. Temporalmente, este trabajo se realizará durante el año 2014, por lo que considerará como válida la reglamentación vigente a la fecha.

Cabe destacar que queda fuera del alcance del presente proyecto, el desarrollo de una herramienta de software de forensia informática. Nos limitaremos a analizar aplicaciones ya existentes.

Por otra parte, excede a los límites de este trabajo el análisis del tráfico de las comunicaciones y la intervención de las líneas telefónicas.

### Marco Teórico

Con el objetivo de abordar las diferentes etapas del proyecto, será necesario introducir y recuperar conceptos de diversas disciplinas.

En primer lugar, debemos efectuar un acercamiento a la problemática legal. Es necesario formar un vocabulario adecuado en la materia, como así también tomar conocimiento acerca de normativa, procedimientos y protocolos aplicables, tanto en la República Argentina (Derecho Penal) como en la Provincia de Córdoba (Derecho Procesal Penal).

A su vez, será necesario entrar en contacto con convenios que existan a nivel regional e internacional sobre cibercriminalidad, como así también determinar el grado de adhesión de nuestro país.

Luego, se torna imprescindible formar un basamento teórico de criminalística y forensia en general, para luego, abocarnos al cómputo forense. Dentro del universo del cómputo forense, como ya anunciamos, nos enfocaremos en la pericia de teléfonos móviles inteligentes, por lo que será menester investigar bibliográficamente cual es el estado del arte.

### Metodología de trabajo

La metodología de trabajo a emplear en el proyecto consta de dos momentos: en una primera instancia un estudio descriptivo, y posteriormente, un estudio comparativo.

Una investigación descriptiva procura describir los hechos tal como son observados, los datos son recolectados sin modificar el entorno del fenómeno estudiado. En un estudio de este tipo, se selecciona un conjunto de asuntos y se analiza cada uno de ellos independientemente, para así, describir, explicitar la situación que se investiga.

Una vez caracterizado tanto el estado actual de la pericia informática en la Provincia de Córdoba, como una serie de herramientas de cómputo forense, procederemos a efectuar un estudio comparativo de los distintos instrumentos de software que se pueden emplear en tal tarea, a fin de arribar a conclusiones que sirvan de sugerencia para mejorar las prácticas actuales.



# **CAPÍTULO 1**

## **MARCO LEGAL**

### Concepto de Derecho

Antes de encarar los ejes temáticos que guiarán este proyecto de investigación, nos pareció relevante recuperar la noción de Derecho. El Derecho es probablemente una de las ciencias que mayor dificultad han tenido sus estudiosos para conceptualizar, como directa consecuencia, una multiplicidad de definiciones han sido elaboradas.

La palabra Derecho proviene del vocablo latino *directum*, que significa sujeción a una regla, no apartarse del buen camino, lo que se dirige o es bien dirigido. A continuación, recuperamos tres diferentes nociones de Derecho, que dan cuenta de la diversidad de las propuestas:

- Para Arauz Castex, abogado y político argentino, “el Derecho es la coexistencia humana normativamente pensada en función de justicia”.
- Para Borda, destacado jurista argentino, “es el conjunto de normas de conducta humana establecidas por el Estado con carácter de obligatorio y conforme a la justicia”.
- Para Salvat, abogado, jurista y escritor argentino, “es el conjunto de reglas establecidas para regir las relaciones de los hombres en sociedad, en cuanto se trate de reglas cuya observancia puede ser coercitivamente impuesta a los individuos”.

Lo concreto es que la convivencia de los hombres en sociedad exige inexorablemente la vigencia de las normas a las cuales deban ajustar su accionar; de forma contraria, reinaría el caos y la vida colectiva sería imposible. Es por esto que hasta en las sociedades más primitivas, siempre existieron normas de conducta (escritas o no) que regulaban la convivencia de los individuos.

Por lo expuesto, podemos afirmar que el Derecho constituye el orden normativo e institucional de la conducta humana en sociedad, basado en postulados de justicia y certeza jurídica, establecido sobre las relaciones sociales existentes que determinan su contenido y carácter en un lugar y momento determinado. Por otro lado, desde el punto de vista objetivo, dicese del conjunto de leyes, reglamentos y demás resoluciones, de carácter permanente y obligatorio, creadas por el Estado para la conservación del orden social.

### Derecho Penal, Derecho Penal sustantivo y adjetivo

Dentro de este conjunto de reglas que constituyen el Derecho, existen algunas que por su incumplimiento e inobservancia, vienen impuestas con una sanción. A este

conjunto de reglas impuestas bajo amenaza de sanción se lo denomina Derecho Penal. En consecuencia, si alguien no observa las reglas con sanción, es merecedor de una pena. Dicho de otra manera, el Derecho Penal está constituido por las disposiciones jurídicas que regulan la potestad punitiva del Estado relacionando hechos, estrictamente determinados por la ley con una pena, medida de seguridad o corrección como consecuencia de realizar un determinado acto, cuyo objetivo es el de asegurar los valores elementales para la sana convivencia de los individuos de una sociedad.

Para concluir si una persona ha vulnerado una regla de conducta con sanción, existe un conjunto de pautas, que la autoridad, el ofendido y/o la víctima y quien es acusado de vulnerarla deben seguir para llegar a establecer si es culpable o no. A este conjunto de reglas jurídicas que regulan la actuación de un tribunal, de las partes (imputado y fiscal) y que ordenan los actos requeridos para decidir si ha de imponerse una sanción, se lo denomina Derecho Procesal Penal.

Es por lo expuesto que somos capaces de distinguir una clasificación dentro del Derecho Penal: El Derecho Penal Sustantivo, y por otro lado, el Derecho Penal Adjetivo. El Derecho Penal Sustantivo es el que conocemos como Código Penal o leyes penales , y en este se encuentran las normas promulgadas por el Estado, establece los delitos y las penas, mientras que el Derecho Procesal Penal es el conjunto de normas destinadas a establecer el modo de aplicación de aquellas.

El Derecho Sustantivo es el que trata sobre el fondo de la cuestión, reconociendo derechos, obligaciones etc. Es aquel que se encuentra en la norma que da vida a una determinada figura jurídica, acto jurídico o figura típica, imponiendo los comportamientos que deben seguir los individuos en la sociedad. Regula el deber ser, el que impone los comportamientos que deben seguir los individuos en la sociedad.

Por su parte, el Derecho Adjetivo está constituido por las normas destinadas a garantizar el ejercicio de los derechos y el cumplimiento de las obligaciones consagradas por el Derecho Sustantivo. El Derecho Adjetivo señala la forma en la que se va a hacer valer el derecho contenido en el Derecho Sustantivo, y ambos crean un cuerpo de leyes que se complementan, pues sin uno el otro no tendría sentido. El Derecho Adjetivo o Procesal está conformado por las normas que regulan el proceso, que es, a su vez, el mecanismo para realizar al Derecho Sustantivo.

### Normativa Penal vigente

Resulta relevante mencionar brevemente la normativa vigente en materia de Derecho Penal en la República Argentina en el corriente año (2014), ya que esta será estructurante para la realización del proyecto.

En materia de Derecho Sustantivo, debemos hacer referencia al Código Penal de la Nación Argentina 2014 (de ahora en más CP). Es importante considerar que para la edición vigente se ha tomado como base el texto ordenado por el decreto 3.992 del 21/12/1984, y sus sucesivas modificaciones. Cabe aclarar que ha sido habitual que los montos de las penas de multa fueran actualizados debido a desvalorizaciones de la moneda.

Se considera menester recuperar los siguientes aspectos:

- En el Título 1 (Libro primero, Disposiciones generales) se señala que la aplicación de este Código es para delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción, como así también para delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo.
- En el Título 2 (Libro primero, Disposiciones generales) se citan las penas que el Código establece: reclusión, prisión, multa e inhabilitación.

En materia de Derecho Procesal, debemos citar tanto el Código Procesal Penal Argentino como el Código Procesal Penal de la Provincia de Córdoba.

El Código Procesal Penal Argentino (de ahora en más CPP)- Ley 23.984 fue sancionado por el Senado y la Cámara de Diputados el 21 de agosto de 1991 y promulgado el 4 de septiembre de 1991, sin embargo, se debe considerar que desde entonces se han introducido sucesivas modificaciones al texto base.

Por su parte, el Código Procesal Penal, Provincia de Córdoba (de ahora en más CPPC) – Ley 8.123, sancionado el 5 de diciembre de 1991 y publicado en el Boletín Oficial del 16 de enero de 1992, también ha sufrido modificaciones que constituyen la versión 2014.

### Delito

Uno de los núcleos conceptuales del Derecho Penal es el de delito. El vocablo proviene del verbo latino *delinquo, delínquere, deliqui, delictum*, cuyo significado es desviarse, abandonar la Ley. En palabras del Dr. Núñez, destacado penalista cordobés,

delito es todo hecho, típico, antijurídico, culpable y punible. Por su parte, para el Dr. Zaffaroni, abogado, escribano y ministro de la Corte Suprema de la República Argentina, el delito es una conducta humana individualizada mediante un dispositivo legal (tipo) que revela su prohibición (típica), que por no estar permitida por ningún precepto jurídico (causas de justificación), es contraria al orden jurídico (antijurídica) y que por serle exigible al autor que actuase de otra manera en esa circunstancia, le es reprochable (culpable). Es importante aclarar algunas nociones:

- Tipo: el principio *nullum crime sine pravia lege poenali* ("Ningún delito, ninguna pena sin ley previa"), deja fuera del área del derecho penal los hechos que en su estructura jurídica no se presentan como tipos predeterminados por el legislador.
- Antijurídico: la tipificación presupone jurídicamente normas prohibitivas u ordenadoras de esos hechos como antijurídicos por ser socialmente inadecuados por su dañosidad para los bienes jurídicos (excepción; se puede excluir la imputación si el autor comete un hecho en defensa de un interés que la ley aprecia como preponderante frente al bien protegido por la pena por ejemplo; la legítima defensa.)
- Culpable: las normas tienen por objeto la regulación de la conducta humana. Se presupone que sus destinatarios son personas dotadas de capacidad y susceptibles de ser objeto de un reproche jurídico por su violación como culpable de ella. El código penal asienta la responsabilidad delictiva en la posesión por parte del autor de la conciencia de la criminalidad del acto y de la posibilidad de dirigir sus acciones.
- Punible: además de los elementos estructurales admite que lo castigue en el caso concreto para satisfacer las otras condiciones establecidas por la ley para que proceda al castigo.

En estricto sentido legal, los códigos penales y la doctrina definen al "delito" como toda aquella conducta (acción u omisión) contraria al ordenamiento jurídico del país donde se produce. Vale aclarar que crimen y delito son términos equivalentes. Su diferencia radica en que delito es genérico, y por crimen se entiende un delito más grave o, en ciertos países, un delito ofensivo en contra de las personas. Tanto el delito como el crimen son categorías presentadas habitualmente como universales; sin embargo los

delitos y los crímenes son definidos por los distintos ordenamientos jurídicos vigentes en un territorio o en un intervalo de tiempo.

### Proceso Judicial

En relación directa con la noción de delito, surge el concepto de proceso judicial. Se entiende por proceso, según el Dr. Gómez Lara (jurista mexicano), al conjunto complejo de actos del Estado como soberano, de las partes interesadas y de los terceros ajenos a la relación sustancial, actos todos que tienden a la aplicación de una ley general a un caso concreto controvertido para solucionarlo o dirimirlo. Para comprender el sentido y alcance de la expresión es importante entender el rol primordial del Estado en el mantenimiento de la paz social. Por su parte, Devis Echandía (jurista y procesalista colombiano), explica que, en un sentido literal y lógico, no jurídico, por proceso se entiende cualquier conjunto de actos coordinados para producir un fin. Ya inmersos en el terreno jurídico, pero con sentido general, entendemos por proceso una serie o cadena de actos coordinados para el logro de un fin jurídico. Haciendo foco en la esfera judicial, se entiende por proceso judicial al conjunto de actos coordinados que se ejecutan por los funcionarios competentes del órgano judicial del Estado, para obtener, mediante la actuación de la ley en un caso concreto, la declaración, la defensa o la realización coactiva de los derechos que pretendan tener las personas privadas o públicas, en vista de su incertidumbre o de su desconocimiento o insatisfacción (en lo civil, laboral o contencioso administrativo) o para la investigación, prevención y represión de los delitos y las contravenciones (en materia penal), y para la tutela del orden jurídico y de la libertad individual y la dignidad de las personas, en todos los casos (civil, penal, etc.).

El Código Procesal Penal de la Nación regula, por su parte, el proceso penal. Los delitos cometidos por personas mayores de edad (mayores de 18 años) serán juzgados por la Justicia Criminal o la Justicia Correccional, según la pena del delito sea o no superior a los tres años. En cambio, respecto de las personas imputadas menores de 18 años se aplica el procedimiento especial regulado por la Ley 22.278 – Régimen Penal de la Minoridad, promulgada en agosto de 1980, y sus sucesivas modificaciones.

Un proceso penal entonces, inicia con la comisión de un hecho delictivo. Este proceso se divide en tres etapas: la *investigación o instrucción preparatoria*, el *plenario, juicio o debate oral y público* y la *ejecución de la sentencia*.

Ante este hecho delictivo, la Justicia inicia su intervención bien sea por que alguien formula una denuncia o por actuación de oficio, es decir sin que la denuncia exista.

Existen entonces dos modos de disparar el proceso penal:

- Por prevención:

El proceso se inicia por prevención cuando las fuerza de seguridad (policía federal, prefectura, policía aeronáutica, servicio penitenciario, etc.) sorprende a un persona in fraganti cometiendo un delito.

- Por denuncia

El proceso se inicia por denuncia cuando una persona particular da noticia sobre la comisión de un delito. El Art. 174 del CPP indica que toda persona que se considere lesionada por un delito cuya represión sea perseguible de oficio o que, sin pretender ser lesionada, tenga noticias de él, podrá denunciarlo al juez, al agente fiscal o a la policía. Cuando la acción penal depende de instancia privada, sólo podrá denunciar quien tenga derecho a instar, conforme a lo dispuesto a este respecto por el Código Penal.

En la Provincia de Córdoba, el primer órgano judicial en intervenir es la Unidad Judicial de la zona donde ocurrió el hecho. El personal de esta unidad judicial, encabezado por un ayudante fiscal, es el encargado de lo que en la jerga se conoce como "medidas urgentes": inspección ocular, diseño del croquis del lugar y toma de testimonios.

La Unidad Judicial deriva el hecho a la Fiscalía de Instrucción del distrito y turno que corresponda. El fiscal de Instrucción, en estricto orden, establece las imputaciones, espera la asignación de abogados, toma indagatorias, testimonios y solicita las pericias necesarias.

La *investigación* es la etapa procesal de recolección de las pruebas necesarias que darán sustento a la acusación, de ahí que también se la llame instrucción preparatoria de la acusación, que tendrá lugar en la próxima etapa. Cuando el juez estimare que las evidencia recolectadas le crearen la sospecha de que la persona ha cometido un delito, la citará a prestar declaración indagatoria a fin de que brinde las explicaciones que estime correspondan, según lo expresado en el Art. 294 del CPP. Posteriormente, el juez deberá resolver su situación procesal adoptando tres clases de decisiones:

- Procesamiento: cuando las pruebas colectadas hagan surgir la "probabilidad" de que el imputado cometió el delito. En este caso, el juez también deberá decidir si dicta o no la prisión preventiva del imputado.

- Sobreseimiento: cuando las pruebas indiquen que el delito no existió, no se cometió o el imputado no participó en él. Es una decisión que desvincula al imputado del proceso.
- Falta de mérito: cuando las pruebas no sean suficientes ni para procesar ni para sobreseer.

En su tarea investigativa, y en el caso de que la investigación culmine en un procesamiento, el fiscal de Instrucción puede solicitar la prisión preventiva de un imputado si considera que el hecho es grave, la condena va a ser grave o existe la posibilidad de que el imputado huya.

Sin embargo, hasta aquí no se debe perder de vista que todo el proceso se basa en un juicio de probabilidad basado en el principio de inocencia que establecen las leyes en nuestro país, esto es que toda persona es inocente hasta que se demuestre lo contrario. Una vez que la causa atravesó la investigación penal preparatoria, se inicia la etapa conocida como "juicio de certeza".

Cuando el juez hubiera procesado, y estimare que la investigación está completa (no existen más evidencias por recoger), remitirá la causa primero al querellante, luego al fiscal y, finalmente al defensor para que digan si, de acuerdo a las pruebas colectadas, corresponde o no llevar a cabo el Juicio Oral.

El *juicio oral* o *debate* es la etapa procesal en el cual se valorará las pruebas recolectadas durante la instrucción para arribar a una decisión final que tomará varios jueces o uno sólo, según que la penalidad del delito supere o no los tres años.

Luego de que la causa fue elevada a juicio, sin oposición ni apelación, y después de una investigación suplementaria, se produce la audiencia. Este debate arranca con la lectura de la acusación para continuar con la declaración de él o los imputados.

Posteriormente declaran los testigos, peritos y se producen los careos en caso de declaraciones disímiles. En una etapa casi final conocida como los "alegatos", interviene el fiscal para presentar sus conclusiones y la investigación, y solicitar la pena que considera adecuada para el delito cometido. La defensa hace exactamente lo mismo.

El imputado por su parte tiene la posibilidad de hacer la última intervención en el recurso oral conocido como "última palabra". Este es el paso previo al veredicto en donde se conoce la absolución o condena del imputado. Los "fundamentos de la sentencia" se conocen recién 15 días después del veredicto.



La sentencia también puede llegar al Tribunal Superior de Justicia mediante un recurso de casación e incluso podría tocar las puertas de la Corte Suprema de Justicia mediante recursos extraordinarios.

Cabe destacar que el debate constituye la etapa principal del proceso penal, pues en ella se decidirá si corresponde o no aplicar pena al imputado, sobre la base de las pruebas recolectadas durante la instrucción o investigación. Aquí se volverá a valorar toda la prueba en una única audiencia, y a cuyo término, el órgano judicial sólo tendrá dos posibilidades para sentenciar: absolver o condenar.

La *ejecución* está vinculada al cumplimiento de la sentencia dictada por un tribunal.

### *Roles y Responsabilidades dentro del Proceso Penal*

A continuación haremos una breve descripción de los actores que intervienen en un proceso penal en la República Argentina.

El juez es la máxima autoridad de un tribunal de justicia, cuya principal función es precisamente ésta, la de administrar justicia, en caso que se presente ante él una situación controvertida entre dos partes. Es un funcionario público que tiene como misión juzgar y hacer ejecutar lo juzgado.

Es menester recuperar el rol del Ministerio Público en el proceso penal, según lo expresado por el Art. 71 del CPPC., el mismo deberá promover y ejercer la acción penal en la forma establecida por la Ley, como así también, deberá dirigir la Policía Judicial y deberá practicar la investigación fiscal preparatoria.

Por su parte, según el Art. 82 del CPP, y respecto a la noción de querellante particular, se indica que toda persona con capacidad civil particularmente ofendida por un delito de acción pública tendrá derecho a constituirse en parte querellante y como tal impulsar el proceso, proporcionar elementos de convicción, argumentar sobre ellos y recurrir con los alcances que en ese Código se establezcan. En caso de haber resultado la muerte de la víctima, ese derecho de querellar lo tendrán el cónyuge, los hijos, padres o su último representante legal.

En cuanto al imputado, podemos definirlo como aquella persona a la cual se le atribuye la participación en un delito o hecho punible, siendo entonces uno de los más relevantes sujetos procesales.

### Labor Pericial

En este apartado haremos foco en los conceptos puntuales referentes a labor pericial en el marco de los procesos judiciales.

Acontece frecuentemente, que la comprobación o la explicación de ciertos hechos controvertidos y conducentes en un proceso judicial, requiere de saberes técnicos ajenos al conocimiento específico del magistrado que entiende en el mismo. De allí la necesidad de que éste sea auxiliado, en la apreciación de esa clase de hechos, para enriquecer su capacidad de juzgar, por personas que posean conocimientos especiales en alguna ciencia, técnica, industria o arte, a quienes se denomina “peritos”.

Se puede describir a la pericia como el conjunto de operaciones técnicas científicas puestas en práctica para el esclarecimiento de un posible hecho ilícito y ordenadas por el Tribunal interviniente; en segundo término, definimos al perito como la persona designada para llevar a cabo dichas operaciones, siempre basadas en sus capacidades científicas o técnicas especializadas.

La prueba pericial, justamente, consiste en la actividad que desarrollarán los peritos dentro del proceso judicial. Acorde con el Art. 231 del CPPC se podrá ordenar una pericia cuando para descubrir o valorar un elemento de prueba fuere necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte o técnica.

El Art. 232 del mismo Código se refiere a la calidad habilitante del perito, indicando que los mismos deberán tener título habilitante en la materia a la que pertenezca el punto sobre el cual han de expedirse, siempre que la profesión, arte o técnica estén reglamentados. En caso contrario, deberá designarse a persona de idoneidad manifiesta.

“La prueba pericial consiste en el informe brindado por una persona ajena al proceso, con especiales conocimientos técnicos, y/o científicos sobre la materia en litigio, que a través de un proceso deductivo (de lo general a lo particular), partiendo de sus conocimientos específicos, los aplica al caso concreto y elabora su opinión fundada con los elementos ciertos que surgen de la causa en análisis.

...El perito designado, es un auxiliar del órgano judicial (...) que atento a su especialidad e idoneidad en determinada materia, contribuye a la dilucidación de la causa, en aquellas cuestiones técnicas y científicas ajenas, al conocimiento del juzgador.

...Se ha sostenido de manera reiterada que la función pericial tiende a suministrar los elementos de juicio al órgano jurisdiccional, en áreas científicas o técnicas

específicas que escapan a la formación jurídica de quien lo integra o por lo menos, que éste no tiene el deber de conocer en profundidad.”<sup>(1)</sup>

En este punto, es relevante remarcar la diferencia conceptual entre el perito y el testigo. Si bien ambos son órganos de prueba introducidos en el proceso por resolución del tribunal, tanto la jurisdicción como la doctrina distinguen sus perfiles.

Existe una distinción temporal, basada en el hecho de que al testigo se lo llama a declarar porque existen constancias de que ha percibido el hecho al momento de suceder; él se limita a contar lo que sus sentidos le han mostrado, sin analizar las razones causa-efecto y los elementos intrínsecos del mismo. Bien se dice que el testigo “depone” y el perito “dictamina”; la diferencia es cualitativa.

Cuando se dan las condiciones de seriedad científica y severidad de análisis el dictamen no se puede comparar con el testimonio, siempre discutible y casi nunca seguro, mucho menos con la confesión, cuyo valor ha decaído hasta quedar en el mero indicio o declaración susceptible de crítica.

El perito se diferencia del testigo por su calidad fungible, porque el operador experimenta y saca conclusiones, resultados científicamente establecidos de antemano.

A diferencia del perito, el testigo sólo es llamado a participar en aquellos procesos en los cuales se deben comprobar los hechos por él presenciados. Su actuación es siempre unipersonal, mientras que la pericia puede ser conjunta.

El Art. 236 del CPPC, que hace referencia al nombramiento y notificación del perito, indica que se designará un perito, salvo que se estimara indispensable que sean más. El/los peritos designados por el órgano judicial son llamados peritos de oficio. El Art. 237 referido a los peritos de control, fija que cada parte podrá proponer a su costa otro perito legalmente habilitado, estos peritos de control normalmente son denominados peritos de parte.

En el Art. 238, acerca de las Directivas, señala que el órgano que ordene la realización de la pericia, formulará las cuestiones a elucidar, fijará el plazo en que ha de expedirse y si lo juzgare, dirigirá personalmente la pericia, asistiendo a las operaciones. Podrá igualmente indicar donde deberá efectuarse aquella y autorizar al perito para examinar las actuaciones o asistir a determinados actos procesales. En síntesis, todas las actividades descriptas en el artículo resultan tendientes a la dilucidación de lo que se expone en la causa. Como el desarrollo de la misma lo dirige el Agente Fiscal, es quien tiene el conocimiento suficiente como para guiar la pericia y formular las preguntas que integran el cuestionario pericial, todas y cada una de las cuales el perito está obligado a

contestar. Las partes también podrán sugerir puntos de pericia, los que tendrán que ser admitidos por el Fiscal, en tanto sean distintos a los indicados por él y conducentes para el proceso.

El Art. 239 hace alusión a la conservación de los objetos, donde se determina que el órgano judicial y los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse. En caso que fuese necesario destruir o alterar los objetos analizados o si hubiese discrepancias sobre el modo de conducir las operaciones, los peritos deberán informar antes de proceder.

El deber pericial abarca las fases sucesivas de: examen, deliberación y conclusión, todas las cuales deben ser practicadas personalmente por los peritos. La eficacia probatoria del dictamen, cuando esta tarea ha sido encomendada a más de un experto, se fundamenta en la actuación conjunta de los peritos, de la cual surgirá un dictamen fundado como resultado de la deliberación plural y razonada basada en el confronto de métodos y criterios.

Con respecto a la ejecución de la pericia, en el Art. 240 del CPPC se establece que siempre que sea posible y conveniente, los peritos practicarán unidos el examen, deliberarán en sesión secreta, a la que solo podrá asistir quien la hubiera ordenado; y si estuvieren de acuerdo, redactarán el dictamen en común; en caso contrario, lo harán por separado. Los peritos de control no están obligados a dictaminar. Este artículo se refiere a la actuación conjunta de los peritos, con el fin de satisfacer dos exigencias: una es la posibilidad de que los peritos ejerzan un recíproco control sobre los métodos y procedimientos utilizados; la otra, que el dictamen sea el resultado de una discusión razonada entre los peritos, respecto de los hechos a los que se refiere la pericia.

De la actividad desarrollada pueden obtenerse resultados homogéneos que conducirán a la confección de un dictamen y conclusiones realizado en forma conjunta. Ante la diversidad de criterios, se producirán piezas separadas.

En el Art. 241 se estipula que si los informes fueren dubitativos, insuficientes o contradictorios, se podrá nombrar uno o más peritos nuevos, según la importancia del caso, para que los examinen y valoren o, si fuere factible y necesario, realicen otra vez la pericia. De igual modo podrán actuar los peritos propuestos por las partes, cuando hubieren sido nombrados después de efectuada la pericia.

En el dictamen, el experto contestará todos los puntos que integran el cuestionario pericial. Limitará su actuación a la evacuación de los puntos que hayan sido elaborados

por el Agente Fiscal en uso de las facultades instructoras otorgadas por el ordenamiento procesal penal.

“...El modo de efectuar las preguntas es tan importante como cuando se las efectúa a los testigos. Los receptores del dictamen, sin renunciar en absoluto a formarse un juicio independiente, deben hacer notar su disposición a dejarse aleccionar por quien fue llamado para emitir juicio técnico.

Se le debe permitir por lo mismo, que se explaye con libertad y continuidad, para de esta manera poder ampliar y evacuar las explicaciones sin ser sometido a un fuego cruzado que lo obligue a emitir respuestas tajantes y breves.

...Los dictámenes parten de la esfera de su experiencia profesional, aprecia los detalles desde un enfoque especializado, de allí que cuando valora los hechos, su labor no puede tener significado definitivo para la determinación del estado de los mismos.

...En las peritaciones de alta tecnicidad, se deberán aprovechar al máximo los recursos disponibles, en una orientación que deje de considerar a la justicia, sus instrumentos y métodos –por ende a los peritos– sujetos a la rigidez de normas que no por establecidas y ricas, dejan de admitir la posibilidad de ser superadas conforme a las exigencias contemporáneas.

...Despojados de toda arrogancia, los emisores-receptores evitarán caer en la omnipotencia de quien cree saberlo todo, juzgando cualquier punto con prontitud y certeza, con lo cual se eludirán las objeciones absurdas que traban la labor del operador, descartando concepciones divergentes...”<sup>(2)</sup>

En alusión a este punto, el Art. 242 advierte que el dictamen pericial podrá expedirse por escrito o hacerse constar en acta, y comprenderá, en la manera de lo posible:

- La descripción de la persona, cosa o hecho examinados, tal como hubieran sido hallados,
- Una relación detallada de las operaciones que se practicaron y de su resultado,
- Las conclusiones que formulen los peritos, conforme a los principios de su ciencia, arte o técnica, y sus respectivos fundamentos, bajo pena de nulidad,
- La fecha en la que la operación se practicó.

El primer punto fija que la pericia contendrá “...la descripción del elemento sometido a examen, lo que permite ponderar la calidad del objeto materia de estudio y las eventuales alteraciones sufridas desde su adquisición para el proceso...”<sup>(3)</sup>.

El segundo inciso hace referencia a la necesidad de que el experto detalle todas y cada una de las operaciones técnicas que –en virtud de sus conocimientos, capacidad y experiencia– desarrolló para arribar a los resultados obtenidos, los cuales también serán descritos en el cuerpo del dictamen y darán origen a las conclusiones (parte fundamental de la pericia).

El tercer ítem establece que el perito fundará las conclusiones definitivas a las que arribó, en base a las diligencias y estudios efectuados y las pruebas que surjan del expediente (que también pueden ser tenidas en consideración).

Resulta menester resaltar que el perito debe procurar que la experticia –todo el dictamen pero, especialmente, las conclusiones– resulte entendible para terceros, ajenos a su ciencia. El dictamen no debe ser una mera opinión del experto, sino que debe hallar sustento científico, de modo tal de suministrar al juez o tribunal los elementos conducentes al sostén de las conclusiones, mediante la utilización de palabras claras y convincentes que permitan su comprensión y razonamiento.

Nos resulta importante recuperar la noción de que el dictamen pericial no resulta vinculante, vale decir que si bien el Tribunal no está obligado a ceñirse estrictamente a las conclusiones del dictamen, ello no admite que pueda apartarse arbitrariamente de la opinión fundada por un perito idóneo, en cuestiones de naturaleza esencialmente técnicas, para lo cual debe brindar razones de entidad suficiente.

“..La labor pericial contribuye a aportar cierta información al sentenciante, en una actividad de asesoramiento, a los fines de facilitar la formación de una opinión fundada acerca de los puntos que fueron objeto de dictamen. Pero luego, una vez que el juez ha formado su opinión fundada, en parte pero no exclusivamente por conducto de ese asesoramiento a cargo del experto, será el magistrado quien, evaluando la prueba pericial no aisladamente sino en conjunto con la totalidad de la prueba incorporada al proceso, conforme a las reglas de la sana crítica, emitirá su juicio a partir de la convicción o certeza moral acerca del acontecer histórico de los hechos materia de juzgamiento; juicio que se concretará en la construcción de una norma individual cuyo objeto es plasmar el valor de lo justo para el caso particular, conforme al derecho vigente y a una noción de equidad.

Es decir, entonces, que al tiempo de ponderar la virtualidad probatoria de la prueba de peritos, el dictamen valdrá tanto como resulte de sus fundamentos y de la claridad de su exposición, ya que el juzgador conserva plena capacidad de establecer su fuerza convictiva mediante una tarea que supone la verificación de las proposiciones y juicios elaborados por el experto, mediante un análisis lógico-gnoseológico del dictamen que culminará a su vez en la formulación de un juicio crítico sobre la actividad probatoria así cumplida.

Aún en los procesos que versan sobre cuestiones eminentemente técnicas (...), supuestos en los que la prueba pericial reviste preponderancia innegable, el juez no se encuentra precisado a aceptar con rigidez las conclusiones periciales... No obstante, los dictámenes no podrán ser dejados de lado ligeramente, ya que la ley no autoriza a los magistrados a determinarse de un modo puramente discrecional ni según su libre convicción, pues el pronunciamiento ha de ser el resultado de un examen crítico del dictamen en su confrontación con los antecedentes de hecho suministrados por las partes y con el resto de las pruebas rendidas. Así, el apartamiento de las conclusiones periciales deberá fundarse, razonablemente, con arreglo a los preceptos de la sana crítica.

Ello, pues si bien es cierto que la ley no confiere a la prueba de peritos el carácter de prueba legal, no lo es menos que ante la necesidad de una apreciación específica del campo del saber del experto designado, técnicamente ajeno al hombre de derecho, para desvirtuarlo será imprescindible ponderar otros elementos de juicio que permitan concluir de un modo fehaciente en el error o en el inadecuado o insuficiente uso que el técnico hubiera hecho de los conocimientos científicos de los que por su profesión o título habilitante ha de suponérselo dotado; o bien en la existencia de otro u otros medios de prueba, de relevancia comparable o superior a la que en el caso revista la prueba pericial, que persuadan al juez de que las conclusiones periciales han de ser dejadas de lado.

Para decirlo de otro modo, el apartamiento de esas conclusiones deberá encontrar apoyo en razones serias, en fundamentos objetivamente demostrativos de que la opinión del experto se encuentra reñida con principios lógicos o máximas de experiencia, evidenciando la existencia de errores de entidad, o que existen en el proceso elementos probatorios de mayor eficacia para provocar la convicción acerca de la verdad de los hechos controvertidos.

De ello se colige que cabe indicar entre otros supuestos de inatendibilidad de la prueba pericial, a los casos en que, no obstante ser técnicamente correcto el dictamen, juegan otros factores que escapan a la apreciación del experto mas no a la del juzgador, quien no debe dejar de evaluarlos en procura de hallar la solución justa del caso.”<sup>(4)</sup>

“...El magistrado tiene plena libertad para valorar los resultados de la pericia e, incluso, le es dado apartarse de sus resultados motivando expresamente su resolución. El principio parte en primer término de haber sido superado el sistema de las pruebas legales (que otorgaban valor incontrastable a la pericia) y luego, dentro de esta misma línea de pensamiento, de la facultad otorgada a los jueces de valorar la prueba de acuerdo a las libres convicciones o a la sana crítica, es decir, la estimación racional de los elementos reunidos en la causa en base a criterios lógicos verificables que, por esa razón, no significan arbitrariedad por parte del juzgador sino, por el contrario, la aplicación motivada de su convencimiento acerca de la validez de la prueba.

El juez no posee un conocimiento mayor que el del perito y por lo tanto, desde el estricto punto de vista técnico-científico, no puede contradecir sus conclusiones pero puede en cambio controlar el grado de aceptabilidad del dictamen, conforme a su propia valoración; es en este sentido que puede decirse, apelando al conocido principio legal, que el juez es peritus peritorum.”<sup>(5)</sup>

Finalmente, el Art. 245 del CPPC fija que el perito deberá guardar reserva de todo cuanto conociere con motivo de su actuación. El órgano que hubiere dispuesto la pericia podrá corregir con medidas disciplinarias la negligencia, inconducta o mal desempeño de los peritos, y aún sustituirlos, sin perjuicio de las otras sanciones que puedan corresponder.

Por su parte, el CPP en el Título III – Medios de Prueba, estipula lo siguiente en materia pericial:

- En referencia a la Inspección judicial, Art. 216., advierte que el juez de instrucción comprobará, mediante la inspección de personas, lugares y cosas, los rastros y otros efectos materiales que el hecho hubiere dejado; los describirá detalladamente y, cuando fuere posible, recogerá o conservará los elementos probatorios útiles.
- Con respecto a las Operaciones técnicas, Art. 222, determina que para la mayor eficacia de las inspecciones y reconstrucciones, el juez podrá ordenar todas las operaciones técnicas y científicas convenientes.



- En alusión Orden de secuestro, Art. 231, fija que el juez podrá disponer el secuestro de las cosas relacionadas con el delito, las sujetas a decomiso o aquellas que puedan servir como medios de prueba. Sin embargo, esta medida será dispuesta y cumplida por los funcionarios de la policía o de las fuerzas de seguridad, cuando el hallazgo de esas cosas fuera resultado de un allanamiento o de una requisita personal o inspección en los términos del artículo 230 bis, dejando, constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o al fiscal intervinientes.
- En cuanto a la Custodia del objeto secuestrado, Art. 233, se establece que los efectos secuestrados serán inventariados y puestos, bajo segura custodia, a disposición del tribunal. En caso necesario podrá disponerse su depósito. El juez podrá ordenar la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la instrucción. Las cosas secuestradas serán aseguradas con el sello del tribunal y con la firma del juez y secretario, debiéndose firmar los documentos en cada una de sus hojas. Si fuere necesario remover los sellos, se verificará previamente su identidad e integridad. Concluido el acto, aquéllos serán repuestos y de todo se dejará constancia.
- Resulta importante recuperar la referencia que el Art. 236 hace a la Intervención de comunicaciones telefónicas. Allí, se indica que el juez podrá ordenar, mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedir las o conocerlas. Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él. (Párrafo incorporado por art. 7° de la Ley N° 25.760, publicada en el Boletín Oficial del 11/8/2003).

#### Principio de Libertad Probatoria

Con respecto a la labor pericial, particularmente en materia procesal, resulta importante destacar que en el proceso penal nacional rige el principio de libertad probatoria en virtud del cual y según el Art. 206 del CPP, “No regirán en la instrucción las limitaciones establecidas por las leyes civiles respecto de la prueba, con excepción

de las relativas al estado civil de las personas”, por lo que todas las evidencias serán en principio válidas, siempre y cuando no vulneren garantías constitucionales del posible afectado por aquellas. Por su parte, el CPPC en su Art. 192 indica puntualmente que todos los hechos y circunstancias relacionados con el objeto del proceso pueden ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes.

Este principio implica que para alcanzar la verdad concreta no se requiere la utilización de un medio de prueba determinado. Todos los medios de prueba son admisibles, es decir, se puede probar con los medios de prueba típicos como también con aquellos que no han sido contemplados en la ley (atípicos) siempre y cuando no recaigan en la ilicitud. Los medios de prueba, para ser admitidos, deberán referirse directa o indirectamente al ilícito objeto de la averiguación y proporcionar elementos útiles para el esclarecimiento de los hechos. Los medios de prueba deben entonces, ser lícitos y no haberse obtenido por acciones o medios prohibidos.

#### *Ley de Protección de Datos Personales*

Especial referencia haremos a dos leyes nacionales relevantes para el desarrollo de este proyecto, la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos. La Ley 25.326 de Protección de los Datos Personales fue sancionada por el Senado y la Cámara de Diputados de la Nación Argentina, reunidos en Congreso el 4 de octubre del 2000, y promulgada 30 de octubre del mismo año. Esta Ley se encuentra íntimamente ligada con el principio de Habeas Data. El Habeas data es una acción constitucional que puede ejercer cualquier persona que estuviera incluida en un registro o banco de datos, para acceder a tal registro y que le sea suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad. La frase legal se utiliza en latín, cuya traducción más literal es “tener datos presentes”. La Constitución Argentina, desde su reforma en 1994, reconoce este derecho, puntualmente en el tercer párrafo del Art. 43. “...Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística...”.

Seis años después de la sanción de la aludida norma constitucional fue promulgada la Ley 25.326, cuya normativa excede el marco del instituto del hábeas data, ya que tiene como finalidad la "protección de los datos personales". A través de sus disposiciones se establecen los principios generales relativos a la protección de los datos, garantiza a toda persona el poder de control sobre los mismos, sobre su uso y destino con el propósito de impedir su tráfico ilícito y lesivo para la privacidad y demás derechos afectados; regula los derechos de acceso, rectificación, actualización, supresión y confidencialidad; impone a los responsables de archivos, registros y bancos de datos y usuarios de datos ciertas y determinadas obligaciones en el tratamiento de datos; contempla la creación de un órgano de control y confiere marco legal a la "acción de protección de los datos personales o de hábeas data", regulación ésta que no es aplicable en la jurisdicción provincial, sino exclusivamente en el fuero federal y en el ámbito nacional.

#### Ley de Delitos Informáticos

Por su parte, la Ley 26.388 de Delitos Informáticos, fue sancionada por el Senado y la Cámara de Diputados de la Nación Argentina, reunidos en Congreso el 4 de junio del 2008, y promulgada de hecho el 24 de junio del mismo año. Esta Ley modifica el Código Penal Argentino para incluir los delitos informáticos y sus respectivas penas. Si bien la Ley no incluye una definición concreta de delito informático, podemos describirlo como un hecho ilícito que se comete mediante la utilización de medios o sistemas informáticos. Dicho de otra forma, podemos definirlo como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." <sup>(6)</sup>. Se trata de delitos ya tipificados en el Código Penal, como robo, hurto, fraude, falsificación, estafa, sabotaje pero que son cometidos a través de herramientas electrónicas o informáticas.

En su Art. 1 amplía el alcance del término "documento" (Art. 77 del CPN), incluyendo toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. En cuanto a los términos "firma" y "suscripción", estos comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Por su parte, los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Como indicamos anteriormente, la Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del CPA con figuras propias y

específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del Código Penal actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en dicho código. Como consecuencia, se tipifican (entre otros) los siguientes tipos de delitos:

- Pornografía infantil por Internet u otros medios electrónicos (Art. 128 C.P.A.);
- Violación, apoderamiento y desvío de comunicación electrónica (Art. 153, párrafo 1° C.P.A.);
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (Art. 153, párrafo 2° C.P.A.);
- Acceso a un sistema o dato informático (Art.153 bis C.P.A.);
- Publicación de una comunicación electrónica (Art.155 C.P.A.);
- Acceso a un banco de datos personales (Art.157 bis, párrafo 1° C.P.A.);
- Revelación de información registrada en un banco de datos personales (Art. 157 bis, párrafo 2° C.P.A.);
- Inserción de datos falsos en un archivo de datos personales (Art. 157 bis, párrafo 2° C.P.A.; anteriormente regulado en el Art. 117 bis, párrafo 1°, incorporado por la Ley de Hábeas Data);
- Fraude informático (Art. 173, inciso 16 C.P.A.);
- Daño o sabotaje informático (Art.183 y 184, incisos 5° y 6° C.P.A.)

## Referencias

- (1) *Santiago, Alicia Noemí*, “¿Deben los jueces valorar en forma distinta la prueba pericial?”, *La Ley* 1997- E, p. 148.
- (2) *Machado Schiaffino, Carlos A.*, “El perito y la prueba”, *Ed. La Rocca, Bs. As.*, 1988, p. 136 y ss.
- (3) *Granillo Fernández, Héctor M. y Herbel, Gustavo*, “Código de Procedimiento Penal de la Provincia de Buenos Aires”, *Ed. La Ley, Bs. As.*, 2005, p. 523.
- (4) *Ammirato, Aurelio L.*, “sobre la fuerza probatoria del dictamen pericial”, *La Ley* 1998-F, 274 – LLP 2000, p. 808.
- (5) *De Elía, Carlos M.*, “Código Procesal Penal de la Provincia de Buenos Aires”, *Ed. Librería El Foro, Bs. As.*, 2003, p. 371 y ss.
- (6) *Definición elaborada por un Grupo de Expertos, invitados por la Organización de Cooperación y Desarrollo Económico, en París, mayo de 1993.*

# **CAPÍTULO 2**

## ***NOCIONES DE INFORMÁTICA FORENSE***

### Informática Forense

El constante reporte de debilidades en sistemas informáticos y la explotación de las fallas ya sea de índole humana, procedimental o tecnológica sobre estas infraestructuras, hacen que sea un escenario tentador y casi perfecto para cultivar delitos informáticos. Quienes realizan estas acciones poseen diferentes motivaciones, alcances y estrategias que desorientan a analistas, expertos y cuerpos de especialistas de investigaciones, porque sus modalidades de ataque y penetración de un sistema a otro varían. Para hacer frente a estos ataques actualmente nos valemos de una rama de las Ciencias Forenses, la Informática Forense.

Como punto de partida, la ciencia forense nos proporciona principios y técnicas que facilitan la investigación del delito criminal, es decir, cualquier principio o técnica que pueda ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal.

Existen derivaciones dentro de las Ciencias Forenses, una de ellas es la Informática Forense. Ésta aparece como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos y para garantizar la verdad alrededor de la evidencia digital que se puede aportar en un proceso. Consiste en la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas reconstruyen el bien informático, examinan datos residuales, autentican datos y explican las características técnicas del uso aplicado a los datos y bienes informáticos.

Citando la definición de Informática Forense para el FBI, decimos que “...es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional...”<sup>(1)</sup>.

La informática forense aparece entonces, como disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos y para garantizar la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Forensia digital es una forma de aplicar conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos, de

eventos que podrían catalogarse como incidentes, fraudes o usos indebidos, bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

La relevancia de la Informática Forense radica en que es cada vez más importante esclarecer los crímenes informáticos, y más aún prevenirlos.

Esta disciplina hace uso de la última tecnología para mantener la integridad de los datos y del procesamiento de los mismos. Además requiere de especialización y conocimientos avanzados en materia de informática y sistemas, por parte de quienes se especializan en esta ciencia, para poder detectar dentro de un dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento del software y hardware, redes, seguridad, hacking, cracking, recuperación de información, etc.

Es de suma importancia resaltar que la informática forense no tiene parte preventiva, es decir, no se encarga de prevenir delitos. Para la prevención de hechos delictivos, de esta naturaleza, nos valemos de la seguridad informática.

En otras palabras, podemos decir que Informática Forense "...es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal"<sup>(2)</sup>. Ampliando el concepto, concluimos que "...es una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnico"<sup>(3)</sup>

La Informática Forense es una aplicación del método científico porque supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y medible, empleando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtiene más evidencia.

Los resultados obtenidos deben ser objetivos e imparciales, implicando un alto grado de profesionalidad para con la tarea realizada. La metodología aplicada debe ser conocida, sabida y practicada, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a las mismas conclusiones. Si esto no se logra, la posibilidad de la pérdida de la evidencia con valor probatorio es inminente con todo lo que con esto conlleva.



La Forensia Informática deberá permitir responder preguntas tales como: ¿Cuándo?, ¿Quién?, ¿Cómo?, ¿Dónde?, ¿Para qué? y ¿Por qué?.

Los usos de la Informática Forense no están ligados estrictamente a hechos informáticos, muchos de ellos provienen de la vida diaria, por ejemplo:

- **Prosecución Criminal:** Evidencia incriminatoria que puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
- **Investigación de Seguros:** La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
- **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Como toda disciplina criminalística, la Informática Forense se compone de varias especialidades, integradas bajo el mismo método, pero diferentes entre sí por sus especialidades físicas o lógicas.

Una clasificación general de la Informática Forense podría ser la siguiente <sup>(4)</sup>:

- **Computacional**
  - a) Fija.
  - b) Móvil
  - c) Integrada al atuendo (vestimenta).
  - d) De base (Sistemas Operativos).
  - e) De aplicación (programas ejecutados en un determinado sistema operativo).
- **Conectividad.**
- **Telefonía Forense**

- Sistema de Posicionamiento Global GPS.
- Archivos Documentales Digitalizados (tratamiento de imágenes, video y audio).
- Residuos Informáticos (tratamiento de residuos físicos y lógicos).

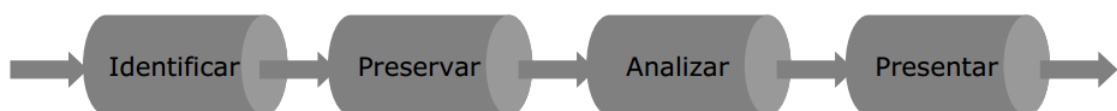
Los especialistas de las Ciencias Forenses aportan su conocimiento y entrenamiento para ayudar a los investigadores a reconstruir la escena del crimen y encontrar pistas, aplicando un método científico para analizar las evidencias disponibles. Elabora hipótesis sobre lo ocurrido para constituir la evidencia y realiza pruebas y controles para confirmar o contradecir esas hipótesis. Un forense no puede conocer el pasado, sólo dispone de información limitada del presente, por ello sólo puede presentar posibilidades basadas en la información limitada que posee.

#### Principio de Locard

Un principio muy utilizado y fundamental en la ciencia forense que cabe recuperar es el Principio de Intercambio o transferencia de Locard, (Edmond Locard, francés fundador del instituto de criminalística de la universidad de Lion). Este principio dice que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa. Es decir que se lleva consigo algo de la escena, porque cada contacto deja un rastro. Si entramos en contacto con la escena del crimen con toda seguridad dejaremos algo ahí, pelo, sudor, huellas, etc., y también nos llevaremos algo cuando abandone la escena, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

#### Metodología y fases de un análisis forense informático

Como ya hemos mencionado, la informática forense es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable.



Debido a que la adquisición de datos puede involucrar un amplio abanico de dispositivos contenedores de información, sucede que antes de comenzar con el proceso de adquisición de datos es necesario realizar un reconocimiento y una correcta documentación de los diferentes tipos de evidencia que se debe adquirir, del sistema informático que se pretende analizar y también, se debe tener en cuenta cuál es el camino del delito, ya que no es lo mismo analizar un caso de homicidio que uno de fraude, por las características inherentes a cada uno de ellos.

También es necesario, antes de comenzar con el proceso de adquisición de datos, tener en cuenta cuál va a ser la información que se debe recolectar, ya que si se decide copiar la totalidad de los datos cuando en realidad sólo se necesita una porción del conjunto, se podría incurrir en una pérdida innecesaria de tiempo, además de aumentar el riesgo a contaminar la evidencia.

Los diferentes elementos que van a ser analizados, y que son material probatorio en un proceso judicial, deben encontrarse claramente identificados con el fin de evitar la pérdida de la información. Poder identificar los diferentes elementos mitiga el riesgo de confundir los elementos que son copia de lo que es evidencia original así como también permite llevar un registro de la ubicación de cada uno de ellos.

La preservación es un proceso continuo a lo largo del proceso forense y que se encuentra entrelazado con la noción de cadena de custodia, al cual dedicaremos el próximo apartado. Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben emplear en sus labores, pues cualquier imprecisión en los mismos puede llevar a comprometer el proceso en su totalidad. Detallamos a continuación, de manera básica, algunos elementos que deben ser considerados para mantenerla idoneidad del procedimiento forense.<sup>(5)</sup>

- Esterilidad de los medios de informáticos de trabajo. Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática.
- Verificación de las copias en medios informáticos. Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual

fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. Adicionalmente, es preciso que el software u aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad científica, para que conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

- Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados. El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.
- Mantenimiento de la cadena de custodia de las evidencias digitales. Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

En cuanto a la fase de análisis, podemos distinguir la etapa de extracción de información física y la etapa de extracción de información lógica. Existen dos fases diferentes de extracción de información: la lógica y la física <sup>(6)</sup>. La diferencia radica en que la extracción física descarta los ficheros de sistema (File System). La fase de extracción lógica, sin embargo, tiene en consideración la totalidad de los archivos del

sistema, incluyendo: archivos de sistema operativo, ficheros de sistema y archivos de las diferentes aplicaciones disponibles.

*Fase de extracción de información física:*

Durante esta etapa se realiza la extracción de información del disco a nivel físico sin considerar los archivos de sistema que se encuentren presentes. Las acciones que se podrían llevar a cabo son: la búsqueda de palabras claves, búsqueda de archivos y la extracción de la tabla de particiones y de espacio del disco físico no utilizado.

Se debe tener en cuenta que:

- Realizar una búsqueda de palabras claves a lo largo del disco físico podría ser de utilidad al analista forense para extraer datos relevantes y para identificar archivos que no pertenezcan al sistema operativo.
- Utilizar herramientas en la búsqueda y extracción de archivos tiene como finalidad el encontrar ficheros que podrían no ser tenidos en cuenta por el sistema operativo y que podrían resultar relevantes en la investigación.
- Por otra parte, analizar la estructura de particiones del disco es útil para comprender e identificar la composición del sistema de archivo, pudiendo determinar si todo el espacio físico del disco duro se encuentra utilizado.

*Fase de extracción de información lógica:*

Esta etapa de extracción de información, desde un medio de almacenamiento, se encuentra centrada en el sistema de archivos y podría incluir datos como por ejemplo: áreas de archivos activos, archivos que fueron eliminados, file slack (es el espacio de almacenamiento de datos que existe desde el final de un archivo hasta el final del último clúster que tiene asignado, en otras palabras, el slack es considerado a la diferencia que existe cuando el tamaño físico de un medio de almacenamiento supera a su tamaño lógico) y el espacio en disco que aún no ha sido asignado.

Los pasos podrían incluir:

- Extracción de información de archivos de sistemas que revelen características tales como: la estructura de directorios, atributos de los archivos, nombre de archivos, fechas y horas, tamaño de archivos y ubicación de los mismos.

- La reducción de datos podría permitir identificar y eliminar archivos conocidos mediante la comparación de Hashes de archivos pre calculados en relación a los Hashes calculados de los archivos presentes en el disco.
- Extracción de archivos pertinentes a la investigación. Los métodos que se utiliza para el cumplimiento de esta tarea podrían ser basados en la búsqueda de los nombres de archivos y extensiones, revisión de los encabezados, el contenido del archivo y la ubicación de los mismos en el medio contenedor.
- Recuperación de archivos que fueron borrados.
- Extracción de archivos protegidos con contraseña, cifrados y con información comprimida.
- Extracción del file slack.
- Extracción del espacio no asignado.

En los dispositivos de telefonía móvil, además de las características mencionadas anteriormente se podrían considerar algunas adicionales, tales como <sup>(7)</sup>:

- Analizar las llamadas que hayan sido aceptadas, perdidas y/o rechazadas.
- Revisar los correos electrónicos almacenados en el dispositivo.
- Revisar los mensajes almacenados en el dispositivo (Mensajes de Voz, MMS, SMS, etc...)
- Revisar el caché del dispositivo móvil.
- Revisar las citas, notas y el calendario del dispositivo en búsqueda de eventos o de información relevante a la investigación.
- Revisar la agenda en búsqueda de números telefónicos que guarden relación con el caso.
- Analizar el historial de navegación web.
- Analizar los mapas y el sistema de navegación GPS.
- Revisar las fotografías y los videos almacenados. Adicionalmente se deberá revisar la meta data de los archivos en búsqueda de información relevante. Por ejemplo, revisarlas coordenadas podría resultar útil a fin de establecer la ubicación de dónde fueron tomadas las capturas.

Cerrando este apartado, haremos referencia a uno de los aspectos más cruciales en una investigación forense, que corresponde la producción de un informe que detalle el proceso que se ha desarrollado. El documento debe ser escrito para comunicar el resultado del análisis digital forense y deberá exponer una teoría

entendible de la investigación de forma tal que, la persona encargada de realizar un juicio sobre la misma cuente con la información necesaria de forma clara y concisa.  
(8)

La producción de informes lógicos y bien estructurados aumenta la probabilidad de convencer a un jurado de que se posee un entendimiento avanzado de lo que se está haciendo y de que la evidencia presentada ante el tribunal, es válida.

El propósito del informe es exponer hechos y la evidencia que ha sido identificada y, aunque exista evidencia que se considere que no resulta de apoyo a la investigación, debe ser mencionada de todas formas en el informe final. En el reporte además, debe constar cuál es el objetivo principal de la investigación que se ha realizado.

La confección del reporte debe ser escrito de forma lógica y ordenada, de manera tal que pueda exponer cuál es el interrogante que debe ser esclarecido, presentar los resultados de la investigación y además, declare conclusiones y recomendaciones. Para lograr una estructura lógica y centrarse en la narración del proceso, se puede proceder a la utilización de apéndices que puedan incluir calendarios, tablas u otra información relevante.

Si el informe debe ser presentado a un público variado, se debería considerar la creación de un glosario que abarque la definición de los conceptos técnicos. El glosario sirve como herramienta de apoyo a quién lo debe leer con el objetivo de subsanar dudas técnicas.

Un buen informe debe responder a: quién, qué, cuándo, dónde y por qué. Además, debe documentar qué acciones fueron realizadas durante el proceso y el porqué de las mismas <sup>(9)</sup>.

Una vez finalizadas todas las etapas de la investigación forense digital y, una vez concluido y presentado el informe a las autoridades pertinentes se debería resguardar toda información en un lugar seguro por si en algún momento futuro se decide volver a indagar en los elementos intervinientes.

### *Cadena de Custodia*

Resulta interesante a esta altura, recuperar el concepto de cadena de custodia informático forense y su preservación. Según el Tomo II del Manual de Informática Forense (Darahuge – Arellano González) la preservación de la cadena de custodia sobre la prueba indiciaria criminalística es un objetivo que afecta a la totalidad de

los miembros del Poder Judicial, los operadores del Derecho y sus auxiliares directos. Entre estos últimos debemos incluir al personal de las fuerzas de seguridad, a los policías judiciales y al conjunto de peritos oficiales, de oficio, consultores técnicos o peritos de parte.

Por esta razón establecer mecanismos efectivos, eficientes y eficaces con la tarea de preservación de la cadena de custodia a partir de métodos y procedimientos que aseguren la confiabilidad de la información recolectada, único elemento integrador a proteger a los activos informáticos cuestionados, ya que incluye la trazabilidad, la confidencialidad, la autenticidad, la integridad y el no repudio de estos, es una necesidad imperiosa para asegurar el debido proceso en cualquiera de los fueros judiciales vigentes.

En términos sencillos, implica establecer un mecanismo que asegure a quien debe juzgar que los elementos probatorios ofrecidos como prueba documental informática son confiables. Es decir, que no han sufrido alteración o adulteración alguna desde su recolección, hecho que implica su uso pertinente como indicios probatorios, en sustento de una determinada argumentación orientada a una pretensión fundada en derecho.

Se considera a la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin asegurar la inocuidad y esterilidad técnica en el manejo de dichos indicios, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.

Para asegurar estas acciones es necesario establecer un detallado y riguroso registro, que identifique la evidencia y su posesión, con una razón que indique lugar, hora, fecha, nombre y dependencia involucrada, en el secuestro, la interacción posterior y su depósito en la sede que corresponda.

Desde la detección, identificación, fijación, recolección protección, resguardo, empaque y traslado de la evidencia en el lugar del hecho real o virtual, hasta la presentación como elemento probatorio, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena es la misma que se está presentando ante el evaluador y/o decisor. Es importante destacar que el procedimiento se caracteriza por involucrar múltiples actores, los que deben estar profundamente consustanciados de su rol a cumplir



dentro de este, sus actividades a desarrollar durante la manipulación de la prueba y sus responsabilidades derivadas.

La prueba documental informática consiste en indicios digitalizados codificados y resguardados en un contenedor digital específico. La información puede estar en uno de los siguientes estados: almacenada, cuando se encuentra en un reservorio a la espera de ser accedida, en desplazamiento, que implica que está viajando en un elemento físico determinado y es susceptible de recolección por medio de la interceptación de dicho elemento y finalmente, en procesamiento.

Es menester en este punto, considerar que un bit es exactamente igual a otro bit. De ahí que una copia bit a bit de un archivo digital es indiferenciable de su original. Esto no resulta un inconveniente sino una ventaja, desde la perspectiva de la cadena de custodia, ya que permite preservar las copias, manteniendo el valor probatorio del original y evitando riesgos para este. La recolección de prueba mediante copia debidamente certificada puede sustituir perfectamente al original. Los mecanismos de certificación digital (hash, firma electrónica, firma digital) son mucho más confiables y difíciles de falsificar que los mismos elementos referidos a la firma y certificación ológrafas.

La cadena de custodia informático forense tiene por objeto asegurar que la prueba ofrecida cumple con los requisitos exigibles procesalmente, lo que implica que debe asegurar:

- Trazabilidad:
  1. Humana: determinación de responsabilidades en la manipulación de la prueba, durante todo el ciclo de vida del análisis
  2. Física: incluyendo la totalidad de los equipos locales o remotos involucrados en la tarea, sean estos de almacenamiento, procesamiento o comunicaciones.
- Lógica: descripción y modelización de las estructuras de distribución de la información accedida y resguardada.
- Confiabilidad: integridad, autenticidad, confidencialidad, no repudio.

Extraído del manual de informática forense.

La informática forense como especialidad dentro de la criminalística debe incluir los requisitos generales establecidos en la inspección judicial en criminalística. En esta especialidad los elementos dubitados pueden ser del tipo físico o virtual. En el caso de

los elementos virtuales la detección, identificación y recolección deberá efectuarse en tiempo real, es decir en vivo, con el equipo encendido. La información es un elemento intangible que se encuentra almacenado en dispositivos que pueden ser volátiles o no. Con el fin de determinar la validez de la información contenida en los mencionados dispositivos será necesario efectuar la correspondiente certificación matemática por medio de un digesto o hash. Esta comprobación es la que permitirá posteriormente determinar la integridad de la prueba recolectada y su correspondencia con el elemento original.

En síntesis, se deberá mantener la seguridad, procurar el resguardo legal y aplicar una metodología estricta.

### Evidencia digital

La evidencia digital es "cualquier información, que sujeta a una intervención humana u otra semejante que ha sido extraída de un medio informático". En este sentido, el término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal"<sup>(10)</sup>. La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso.

A diferencia de la documentación tradicional en papel, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otra característica única de la evidencia digital es el potencial de realizar copias no autorizadas de archivos, sin dejar huellas ni rastros de que se realizó una copia.

Cuando un infractor ha generado un delito, éste intenta manipular y alterar la evidencia digital tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, en la actualidad este problema es aminorado con algunas características que posee este tipo de evidencia. Ésta puede ser duplicada de forma exacta bit a bit, y esa copia es factible de ser examinada como si fuera la original. Esta práctica se emplea con el fin de no manipular los originales y evitar el riesgo de dañarlos.

En la actualidad, con las herramientas existentes es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada. La evidencia de digital es muy difícil de eliminar. Cuando un registro es borrado del disco duro de la computadora, y éste ha sido formateado, todavía es posible recuperarla. Cuando las personas involucradas en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

La evidencia digital se puede clasificar en tres categorías <sup>(11)</sup>:

- Registros generados por computador: estos registros son aquellos, que como su nombre lo indica, son generados como efecto de la programación de una computadora. Los registros generados por computadora son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.
- Registros no generados sino simplemente almacenados por o en computadoras: estos registros son aquellos generados por una persona, y que son almacenados en la computadora, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.
- Registros híbridos que incluyen tanto registros generados por computadoras como almacenados en los mismos: los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

No debemos dejar de mencionar los cuidados que se han de tener en cuenta con respecto a la manipulación de la evidencia digital. Los requisitos que se deben cumplir son:

- Hacer uso de medios forenses estériles (para copias de información)
- Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
- Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.
- Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.

- Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas las acciones tomadas con respecto a ella, mientras esté en su poder.
- Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital serán quienes deben garantizar el cumplimiento de los principios anteriores.

Para la gestión de la evidencia digital existen gran cantidad de guías y buenas prácticas que nos indican cómo realizarla. Las guías tienen como objetivo identificar evidencia digital con el fin de ser usada dentro de una investigación. Estas guías se basan en el método científico para concluir o deducir algo acerca de la información.

### Prueba y evidencia

Pero al hablar de evidencia no debemos dejar de lado el concepto de prueba, precisamente de prueba informática. Entendemos que los términos evidencia y pruebas no deben utilizarse como sinónimos, pues no son lo mismo.

Evidencia es la categoría absoluta que no admite dudas, la certeza clara y manifiesta de la verdad o realidad de algo, mientras que prueba se define como la forma, argumento, instrumento y otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo; como el indicio, señal o muestra que se da de algo.

Según el Diccionario Panhispánico de Dudas <sup>(12)</sup>, el empleo indiscriminado en español de la palabra evidencia como sinónimo de prueba o de indicio, se debe al calco censurable del inglés evidence. En inglés, evidence es toda prueba (circunstancial, testimonial, material, documental, etc.) que se alega en un proceso judicial. En cambio en español, solo sería aceptable como sinónimo de prueba evidente, esto es, prueba clara y manifiesta.

La prueba documental informática es una especie de género de prueba documental clásica. Definimos como prueba documental clásica a la que se constituye mediante documentos. Un documento se define como una cosa, con función representativa de hechos. En síntesis, una prueba documental clásica es toda representación material destinada e idónea para reproducir cierta manifestación del pensamiento; todo objeto producto de un acto humano que represente a otro hecho u objeto; es un objeto material originado por un acto humano, susceptible de representar por sí mismo y para el futuro un hecho o una serie de hechos percibidos en el momento de su concepción.

La diferencia entre prueba documental clásica y prueba documental informática se refiere al soporte de las mismas. En la clásica, el soporte consiste en papel o elementos contenedores analógicos, como por ejemplo películas, papel, cintas, etc. En cambio, el soporte de la prueba documental informática se caracteriza por la digitalización de sus componentes y su resguardo en medios aptos para esta (soporte magnético u óptico).

Entre las características más sobresalientes de este tipo de prueba, podemos mencionar <sup>(13)</sup>:

- Principio de identidad atípico. Siempre es posible identificar entre el original y la copia de un documento en soporte de papel. En cambio, en el caso de copia digital de un archivo, estos son inidentificables, ya que un bit es idéntico a otro y la suma de bits componen ambos archivos, que se constituyen en dos originales indistinguibles.
- Posibilidad de modificación por medios locales o remotos, accidentales, culposos o dolosos.
- Divisibilidad del documento. Esta característica es más fácil de comprender por medio de un ejemplo: dos comerciantes intercambian mensajes de correo electrónico, uno de ellos con una oferta y el otro con la respuesta a la aceptación de la oferta por parte del primero. De esta manera se ha conformado un contrato comercial. En cierto momento una de las partes, toma el mensaje de su interlocutor y lo modifica, agregándole o quitándole texto. En el momento del reconociendo por parte del supuesto autor del mensaje, este no puede ni debe impugnar la totalidad del mensaje, sino únicamente la parte que fue modificada y que no coincide con sus propios resguardos de información.
- De la misma forma que el Código de Procesal Penal de la Provincia de Córdoba establece la subsidiariedad automática de la pericia caligráfica, respecto a la prueba documental clásica, la prueba documental informática lleva implícita la prueba pericial informático forense, para el caso de negativa (Se define como Prueba Pericial a la suministrada por un tercero que a raíz de un encargo judicial a uno o varios testigos expertos, que fundados en los conocimientos científicos o prácticos que poseen, comunican al juez las comprobaciones, opiniones o deducciones extraídas de los hechos sometidos en su dictamen). De manera frecuente requiere de

su convalidación mediante una prueba de informes (medio para aportar al proceso datos sobre hechos concretos, claramente individualizados y controvertidos, que resulten de la documentación, archivos o registros de terceros o de las partes).

### *Roles y responsabilidades del Perito Informático*

Particularmente el Perito Informático Forense o Perito Auditor Forense es un profesional que cuenta con conocimientos especializados referidos a las nuevas tecnologías, y que a través de su capacitación y experiencia, suministra información u opinión fundada a profesionales, empresas y a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen.

El perito informático es el encargado de analizar los diferentes elementos informáticos, y buscar aquellos datos que puedan constituir la evidencia digital que servirá, de manera decisiva, para el esclarecimiento del litigio al que ha sido asignado en un proceso legal, solucionando los aspectos y conocimientos que el juez o los tribunales desconocen y no están obligados de conocer. Puede ser nombrado judicialmente y propuesto por una o ambas partes, ambos ejercen la misma influencia en el juicio.

Brevemente podemos mencionar que entre sus funciones se encuentra la de asesorar, emitir informes judiciales o extrajudiciales, a partir de sus conocimientos científicos y técnicos en su papel del de auxiliar de Magistrados, Jueces, Abogados, Tribunales, etc. Se lo define como un auxiliar de la justicia que tiene como tarea principal la de asesorar al juez respecto a temas relacionados con la informática.

En el ámbito jurídico, el Perito Judicial Informático es un profesional nombrado por la autoridad del proceso, a fin de que mediante juicio científico-técnico, dictamine con veracidad e imparcialidad, opinando y emitiendo conclusiones sobre puntos concretos relacionados con hechos o circunstancias, sus causas o efectos, para cuya apreciación son indispensables conocimientos especializados.

La obtención de información digital (evidencias electrónicas) es lo primordial para lograr el éxito de en una investigación criminal, aspecto que demanda de los Peritos Informáticos encargados de la recolección preservación, análisis y presentación de las evidencias digitales un eficaz trabajo que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal.

El objetivo del Perito Informático es la de recuperar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal. El perfil del Perito debe ser técnico, con amplios conocimientos legales y con una formación universitaria en derecho procesal civil, penal, administrativo, laboral que le permitirá desarrollar su tarea sin que la misma sea descalificada o impugnada durante su presentación judicial. Tiene que ser experto y tener conocimientos forenses, de investigación legal y criminalística; siendo de vital importancia que esté familiarizado con las pruebas electrónicas. Se le exige además de su formación, la adquisición de habilidades técnicas y científicas usando un lenguaje científico que permita que al que no posee el entendimiento en esta ciencia pueda comprender el hecho.

El dictamen del Perito Judicial Informático es una declaración de ciencia que debe sustentarse en reglas probadas, lógicas y verificadas, y ha de valerse de los procedimientos técnicos forenses en medios electrónicos que fortalecen y desarrollan una línea de investigación forense en informática.

Las tareas a desarrollar por el perito informático no varían en demasía de la de otros peritos judiciales. Él debe recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada.

Entre sus deberes podemos mencionar:

- Aceptar el cargo que le es asignado.
- Colaborar con el resto de los peritos o consultores técnicos.
- Declarar ante el juez, en el caso de que este lo requiera.
- Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas.
- Respetar el código de ética que le impone su profesión.

Las áreas de su actuación son:

- Propiedad industrial: espionaje y/o revelación de secretos.
- Acceso o copia de ficheros de la empresa, planos, fórmulas, costes,
- Uso de información: Competencia desleal de un empleado.
- Vulneración de la intimidad. Lectura de correo electrónico.
- Despido por causas tecnológicas.

- Valoraciones de bienes informáticos.
- Interceptación de telecomunicaciones.
- Protección de datos personales y datos reservados de personas jurídicas.
- Apoderamiento y difusión de datos reservados.
- Manipulación de datos o programas.
- Hardware, redes y componentes (todos los sistemas).
- Instalaciones y desarrollos llave en mano.
- Vulneración de la buena fe contractual.
- Publicidad engañosa, competencia desleal.
- Delitos económicos, monetarios y societarios.
- Delitos contra el mercado o contra los consumidores.
- Delitos contra la propiedad intelectual.
- Uso de software sin licencia.
- Piratería. Copia y distribución no autorizada de programas de ordenador.
- Daños mediante la destrucción o alteración de datos.
- Sabotaje.
- Estafa, fraudes, conspiración para alterar el precio de las cosas.
- Pornografía infantil: acceso o posesión, divulgación, edición.
- Uso indebido de equipos informáticos: daños o uso abusivo.

Sin duda, el Perito Judicial Informático, será el profesional más demandado por una sociedad cada vez más tecnológica y la prueba electrónica es reina en la investigación criminal actual.

### Cibercrimen

Si bien la labor forense informática es aplicable en el esclarecimiento de prácticamente cualquier tipo de delito, resulta importante hacer mención especial al cibercrimen.

Sin lugar a duda, la delincuencia informática constituye uno de los máximos exponentes de las nuevas realidades delictivas. Cada día se hace más evidente que el desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables.



Es necesario efectuar una serie de consideraciones acerca de lo que se entiende por delincuencia informática o cibercrimen (término empleado por el Convenio del Consejo de Europa sobre el Cibercrimen, de 8 de noviembre de 2001). La delincuencia informática está constituida por el conjunto de actos (punibles o dignos de incriminación) en los cuales el ordenador o computadora (o el procesamiento automatizado de datos) es el instrumento o el objeto de la comisión. En definitiva, se trata de poner de manifiesto que los denominados delitos informáticos tanto pueden manifestarse en conductas orientadas a incidir ilícitamente en el instrumental informático (que sería el objeto material del delito) como en aquellas que se sirven de medios informáticos para cometer diversos tipos de delitos (desempeñando en este caso, el papel de medio o instrumento del delito).

La delincuencia informática no sólo ha generado la necesidad de hacer frente a nuevas modalidades delictivas en relación con delitos clásicos sino también, de abordar el tratamiento de nuevas conductas en lo que se refiere a los resultados, como a los medios de comisión.

La fenomenología delictiva conjuntamente con la informática aparece en el horizonte penal actual constituyendo una problemática a la que se debe dar respuesta tanto sustantiva como procesalmente. Prueba de tal necesidad es el voluminoso catálogo de delitos encuadrables dentro de una u otra modalidad de delincuencia informática: estafa y fraudes informáticos, daños informáticos, contra la propiedad intelectual, contra la libertad e indemnidad sexual (difusión de pornografía, exhibicionismo), contra la intimidad (sniffers, hacking), etc. Un catálogo en constante ampliación y concreción típica.

Para entender mejor de que se trata cuando hablamos de cibercrimen o ciberdelincuencia, vamos a citar características generales de este hecho.

La primera característica es la referida al autor del hecho delictivo. Los medios informáticos, por su carácter técnico y de especiales particularidades (velocidad, permanencia, etc.) suponen un importante factor criminógeno que, respecto al autor del hecho, éste se manifiesta en la facilitación de la conducta delictiva y en una situación cualificada del mismo, ya que los conocimientos necesarios para realizar las conductas ilícitas requieren un especial grado de especialización. Pero además están quienes, a causa de su ocupación profesional, viven en contacto directo con los recursos informáticos y por ende, tienen mayores facilidades para cometer este tipo de delitos, relacionados con el uso de la informática. En cuanto a lo que respecta a propiedades

técnicas, éstas son las comunes a cualquier labor que se desarrolle empleando medios informáticos: gran capacidad de almacenamiento de datos, velocidad, rapidez y exactitud en las operaciones, flexibilidad en las aplicaciones, permanencia y automatismo, etcétera. Todo ello combinado permite que las conductas criminales se perpetren de forma reiterada, ágil y rápida, con unas consecuencias sumamente perjudiciales para la sociedad toda.

Con respecto a los daños que ocasionan, estos se caracterizan por su eventualmente elevada dimensión y la derivada capacidad de expansión de los mismos.

En referencia a las propiedades de las características del cibercrimen en el acto de ejecución de hechos delictivos, podemos mencionar las siguientes repercusiones procesales:

- En primer lugar, dichas conductas no dejan "huellas" tradicionales (vestigios materiales de la actividad delictiva como huellas dactilares, restos de ADN, etc.) sino "huellas electrónicas", que revisten gran complejidad y un carácter sumamente novedoso.
- Aunque el rastreo de los pasos seguidos en la ejecución de la actividad ilícita es posible en muchas ocasiones, se ve entorpecido por su inserción en una combinación de miles de procesos informáticos llevados a cabo diariamente. Por otra parte, se trata de procedimientos de investigación de carácter muy técnico, y es necesario expertos en la materia, lo que genera costos altos.
- Por otra parte, la condición de especialistas de quienes cometen los ilícitos les permite borrar o dificultar el seguimiento de las actuaciones practicadas para la ejecución del delito, con lo que, a la ya tradicional complejidad de la investigación se agrega el extra de complicación.
- A todas estas notas (dificultad de rastreo, borrado de las huellas, etc.) se le suma el propio carácter impersonal que implica el recurso informático y, en particular, a Internet, que facilita el anonimato del infractor, en ocasiones hasta el punto de hacer indeterminable su identidad.
- Debemos también mencionar a la proveedora del servicio informático. Las repercusiones que generan para el proceso penal la presencia de un intermediario de carácter privado o administrativo (como son los proveedores de telecomunicaciones), sin cuya participación resultaría

imposible efectuar el intercambio de información preciso. La investigación de estos delitos se enfrenta con un tercero en discordia cuya colaboración es necesaria para la labor investigadora.

Igualmente trascendente es el carácter transfronterizo de los procesos informáticos. Consecuencia de la globalización y las nuevas tecnologías, esto permite cometer los hechos delictivos en diversos países simultáneamente, por organizaciones delictivas radicadas en diferentes estados y con cientos de integrantes. Este fenómeno obliga a una actuación solidaria por parte de las autoridades de los distintos países afectados (origen de la necesidad de una armonización legislativa o, al menos, de una cooperación policial y judicial articulada a un nivel supranacional). En síntesis, la delincuencia informática presenta como rasgos agregados a la complejidad técnica, su carácter supranacional y favorable a la ejecución por parte de organizaciones criminales.

- Particularmente procesal es la problemática relacionada a la preservación de la prueba a ser utilizada en el juicio oral. La dificultad de esta preservación está dada por el carácter volátil de algunos datos informáticos, lo que facilita considerablemente su eliminación.
- La investigación de las conductas encuadradas en la delincuencia informática está muy relacionado con el derecho a la intimidad y al secreto de las comunicaciones de los ciudadanos y obliga a tener un especial cuidado en la realización de las indagaciones necesarias de forma que no se cuestione el respeto a los derechos citados.

A esta altura, consideramos necesario articular el concepto de Cibercrimen con el de Informática Forense. Cuando se comete un cibercrimen, la información queda almacenada, en la mayoría de los casos en forma digital, lo que genera un gran problema. Las computadoras guardan la información del crimen de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, y es allí donde se debe empezar a manipular mecanismos diferentes a los tradicionales. Con ello surge el uso y estudio de la computación o informática forense como una ciencia de apoyo a situaciones que requieren atención legal.

Resaltando el carácter científico de la Informática Forense, ésta tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método

científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

## Referencias:

<sup>(1)</sup> Noblett, Michael G. "Recovering and Examining Computer Forensic Evidence". Año 2000. Disponible en: <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm>

<sup>(2)</sup> <sup>(3)</sup> Gómez, Luis Ángel Ingeniero, Segundo Comandante, jefe de División Seguridad Informática, Gendarmería Nacional Argentina. "La informática forense, una herramienta para combatir la ciberdelincuencia.". Disponible en: <http://www.minseg.gob.ar/node/1050>

<sup>(4)</sup><sup>(13)</sup> Darahuge, María Elena, Arellano González Luis E. "Manual de Informática Forense II. (Prueba Indiciaria Informático Forense)". Ed. Errepar. Primera Edición. Año 2012.

<sup>(5)</sup> Jeimy J. Cano, Ph.D, CFE. "Introducción a la informática forense". Disponible en: <http://www.estudiocriminal.com.ar/media/Introduccion%20a%20la%20Informatica%20Forense.pdf>

<sup>(6)</sup> Messina, Mariano. "Aplicabilidad metodológica de la informática forense en la obtención de resultados eficientes en procesos judiciales argentinos". Trabajo de Investigación, Universidad del Salvador, Argentina. Año 2012.

<sup>(7)</sup> EC-Council (2010). "Investigating Wireless Networks and Devices". Disponible en: [http://news.asis.io/sites/default/files/Computer\\_ForensicsInvestigating\\_Wireless\\_Nets.pdf](http://news.asis.io/sites/default/files/Computer_ForensicsInvestigating_Wireless_Nets.pdf)

<sup>(8)</sup>The National Center for Forensics Science (2003). "Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation". Disponible en: [http://www.classstudio.com/scaltagi/papers/grad\\_papers/forensics/Palmer/digital\\_evidence\\_in\\_courtroom.pdf](http://www.classstudio.com/scaltagi/papers/grad_papers/forensics/Palmer/digital_evidence_in_courtroom.pdf)

<sup>(9)</sup> Kleiman, Dave. "The Official CHFI Exam 312-49 Study Guide for Computer Hacker Forensics Investigators". Año 2007

<sup>(10)</sup> Ajoy Ghosh. "Guidelines for the Management of IT Evidence". Año 2003. Disponible en: <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf>

<sup>(11)</sup> *Cano Martines Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. “Evidencia Digital: contexto, situación e implicaciones nacionales”. Año 200. Disponible en:*

*<http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/Na sTecnologias6.pdf>*

<sup>(12)</sup> *El Diccionario panhispánico de dudas (DPD). Se puede consultar aquí: <http://www.rae.es/recursos/diccionarios/dpd>*

*Da respuesta, desde el punto de vista de la norma culta actual, a las dudas lingüísticas más habituales (ortográficas, léxicas y gramaticales) que plantea el uso del español.*

# **CAPÍTULO 3**

## ***NORMATIVA***

## ***INTERNACIONAL***

### Convenio de Budapest

Se conoce informalmente como Convenio de Budapest al Convenio sobre la Cibercriminalidad hecho en Budapest, en el seno del Consejo de Europa. Este es el primer y único tratado internacional que tiene por objetivo afrontar a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

Referente a los Estados que forman parte del convenio, en la actualidad, tan sólo treinta Estados han ratificado el Tratado, de un total de cuarenta y seis firmas. Estos países son los miembros del Consejo de Europa: Bélgica, Dinamarca, Francia, Irlanda, Italia, Luxemburgo, Holanda, Noruega, Suecia, Reino Unido, Grecia, Turquía, Islandia, Alemania, Austria, Chipre, Suiza, Malta, Portugal, España, Liechtenstein, San Marino, Finlandia, Hungría, Polonia, Bulgaria, Estonia, Lituania, Eslovenia, República Checa, Eslovaquia, Rumania, Andorra, Letonia, Albania, Moldavia, Macedonia, Ucrania, Rusia, Croacia, Georgia, Armenia, Azerbaiyán, Bosnia-Herzegovina, Serbia, Mónaco y Montenegro. El Consejo de Europa es la más antigua de las organizaciones que persiguen los ideales de la integración europea, y es asimismo la única que integra en su seno a todos los Estados europeos, con la salvedad de Bielorrusia, Kazajistán y la Ciudad del Vaticano, excluidos por ser sus regímenes políticos incompatibles con los principios que sustentan la pertenencia al Consejo. Tienen el estatus de observadores la Santa Sede y cinco estados no europeos: los Estados Unidos, Canadá, Japón, Israel y México.

El Convenio de Budapest y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de ese mismo mes se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron.

El 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre Cibercrimen entró en vigor. Los Estados que han ratificado el Protocolo Adicional son necesarios para penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como de las amenazas racistas y xenófobas e insultos.

El tratado señala los delitos informáticos en los siguientes grupos, y define los tipos penales que han de considerarse para cada uno ellos:



- Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Según el Dr. Rodríguez Bernal, destacado penalista español, los hitos fundamentales en la creación del Tratado centran las bases en 1983, cuando un grupo de expertos se reúne y recomienda a la Organización para la Cooperación y Desarrollo Económico (de ahora en más OCDE) la necesidad de armonización en los delitos informáticos. Tres años después esto se materializa en un informe. A partir de entonces el Consejo de Europa toma la iniciativa, y en 1989 publica la Recomendación nº 89, mostrando la tendencia que nos llevará al Convenio de Budapest.

En 1997 se inician las negociaciones para la elaboración del Tratado propiamente dicho. El Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, influirá decisivamente en el contenido de éste. Existieron treinta versiones del proyecto antes de llegar al definitivo.

En 2000, se reúnen en Marsella, los ministros de Justicia e Interior de la Unión Europea, y éstos deciden volcarse en la labor del Consejo de Europa, dejando a éste la elaboración final del Tratado.

Finalmente, el comité del Consejo encargado de redactar el proyecto alcanza un consenso y se publica el “Proyecto de Convención sobre el Delito Cibernético” el 27 de abril de 2000. El Comité de Ministros aprueba finalmente el proyecto el 8 de noviembre de 2001, y es abierto a la firma en día 23 del mismo mes.

Si nos referimos a la estructura del Convenio, el mismo consta de 48 artículos y un preámbulo inicial. Posee cuatro capítulos, divididos en secciones y títulos.

- El primer capítulo comprende un precepto, referido a la terminología usada en el texto.
- El segundo capítulo, titulado “Medidas que deberán adoptarse a nivel nacional”, incluye elementos tanto de Derecho material (responsabilidad

penal, tentativa, complicidad, etc.) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción, etc.).

- El tercer capítulo se refiere acerca de la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7.
- El cuarto capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

La totalidad del Tratado, en lo referido a preceptos de aplicación material, se puede dividir, conceptualmente, en dos partes:

- Derecho Penal Internacional, constituido por las disposiciones 2 a 13.
- Derecho Procesal Penal Internacional, en los artículos 14 a 35.

En el preámbulo, se reconoce el principal objetivo del Convenio “aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional”. Además fomenta el interés por intensificar la cooperación internacional para “una lucha efectiva contra la ciberdelincuencia, en materia penal reforzada, rápida y operativa”. Subraya que “el presente Convenio pretende completar dichos Convenios (en referencia a acuerdos de cooperación en materia penal) con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos...”.

El Convenio de Cibercriminalidad persigue básicamente tres objetivos en torno a los cuales se estructura:

- Armonizar el Derecho Penal material.
- Establecer medidas procesales o cautelares adaptadas al medio digital.
- Poner en funcionamiento un régimen rápido y eficaz de cooperación internacional.

Se definen en el Convenio, los siguientes delitos: acceso ilícito, interceptación ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos.

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que estipula que cualquier publicación de propaganda racista y xenófoba a través de redes informáticas es una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.

Siguiendo con el tema del Cibercrimen, y considerando como primordial la actuación de nuestro país frente a este tema, nos abocamos a mencionar la adhesión de Argentina al Convenio de Budapest. Dicha adhesión se realizó en el marco de la quinta Conferencia Anual sobre Cibercrimen del Consejo de Europa, llevada a cabo entre el 23 y el 25 de marzo de 2010, en Estrasburgo. Fue allí donde el Subsecretario argentino de Tecnologías de Gestión, Eduardo Thill, encabezó la delegación argentina que participó de la conferencia. En la conferencia se dieron cita más de 300 expertos en delitos informáticos de más de 60 países, y fue inaugurada por la Secretaria General del Consejo de Europa, Maud de Boer-Buquicchio. En dicha confederación el Subsecretario Thill manifestó la adhesión de nuestro país a la Convención de Budapest sobre Cibercrimen.

Al ser los cibercrimen a gran escala de carácter transnacional, como las redes de pedofilia o de lavado de dinero, la Convención de Budapest brinda un marco veloz y seguro, de cooperación y colaboración internacional para la persecución de estos delitos. La participación de Argentina en ella permite la cooperación de fuerzas de los distintos países y el asesoramiento de expertos técnicos.

La adhesión de Argentina a la Convención de Budapest (de ahora en más, CB) se enmarca en las políticas del país en temas referidos a los delitos informáticos, como la Ley Habeas Data y la Ley 26.388 de Reforma del Código Penal, que incorpora la tipificación de delitos informáticos, y que fuera aprobada en junio de 2008. En ella se reconoce la validez de los documentos y las firmas digitales como equivalentes a los

documentos en cualquier otro soporte, a la vez que se reconoce la privacidad e inviolabilidad del correo electrónico, colocándolo a la misma altura que el correo epistolar. Asimismo, prevé sanciones para los delitos que se cometan por medio de las TIC's.

*Articulación del Convenio de Budapest con la normativa legal argentina <sup>(1)</sup>*

A continuación realizaremos una revisión del encaje del Convenio con la norma penal vigente de nuestro país (Código Penal Argentino, CP), de todos los artículos y apartados; con excepción de las secciones interpretativas o referidas a cuestiones accesorias, como las reservas, a no ser que éstas contengan elementos de interés.

Un encaje coherente significará dos cosas: la ausencia de problemas en lo referente a la ratificación y cumplimiento del tratado, y la prueba del grado adaptación del Derecho local al plano internacional en el tema de ciberdelitos. Si en caso contrario se encuentra alguna distinción, será necesario una modificación en la normativa estatal y una reserva al Convenio sobre Cibercriminalidad.

En primer lugar, respecto al Derecho Procesal Penal presente en el convenio, los artículos 2, 3, 4, 5, 7, 8, 10, 11 y 12 del Convenio sobre la Cibercriminalidad no presentan obstáculos, pues se encuentran contemplados por el Código Penal Argentino en distintos preceptos.

El Art. 2 del CB fija respecto al acceso ilícito lo siguiente: “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.” Dicho artículo está contenido en el Art. 153 bis del CP, el cual fija que será reprimido con prisión el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

El Art. 3 del CB establece que “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas

procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.” Dicho artículo está incluido en el segundo inciso del Art. 153 del CP, que establece como delito el interceptar o captar comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

Los Art. 4 y 5 del CB contemplan dos variantes de lo que conocemos como daños informáticos. El Art. 4, en referencia a la interceptación ilícita dispone que:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

El Art. 5, por su parte, y en alusión a la interferencia en el sistema, dispone que “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.”

En principio ambos artículos citados serían reconducibles al Art. 183 del CP donde se indica que será reprimido con prisión el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos.

El Art. 7 del CB alude a la falsificación informática y ordena que “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal”. Dicho artículo figura contenido principalmente en el Art. 255 del CP, que hace referencia a la pena aplicable a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la

autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público, y en el anteriormente citado Art. 183 del CP.

El Art. 8 del CB se refiere al fraude informático, puntualmente decreta que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

- a) cualquier introducción, alteración, borrado o supresión de datos informáticos;
- b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

El apartado «a» entra dentro del mencionado Art. 183 del CP. Por su parte, el apartado «b» queda contenido en el Art. 173 inciso 16 del CP: “el que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos”, como un caso especial de defraudación.

No aparecen las conductas del Art. 10 del CB, que hace alusión a delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, en el Código Penal Argentino, pero no existen mayores inconvenientes si tenemos en cuenta que la Ley 11.723 – Régimen Legal de la Propiedad Intelectual, prevé dichas acciones en el Art. 71 y sucesivos: “el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley”.

No existen problemas con respecto al Art. 11 (Tentativa y Complicidad) del CB, si tomamos en cuenta los Art. 45 y 46 del CP: “los que tomasen parte en la ejecución del hecho o prestasen al autor o autores un auxilio o cooperación sin los cuales no habría podido cometerse”, “los que cooperen de cualquier otro modo a la ejecución del hecho y los que presten una ayuda posterior”; y el Art. 42 del CP: “el que con el fin de cometer un delito determinado comienza su ejecución, pero no lo consuma por circunstancias ajenas a su voluntad, sufrirá las penas determinadas en el artículo 44”.

Por último, el artículo 12 (Responsabilidad de las personas jurídicas) del CB no se refiere exclusivamente a las normas penales, sino también a la posibilidad de establecer responsabilidad a las personas jurídicas a través de las vías civil y administrativa, por lo que a priori, parece poseer encaje en el ordenamiento argentino.

Sin embargo, refiriéndonos al Derecho Sustantivo, los artículos 6 y 9 generan preocupaciones de mayor índole. Resulta menester recuperar ambos artículos para desarrollar el concepto.

#### Artículo 6 - Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
  - a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
    - i. un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;
    - ii. una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5;
  - b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o a.ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.
2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.
3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta,

la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

El conflicto se presenta ya que ni el apartado 1.a).ii ni el 1.b) se hallan comprendidos en la ley penal. Dado el importante problema que supone para la adhesión de Argentina al Convenio sobre la Cibercriminalidad, la doctrina ha realizado una interpretación más relajada del apartado 1.a).ii entendiendo que se articula en el Art.173 inciso 16 del CP (citado anteriormente), como un caso especial de defraudación. En primer lugar, el apartado 1.a).i, podría encajar en el Art. 183 del CP, “el que [...] vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños”. En cuanto al apartado 1.b), la posesión de diversos elementos informáticos para cometer alguno de los delitos enunciados, no se haya tipificado en el Código Penal, lo cual podría superarse haciendo uso de la reserva descrita en el apartado tercero del mismo artículo.

#### Artículo 9 - Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
  - a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
  - b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
  - c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,
  - d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
  - e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.
2. A los efectos del anterior apartado 1, por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de:
  - a) un menor comportándose de una forma sexualmente explícita;
  - b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
  - c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.



3. A los efectos del anterior apartado 2, por menor se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.
4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

En cuanto al Art. 9, los problemas pueden corregirse con la simple reserva de los apartados «d» y «e». Este Art. encaja con el Art. 128 del CP: “el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales [...] el que tuviere en su poder representaciones de las descritas en el párrafo anterior con fines inequívocos de distribución o comercialización”. Queda expuesto que la simple tenencia de material pornográfico infantil no constituye delito en la República Argentina.

Respecto al Derecho Procesal Penal, la reglamentación del convenio no plantea demasiados problemas. Los artículos 14 a 21 Convenio de Budapest, relativos a los datos informáticos, son aceptables en el orden argentino, dando por sentado que la “autoridad” a la que se refieren estos mandatos, capaz de afectar los derechos individuales (Art. 18 y 19 de la Constitución Argentina), debe ser judicial.

El Art. 22 del CB referido a la jurisdicción, plantea ciertas dificultades. En particular existen inconvenientes con el apartado 1.d): “por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo”. Este artículo afirma el principio de personalidad como criterio de atribución de jurisdicción. Argentina emplea, sin embargo, un criterio de personalidad más restringido: “delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo” (Art. 1 inciso 2 del CP).

A priori, no generan problemas los artículos 24 a 33 del CB. Las disposiciones de los artículos 28 y 32 del CB se pueden enmarcar dentro de la Ley de Protección de Datos de Personales.

En cuanto al Art.34 del CB, será necesaria la introducción de “una declaración interpretativa en sentido que el registro en tiempo real sea resultante del cumplimiento de una orden de autoridad competente” y en relación al Art. 35 del CB, la necesidad de “trabajar minuciosamente en la definición de la estructura concreta que asumirá este

punto de contacto”<sup>(2)</sup>. Las cláusulas finales (Arts. 36 a 47) no generan mayores problemas.

### Guías de Buenas prácticas

En la actualidad se encuentran disponibles una variedad de guías que contienen recomendaciones acerca de las mejores prácticas a la hora de trabajar con evidencia digital. Distintos autores y organizaciones a lo largo del globo han redactado este tipo de guías en informática forense, que en general comparten los lineamientos generales, sin embargo, en la actualidad no existe un proceso formal unificado.

De la totalidad de recomendaciones existentes, muchas abarcan solo una parte del proceso completo para recuperar información, otras son muy generales, otras focalizan únicamente en los temas delictivos, y ninguna de ellas aborda las técnicas existentes para realizar ciertas tareas, las herramientas disponibles en el mercado en la actualidad, así como tampoco las diferentes alternativas de acuerdo a la plataforma de software del equipo a periciar.<sup>(3)</sup>

Recuperamos a continuación, aquellas que son aplicadas por la Dirección de Análisis Criminal y Tecnologías de la Información (de ahora en más DACTI) de la Policía Judicial de Córdoba.

### RFC 3227

Una de las guías de mejores prácticas existentes a nivel mundial y que se toma como base en el accionar de la DACTI es la RFC 3227.

Una RFC, Request for Comments, es un conjunto de publicaciones del Internet Engineering Task Force (IETF) que describen diferentes aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos. Cada RFC constituye un memorando que ingenieros o expertos en la materia han hecho llegar al IETF, el consorcio de colaboración técnica más importante en Internet, para que éste sea valorado por el resto de la comunidad.

La traducción literal de RFC al español es "Petición de comentarios". La IETF publica oficialmente sus informes en forma de peticiones, disponibles para todos, lo cual permite clarificar una gran cantidad de temas relacionados con TCP/IP. Cada RFC representa una propuesta de especificación, que puede volverse obsoleta en cualquier momento si se publica un nuevo documento RFC. Por lo tanto, estos documentos son archivos de texto que llevan el nombre "rfcxxxx.txt" donde xxxx es un número que se

incrementa por cada RFC nueva. Actualmente existen más de 2000. En realidad, cualquier persona puede escribir una RFC y enviarla al coordinador del IETF. Si se acepta, aparecerá una vez que los coordinadores la hayan evaluado. La RFC1543, cuyo título es Instrucciones para autores de RFC, explica cómo redactar una RFC. Estas publicaciones datan del año 1969, aproximadamente, cuando Steve Crocker inventó un sistema eficaz de hacer llegar las propuestas técnicas al resto de grupos de trabajo que experimentaban con ARPANET, la precursora de Internet.

Los protocolos más importantes de Internet están definidos por RFC, como el protocolo IP detallado en el RFC 791, el FTP en el RFC 959, o el HTTP en el RFC 2616.

La RFC 3227, “Guía Para Recolectar y Archivar Evidencia (Guidelines for Evidence Collection and Archiving)” <sup>(4)</sup> fue redactada en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Este es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con instrucciones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. Además explica algunos conceptos relacionados a la parte legal.

La estructura de la guía es la siguiente:

- Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
- El proceso de recolección: transparencia y pasos de recolección.
- El proceso de archivo: la cadena de custodia y donde y como archivar.

Estos son los puntos más importantes relacionados con dicho proceso:

Principios durante la recolección de evidencias

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).

- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.

De acuerdo a esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco.
- Logs del sistema.1
- Configuración física y topología de la red.
- Documentos.

#### Acciones que deben evitarse

Se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en el caso de que sea necesario:

- No apagar la computadora hasta que se haya recopilado toda la información.
- No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes.

- ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.
- Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo al orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
- Documentar cada paso.
- No olvidar a la gente involucrada. Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

En referencia a la cadena de custodia, establece que esta debe estar claramente documentada y se deben describir los siguientes puntos:

- ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
- ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
- ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?
- En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.

Por otro lado, se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

Existen una serie de pautas que deben de ser seguidas a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

Se deben utilizar herramientas ajenas al sistema ya que éstas pueden haberse visto comprometidas, principalmente en los casos de malware.

Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.

Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CD, USB, etc.).

Se debe preparar un conjunto de utilidades adecuadas a los sistemas operativos con los que se trabaje.

El kit de análisis debe incluir los siguientes tipos de herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

Norma ISO/IEC 27037:2012 <sup>(5)</sup>

La norma ISO/IEC 27037:2012 - Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital, es empleada como marco referencial en el seno de la DACTI, como así también es referente a nivel nacional e internacional. Esta norma provee recomendaciones sobre mejores prácticas en la tarea de identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio. Se orienta a su uso en investigaciones forenses digitales, destinadas al esclarecimiento de hechos en los que interviene de alguna forma un recurso electrónico o digital.

Por su parte, la serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas sugeridas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información. En particular, la primera edición de esta norma fue publicada el 15/10/2012 en Ginebra, Suiza.

La norma proporciona orientación para lidiar con situaciones frecuentes a lo largo de todo el proceso de tratamiento de la evidencia digital. Pretende ayudar a las organizaciones en sus procedimientos de tratamiento de circunstancias excepcionales que involucran datos gestionados en ellas, de forma que se pueda facilitar el intercambio de evidencias digitales potenciales y su presentación como prueba en juicio o arbitraje. Esta norma es muy relevante debido a que hasta el momento de su publicación, solo se contaba con documentos publicados por el NIST (Instituto Nacional de Estándares y Tecnología – Estados Unidos), el departamento de Justicia de los Estados Unidos y el FBI entre otros, todas circunscriptos a un territorio específico, pero no existía norma alguna de alcance global.

La norma incluye dos párrafos muy relevantes: un glosario de términos y definiciones y uno de abreviaturas. Disponer de este tipo de referencia es de enorme valor a la hora de redactar dictámenes periciales. Entre los términos incluidos hay dos

que son relevantes ya que define los roles del profesional involucrado en esta etapa del cómputo forense. En concreto, establece dos roles especialistas en la gestión de las evidencias electrónicas:

- Digital Evidence First Responders (DEFRR): experto en primera intervención de evidencias electrónicas. Es el individuo autorizado, entrenado y calificado para actuar en el primer momento en la escena del hecho que posee la experticia para manipular, recolectar y adquirir evidencia digital.
- Digital Evidence Specialists (DES): experto en gestión de evidencias electrónicas. Es un individuo que posee el conocimiento especializado y la experticia para resolver situaciones técnicas vinculadas con el manejo de evidencia digital y efectuar el análisis forense requerido.

El alcance de la norma define los dispositivos y las funcionalidades que son incluidas en la misma, a saber:

- Medios de almacenamiento digitales utilizados en computadoras tales como discos duros, discos flexibles, discos ópticos y magneto ópticos, dispositivos de datos con funciones similares
- Teléfonos móviles, asistentes digitales personales, dispositivos electrónicos personales, tarjetas de memoria
- Sistemas de navegación móvil
- Cámaras digitales y de video (incluyendo CCTV)
- Computadoras de uso generalizado conectados a redes
- Redes basadas en protocolos TCP / IP y otros.
- Dispositivos con funciones similares a las anteriores

Entre sus características cabe mencionar:

- Aporta orientación sobre el manejo de la evidencia digital. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación a entornos jurisdiccionales.
- Cubre toda una gama de tipos de dispositivos y circunstancias, por lo que la orientación dentro de la norma es ampliamente aplicable.

Es sabido que la evidencia digital es frágil y que su incorrecta manipulación puede producir contaminación de la misma, alterando su contenido. La norma establece los principios de relevancia, confiabilidad y suficiencia así como también las siguientes

etapas para el manejo de la evidencia digital: Identificación, Recolección, Adquisición y Preservación. Señala que DEFR y DES deberán documentar todas sus acciones, las que se regirán por los siguientes principios:

- Minimizar el manejo de la evidencia digital
- Documentar cualquier acción que implique un cambio irreversible
- Adherirse a las regulaciones y leyes locales
- No extralimitarse en sus funciones

La norma reconoce que en ocasiones se trabaja directamente con la evidencia original pudiéndose efectuar tareas que impliquen cambios irreversibles, pero a la vez establece con claridad que el analista forense debe supeditarse a las regulaciones vigentes en su territorio y al mandato de autoridad judicial.

Es menester recuperar los principios establecidos en la norma:

- Relevancia: este es un concepto jurídico que indica que la evidencia digital debe estar relacionada con los hechos investigados.
- Confiabilidad: la evidencia debe ser confiable por lo que debe ser repetible y auditable por un tercero que usando el mismo principio de operación aplicado llegue a idénticos resultados.
- Suficiencia: la evidencia recolectada debe ser suficiente para sustentar los hallazgos obtenidos por el analista forense, es lo que denomino recolección efectiva.

En concordancia con los principios expuestos, la normativa define los siguientes procesos para el manejo de la evidencia digital:

- Identificación: es el reconocimiento de donde se halla la evidencia digital, sea esta física o lógica.
- Recolección: frecuentemente el DEFR deberá tomar la decisión de recolectar la evidencia y trasladarla al laboratorio para su adquisición, en función del tiempo y los recursos informáticos disponibles en la escena del hecho, sustentado por el mandato judicial. En cualquier caso, deberá documentar su decisión fundamentándola y estará preparado para defenderla en un juzgado.
- Adquisición: es el proceso de copia forense que el DEFR realizará obteniendo una copia binaria exacta del contenido lógico o físico de los objetos involucrados en la investigación. La norma establece que la copia



debe ser verificada con un "método de verificación probado" evitando expresarse sobre la utilización de algún HASH en particular.

- Preservación: la evidencia digital deberá ser preservada para asegurar su integridad durante todo el proceso. Esto incluye el embalaje, que en algunos casos tiene requerimientos especiales, por ejemplo un teléfono celular deberá ser almacenado en una bolsa de Faraday.

La norma introduce también el concepto de Cadena de Custodia y establece cuales son los elementos mínimos que esta debe contener:

- Un identificador univoco de la evidencia
- Quién accede a la evidencia, en qué momento y en qué ubicación física
- El pasaje de la evidencia de un sitio a otro y tareas realizadas
- Cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones
- También se consideran las precauciones en la escena del hecho, como proceder con los equipos encontrados en la misma y los roles, responsabilidades y competencias del personal destacado en la escena.

En correspondencia con los lineamientos de la serie de normas ISO 27000, el documentar las acciones, decisiones y omisiones es fundamental, en especial cuando el incidente informático incluye evidencia digital que podría introducirse en ámbito judicial.

Ya adentrándonos en la norma, también se brindan recomendaciones para la recolección y adquisición de dispositivos digitales que se encuentran apagados, encendidos, conectados en red así como también se dedica un capítulo a la recolección, adquisición y preservación de sistemas de video vigilancia basados en computadoras o embebidos.

Según el Ing. Gustavo Pressman (Especialista argentino certificado en Informática Forense) esta normativa si bien no modifica las reglas del juego conocidas, sienta un precedente para el uso de un lenguaje común propio de la actividad forense informática, en especial en el ámbito judicial donde los interlocutores no tienen conocimiento del vocabulario técnico y su significación, así como tampoco de los procesos empleados en el manejo de la Evidencia Digital. La norma ordena muchas de las actividades y conductas que se practican cotidianamente un laboratorio pericial y que constituyen las mejores prácticas forenses, haciendo hincapié en la importancia de documentar.

*PURI – Proceso Unificado de Recuperación de Información* <sup>(6)</sup>

El proyecto PURI es una iniciativa que consiste en el estudio de las técnicas y herramientas disponibles en el mercado con el fin de generar un proceso unificado para recuperar información, y presentar propuestas de desarrollo de nuevas técnicas y herramientas. Resulta relevante incorporar este aporte en nuestro trabajo debido a que las autoridades de la DACTI expresaron que a nivel nacional, toman como referencia el PURI en el proceso continuo de benchmarking al que someten sus prácticas y protocolos.

Este proyecto de investigación fue desarrollado por la Facultad de Ingeniería de la Universidad FASTA (Universidad privada de la Fraternidad de Agrupaciones Santo Tomás de Aquino, Mar del Plata, Argentina) y procura colaborar con los informáticos forenses y con los organismos de justicia en el encuentro de un proceso que constituya una guía y referencia en la actuación forense. La investigación tuvo una duración de 24 meses, entre marzo de 2011 y marzo de 2013. El objetivo de la misma consiste en la construcción de un proceso unificado que sirva de base en la tarea de recuperación de la información digital en equipos de computación. Ante la heterogeneidad de soluciones existentes, se contempló la necesidad de un proceso formal unificado que valide la labor del profesional informático forense, que considere la multiplicidad de dificultades y que permita contar con una guía orientadora y rectora frente a cada problemática. El equipo de trabajo está conformado por Ariel Podestá, Ingeniero Informático, Investigador de la Facultad de Ingeniería de la UFASTA, Bruno Costanzo, Técnico en Informática, Auxiliar de Investigación, Alumno en la Facultad de Ingeniería de la UFASTA, Julián Waimann, Técnico en Informática, Auxiliar de Investigación Alumno, Facultad de Ingeniería de la UFASTA, Martín Castellote, Ingeniero Informático, Investigador de la Facultad de Ingeniería de la UFASTA, Bioinformático en INTA EEA Balcarce, y Rita Sansevero, Ingeniera en Informática, docente e investigadora de la Facultad de Ingeniería de la UFASTA.

El proyecto PURI nace de la conjunción de dos cátedras docentes de la facultad de Ingeniería de la UFASTA, la cátedra de Sistemas Operativos y la de Informática y Derecho. Tiene como horizonte la generación de un proceso unificado para recuperar información y la presentación de propuestas de desarrollo de nuevas técnicas y herramientas, a partir de la detección de carencias.

Un Proceso Unificado de Recuperación PURI está compuesto por cuatro fases básicas: Adquisición, Preparación y Análisis y Presentación.

Fase de Adquisición: esta fase comprende toda actividad vinculada con la generación de una réplica exacta de todo el contenido digital alojado en el dispositivo original. El motivo de realizar una copia de tal información viene originado por distintas razones que se mencionan a continuación.

La ciencia forense debe respetar tres principios básicos: no contaminación, actuar metódicamente y mantener la cadena de custodia. Justamente en las ciencias informáticas la no contaminación se garantiza a través de la copia bit a bit del original, de esa manera, al trabajar sobre la copia se resguarda el original y se garantiza la no contaminación de la evidencia.

Además, el proceso de recuperación de información demanda cierto tiempo, durante el cual el dispositivo quedaría inutilizado para otras actividades. Al trabajar sobre la copia, se podría reintegrar el original al propietario.

Eventualmente el dispositivo que almacena la información en cuestión puede no ser siempre el más indicado para llevar a cabo las pruebas requeridas, debido a problemas de accesibilidad o velocidad. Esta es otra razón que fundamenta la obtención de una copia exacta de los datos a fin de trabajarlos eficientemente en un entorno apropiado.

En escenarios donde la justicia se encuentra involucrada es de crucial importancia exista un modo de reproducir las tareas efectuadas por el perito informático sobre la información original y obtener los mismos resultados. Esto no se lograría si no es contando con una réplica exacta del contenido del dispositivo.

Esta fase de adquisición comprende etapas que de acuerdo al entorno en el que se deba llevar a cabo la recuperación de la información, aplicará o no involucrarlas en el proceso. Es así que se procedió a dividir la adquisición de dispositivos móviles de otros dispositivos por sus características altamente diferenciadoras a todo nivel, tanto físico (hardware), cómo lógico (software).

Fase de Preparación: esta fase involucra todos los procedimientos necesarios para generar el entorno de pruebas preciso para llevar a cabo en primer lugar la inspección, y eventualmente la recuperación de evidencias digitales.

Como primera etapa, la fase de preparación contempla la restauración de la imagen. Esto significa que si la misma se encontrara dividida, encriptada o comprimida deberá realizarse el proceso contrario, a fin de lograr el original. A continuación se deberá validar que la restauración ha sido exitosa mediante un algoritmo de hash.

Si la imagen que se obtuvo es de un sistema de archivos de un determinado sistema operativo, entonces será útil generar una máquina virtual que tome dicha imagen como su disco principal. Al hacerlo se debería realizar una copia a fin de no alterar la imagen original. Opcionalmente puede montarse la imagen a fin de tratar los datos contenidos en la misma como un dispositivo de almacenamiento conectado al equipo de trabajo.

Finalmente esta etapa contempla la identificación de tipos de sistemas de archivos y sistemas operativos contenidos en los medios de almacenamiento originales.

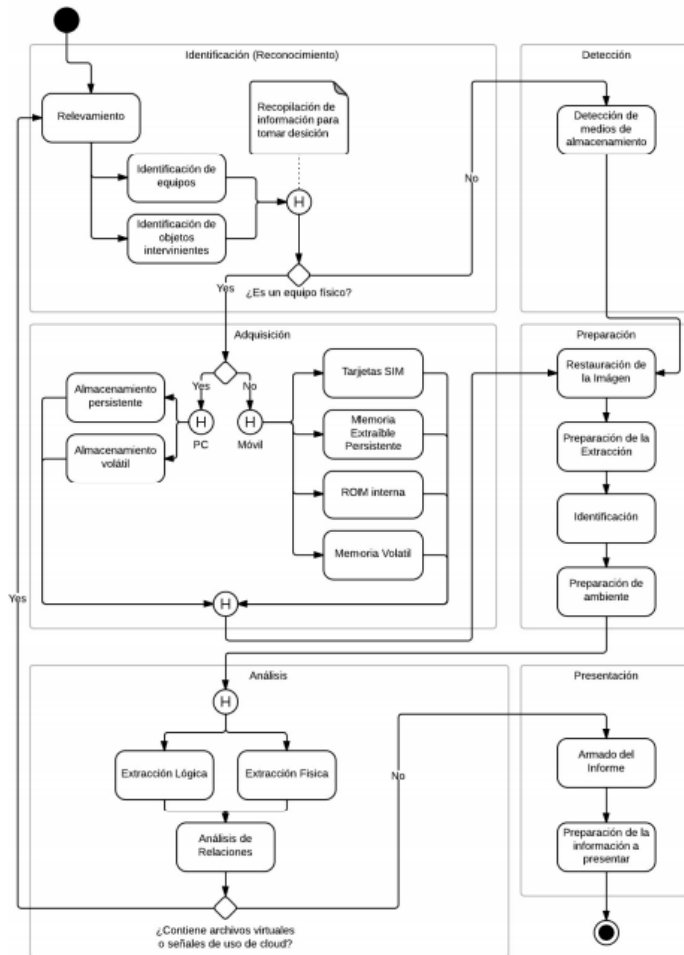
Fase de Análisis: esta fase comprende el fuerte del trabajo en donde se analiza el contenido adquirido en busca de vestigios de lo que se quiere hallar. El objetivo final de la fase de análisis en el caso de un proceso judicial o pre-judicial es encontrar la denominada Evidencia Digital, es decir, aquello que relaciona el hecho ocurrido con el “imputado” y la “víctima”. Entonces, se piensa en la evidencia digital como en un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

La fase de análisis comprende las siguientes etapas: extracción lógica, extracción física y finalmente, análisis de relaciones. La extracción lógica representa la recuperación de información eliminada a partir del sistema de archivos. Por esa razón se denomina “lógica”, ya que no se accede en forma directa a los bloques, sino a través del Sistema de Archivos, y del Sistema Operativo como intermediario. La mayoría de los sistemas operativos no eliminan la información en el momento en el que un usuario solicita el borrado de un archivo determinado, sino que, de alguna manera, dejan registrado que el espacio que ocupaba dicho archivo ahora se encuentra disponible. De esta manera, por ejemplo, si fuese posible hallar tal espacio entonces sería posible reconstruir la información original. La extracción física comprende la búsqueda de la información directamente en el espacio de datos omitiendo todo tipo de estructura de sistema de archivos. Con lo cual se da caso omiso a los metadatos y se aplican diferentes técnicas sobre el contenido puro del bloque en el dispositivo de almacenamiento. La etapa de análisis de relaciones trata justamente de identificar relaciones entre conjuntos de archivos, con el fin de obtener una conclusión. Esto involucra puntualmente la identificación de relaciones entre conjunto de archivos vinculados a una actividad en particular (ej.: archivos relacionados a la navegación por Internet) y la verificación de aplicaciones instaladas, entre otros.

Fase de Presentación: en la fase de presentación se deben tomar todos los recaudos para redactar el informe forense, de manera tal que todas las actividades realizadas

queden plasmadas en el documento, y permitan reproducir el camino y reproducir la pericia en juicio de ser necesario. Por otro lado, deberán observarse los requerimientos existentes en el código de procedimiento vigente “cuestiones de forma” respecto a la información exigida en su presentación.

A continuación incluimos un diagrama que sintetiza las fases del PURI.



Actualmente se encuentra en curso el PURI en Smartphones, proyecto conjunto UFASTA – UNIANDES (Universidad Regional Autónoma de los Andes, Ecuador) para adaptar PURI a Smartphones.

Red G8 24/7 para Delitos de Alta Tecnología <sup>(7)</sup>

Para concluir con este apartado haremos mención a la Red G8 24/7 para la Conservación de la Información, de la cual la República Argentina forma parte, por ser el exponente más importante de colaboración internacional. El G8 es un grupo informal de países del mundo cuyo peso político, económico y militar es tenido por relevante a escala global. Está conformado por Alemania, Canadá, Estados Unidos, Francia, Italia,

Japón, Reino Unido, Rusia (temporalmente excluida por la crisis de Crimea). Además, la Unión Europea cuenta con representación política.

Los puntos de contacto G8 24/7 se proporcionan para investigaciones de material probatorio electrónico que requieren asistencia urgente de autoridades extranjeras. Los delitos de alta tecnología presentan retos distintos para las autoridades de aplicación de la ley. En las investigaciones relacionadas con redes informáticas, a menudo es importante que investigadores con conocimiento tecnológico específico reaccionen con velocidad como nunca antes para preservar información electrónica y ubicar sospechosos, a menudo pidiéndole a los servidores de servicio de Internet que les ayuden a conservar la información. Por lo tanto, para mejorar y suplementar (pero no reemplazar) a los métodos tradicionales de obtención de ayuda, el G8 ha creado la Red como un mecanismo nuevo para lograr contactos entre las autoridades de Estados Participantes y de otras jurisdicciones autónomas de Estado (en lo sucesivo “Participantes”).

Para utilizar esta red, los agentes de aplicación de la ley que busquen la asistencia de un Participante extranjero pueden contactarse con el punto de contacto de 24 horas de su propio estado o jurisdicción autónoma de aplicación de la ley, y tal individuo o entidad, de ser debido, se contactará con su homólogo en el Participante extranjero. Los Participantes en la Red se han comprometido a hacer el mayor esfuerzo para asegurarse de que los Proveedores de Servicio de Internet congelen la información que busca el Participante requirente lo más pronto posible. Los Participantes además se han comprometido a hacer el mayor esfuerzo para presentar la información con prontitud. Aquello queda sujeto al entendimiento de que las consideraciones jurídicas y técnicas, o los recursos, del Participante al que se le hace la solicitud pueden afectar la medida en la que, y el periodo de tiempo en el que, el Participante pueda presentar el material probatorio, como también el proceso de Asistencia Jurídica Mutua, mediante el cual el país requirente solicita información a través del procedimiento usual de tratados de asistencia jurídica mutua o cartas rogatorias.

Haremos una breve descripción de los requisitos para ser miembro de esta red, ya que para unirse a la misma un candidato debe ser capaz de proporcionar:

- Punto de contacto disponible 24/7: esto significa una persona que puede ser contactada 24 horas al día, 7 días a la semana, para dársele información y/o solicitar ayuda de otros países parte de la Red. Ser un punto de contacto no requiere que se establezca una unidad formal de delitos de informática. En

algunas jurisdicciones, el punto de contacto lo forman unos pocos investigadores interesados en los ciberdelitos, en otras, el punto de contacto es parte de una unidad formal. Además, algunos puntos de contacto son centros de telecomunicaciones que conectan al llamador con el debido oficial, mientras que otros son personal con experiencia de investigación o técnica.

- Punto de contacto que hable inglés: esto es por motivo de viabilidad, ya que la red es mucho más sencilla si hay un lenguaje en común, y el inglés es el idioma más hablado, especialmente en relación con la informática y la Internet.
- Punto de contacto con conocimiento técnico: la persona que reciba las llamadas debe tener un nivel de conocimiento básico sobre los delitos informáticos
- Conocimiento de leyes y políticas domésticas: como investigador de aplicación de la ley de ciberdelitos, la persona que atienda la solicitud debe entender su autoridad para conservar y recolectar material probatorio electrónico. Además debe saber, o tener la capacidad de enterarse rápidamente, qué tipos de asistencia puede prestar a países extranjeros de conformidad con las leyes de su país.

La importancia de esta red deriva de la urgencia de dar respuesta oportuna a los delitos informáticos y a la problemática de la transterritorialidad de los mismos.

Referencias:

(1) *Andrés Díaz Gómez. “El Delito Informático, su problemática y la cooperación internación como paradigma de su solución: El Convenio de Budapest. Especial consideración a España y Argentina”. Universidad de La Rioja, España. Este artículo fue tomado como base para la elaboración del inciso.*

(2) *HOLOGRAMATICA – Facultad de Ciencias Sociales – UNLZ – Año VII, Número 14, V5 (2011), pp. 27-86.*

(3)(6) *La Informática Forense y el Proceso de Recuperación de Información Digital*  
*Ana Haydée Di Iorio*

(4) *BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible en: <http://www.rfceditor.org/rfc/rfc3227.txt>*

(5) *Ing. Gustavo Pressman, “ISO/IEC 27037: ¿Plantea una nueva forma de hacer Análisis Forense?” Disponible en:*

*<http://www.issaarba.org/node/70>*

(7) *“La Red G8 24/7 Para la Conservación de Información. Declaración de Protocolo” Disponible en:*

*[http://www.oas.org/juridico/english/cyb\\_pan\\_G8\\_sp.pdf](http://www.oas.org/juridico/english/cyb_pan_G8_sp.pdf)*



# **CAPÍTULO 4**

***CONSIDERACIONES***

***BÁSICAS SOBRE***

***SMARTPHONES***

***ANDROID***

### Introducción

A continuación incluimos una serie de conceptos básicos sobre telefonía móvil, que servirán de punto de partida para la presentación de protocolos de actuación forense.

En los párrafos siguientes se provee una síntesis general de las características relevantes de los smartphones, siempre desde la óptica del presente trabajo. Desarrollar un entendimiento de los componentes y la organización interna de los dispositivos móviles es un pre-requisito para entender las implicancias involucradas en el análisis forense de los mismos.

Se denomina Smartphone (teléfono inteligente) al segmento de móviles que poseen características que simulan el funcionamiento de un computador, hecho que los convierte en dispositivos altamente funcionales. Debido al ritmo acelerado con que la tecnología móvil evoluciona, cabe destacar que este apartado captura una instantánea del momento actual en materia de teléfonos móviles inteligentes.

Distintos aparatos poseen distintas características físicas y técnicas. Haremos foco en forma genérica en dispositivos con Android, debido a que actualmente es el SO más popular a nivel regional (Argentina) y global.

### Características de los dispositivos móviles

Actualmente los dispositivos móviles son capaces de ejecutar un conjunto de funciones que van desde las que provee un simple teléfono hasta las de una computadora personal. La mayoría de los teléfonos celulares tienen un conjunto básico de características y funciones comparables. Poseen un microprocesador, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), un módulo de radio, un procesador de señal digital, un micrófono y un altavoz, un conjunto de teclas y una pantalla de cristal líquido (LCD). El sistema operativo se almacena o en una memoria NAND o NOR mientras que la ejecución del código ocurre típicamente en la RAM.

Slots empotrados para tarjetas SD (Secure Digital) pueden soportar memorias removibles con capacidad de almacenamiento entre 64 GB y 2TB. A su vez, conectividad Wireless, tal como infrarrojo, Bluetooth y WiFi, suelen ser incluidas en el equipo y soportan distintos protocolos para intercambiar datos.

En general, podemos clasificar los dispositivos móviles como teléfonos celulares (aquellos que permiten efectuar llamadas y comunicarse vía mensajes) y smartphones (aquellos que ofrecen capacidades más avanzadas en términos multimedia, similar a los

de una computadora personal). La caracterización que a continuación presentamos pretende ser ilustrativa y bajo ningún punto de vista, agota las caracterizaciones posibles. La misma fue extraída de “Guidelines on Mobile Device Forensics” publicada por el NIST (Instituto Nacional de Estándares y Tecnologías, Departamento de Comercio de Estados Unidos) en mayo de 2014. Incluimos un cuadro comparativo en términos de hardware y otro en términos de software. Generalmente los smartphones introducen una nueva característica o funcionalidad y con el paso del tiempo, los teléfonos celulares terminan también incluyéndola.

Tabla comparativa de Hardware

	Teléfono celular	Smartphone
Procesador	Velocidad limitada (~52Mhz)	Velocidad superior (~1GHz dual-core)
Memoria	Capacidad limitada (~5MB)	Capacidad superior (~128GB)
Display	Tamaño pequeño, a color	A color, de gran tamaño y definición
Ranura para tarjetas	Ninguna, MicroSD	MicroSDXC
Cámara	Fija y de video	Fija, panorámica y video (HD)
Entrada de texto	Teclado numérico, teclado QWERTY	Pantalla táctil, reconocimiento de escritura a mano, teclado QWERTY
Entrada de voz	Ninguna	Reconocimiento de voz (para el marcado y el control)
Interfaz celular	Voz y datos limitados	Voz y datos de alta velocidad
Posicionamiento	Ninguno, Receptor GPS	Receptor GPS
Wireless	IrDA, Bluetooth	Bluetooth, WiFi, y NFC
Batería	Fija/removible, recargable, de polímero de litio	Fija/removible, recargable, de polímero de litio

Tabla comparativa de Software

	Teléfono celular	Smartphone
Sistema Operativo	Cerrado	Android, BlackBerry OS, iOS, Symbian, WebOS y Windows Phone
PIM (Manejo de información)	Agenda de contactos,	Agenda de contactos

personal)	calendario y recordatorios	mejorada, calendario y recordatorios
Aplicaciones	Mínimas (juegos, bloc de notas)	Aplicaciones (juegos, ofimática y redes sociales)
Llamadas	Voz	Voz, video
Mensajes	Texto, MMS	Texto, texto mejorado. Mensajes multimedia
Chat	Mensajería instantánea	Mensajería instantánea mejorada
Email	Vía mensaje de texto	Vía servidor POP o IMAP
Web	Vía WAP	HTTP directo

Sucinta mención haremos al SO Android, que actualmente constituye la plataforma más popular a nivel mundial. Android es un sistema operativo basado en Linux, diseñado principalmente para móviles con pantalla táctil como smartphones, tablets, notebooks, entre otros. En cuanto a la conectividad, el SO soporta GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE, HSDPA, HSPA+ y WiMAX. Android, al contrario que otros sistemas operativos para dispositivos móviles como iOS o Windows Phone, se desarrolla de forma abierta y se puede acceder tanto al código fuente como a la lista de incidencias donde se pueden ver problemas aún no resueltos y reportar problemas nuevos. Millones de personas emplean Android a lo largo y a lo ancho del globo porque la plataforma hace que los dispositivos móviles sean más poderosos y útiles.

### Tarjeta SIM

Bajo el framework GSM (Sistema Global para las Comunicaciones Móviles) nos referimos a los dispositivos móviles como particionados en dos componentes: el UICC (Integrated Circuit Card) y el equipo móvil. Generalmente el UICC es referido como el módulo de identidad, consiste en un componente removible que contiene información esencial acerca del abonado. El equipo móvil no puede operar de manera plena sin el UICC. La principal función del UICC es autenticar al usuario del dispositivo móvil en la red para proveerle acceso a los servicios a los que está subscripto.

Una tarjeta SIM (del inglés Subscriber Identity Module, Módulo de Identificación de Abonado) es una tarjeta inteligente desmontable usada en teléfonos móviles y

módems HSPA o LTE que se conectan al puerto USB. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta. La tarjeta SIM almacena algunos identificadores y algoritmos necesarios para autenticar al suscriptor en la red. Un usuario puede remover la SIM de su equipo móvil e insertarla en otro móvil compatible y reanudar la operación del mismo sin la intervención de la proveedora de servicio telefónico, conservando su número telefónico, plan de servicio e incluso el directorio de marcado rápido. Los archivos dentro de la tarjeta SIM son utilizados por los usuarios para almacenar información de la configuración de la red, contactos y enviar y recibir mensajes de texto. La SIM constituye entonces otro punto factible de ser analizado en un proceso forense.

El uso de la tarjeta SIM es obligatorio en las redes GSM. La capacidad de almacenamiento de una tarjeta SIM está entre 2KB y 128KB

Existen actualmente tres tipos de tarjetas SIM

- Tarjeta MiniSIM: este modelo de tarjeta es el más común ya que desde muchos años atrás ha sido el utilizado en los teléfonos móviles. La capacidad de almacenamiento va desde los 2KB a 16 o 32KB



- Tarjeta MicroSIM: son iguales que las tarjetas MiniSIM pero con un tamaño más reducido, de esa forma se aprovecha mejor el espacio interno de los smartphones para poder hacerlos más potentes. Este tipo de tarjetas tiene una mayor capacidad y permite un mayor almacenamiento que su antecesora, pudiendo guardar más ajustes y aplicaciones y tener más seguridad. El usuario de la tarjeta MicroSIM podrá tener un mayor número de contactos en su agenda. Es decir, la reducción del tamaño no implica una reducción de la capacidad, sino todo lo contrario. La MicroSIM se utiliza en los últimos modelos de smartphones, como la serie Galaxy de Samsung o Lumia de Nokia. La capacidad de almacenamiento de una tarjeta MicroSIM va desde 32KB hasta los 128KB.



- Tarjeta NanoSIM: ofrece una nueva reducción del tamaño, pero no es más que eso, una reducción tanto de sus dimensiones como del grosor. La NanoSIM es un 30% más pequeña que la MicroSIM pero está compuesta, igual que las anteriores, por un chip de almacenamiento. Esta tarjeta llega de la mano del lanzamiento del iPhone 5 y de las últimas generaciones de iPad y iPad mini. La capacidad de almacenamiento de una tarjeta NanoSIM es de 128KB



### Equipo Móvil

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

El equipo móvil está diseñado para movilidad, tiene un tamaño compacto, con baterías recargables y es ligero. Todos los equipos móviles tienen un número de características en común, pero los fabricantes tratan de diferenciar sus productos por lo que ejecutan funciones adicionales para hacerlos más atractivos a los consumidores.

El sistema operativo del dispositivo se mantiene en la memoria ROM, y es factible de ser borrado y reprogramado con herramientas adecuadas. La memoria RAM se mantiene activa por medio de baterías, y su daño o agotamiento hace que la información en ella contenida se pierda.

Los equipos móviles desarrollados recientemente disponen de microprocesadores cada vez más avanzados e incluyen una capacidad de memoria considerable, es extendido el uso de memorias extraíbles y periféricos especializados.

#### Componentes de hardware de un móvil con Android<sup>(1)</sup>

A continuación se citan de forma genérica los componentes de hardware de un smartphone con Android.

- CPU, del tipo ARM (Advanced RISC Machines) de la compañía ARM. Holdings, la arquitectura es del tipo RISC (Reduced Instruction Set Computer- Conjunto de Instrucciones de Computadora Reducido).
- Módem y radio, de banda base. Hardware y software que permiten la conexión a la red celular y de transmisión de voz y datos.
- Memoria volátil RAM.
- Memoria no volátil Flash NAND.
- Sistemas de Posicionamiento Global – GPS.
- Redes Inalámbricas tipo Wi-fi.com y Bluetooth.
- Memoria removible: Tarjeta Digital Segura (SD).
- Pantalla Táctil.
- Cámara.
- Teclado por pantalla.
- Batería.
- Conector Universal Serial Bus (USB).
- Medidor de aceleración y giroscopio, detecta y cambia la interfaz del usuario basándose en movimientos y rotaciones acordes a la forma en que es sostenido el celular.
- Parlantes y micrófono.

#### Componentes de software de un móvil con Android<sup>(2)</sup>

Android es un conjunto de capas o una pila de software para dispositivos que incluye un sistema operativo, middleware y aplicaciones.

- Las aplicaciones incluyen cliente de correo electrónico, programas SMS, calendario, mapas, navegador de internet, contactos, etc. Las aplicaciones son escritas en el lenguaje de programación Java.

- La infraestructura digital o framework ofrece una plataforma abierta de desarrollo que les permite a los programadores construir aplicaciones innovadoras, tomando ventaja de:
  - los dispositivos de hardware.
  - el acceso a la información local.
  - la ejecución de servicios en segundo plano.
  - la configuración de alarmas.
  - las notificaciones en la barra de estado, entre otras capacidades.

Los programadores tienen acceso completo al mismo API que utilizan las aplicaciones del sistema. La arquitectura de aplicación está diseñada para simplificar la reutilización de los componentes, cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede hacer uso de dichas capacidades bajo determinadas restricciones de seguridad dentro de la infraestructura de desarrollo. Este mismo mecanismo permite a los usuarios reemplazar los componentes.

- Librerías: Android incluye una serie de librerías de C y C++, tales como System C (libc de BSD), Multimedia, LibwebCore, SGL, SQLite, por nombrar algunas de las principales.
- La máquina virtual Dalvik VM ejecuta las aplicaciones sobre el sistema operativo de los dispositivos Android y fue escrita de forma tal que un dispositivo Android puede ejecutar múltiples máquinas virtuales de manera eficiente. Los programas son escritos en Java y compilados a un código intermedio entre el código fuente y el lenguaje de máquina (Bytecode).
- La máquina virtual Dalvik utiliza su propio conjunto de instrucciones de 16 bits que trabaja directamente sobre las variables locales. Generalmente, las variables locales eligen un registro virtual de 4 bits. La reducción del tamaño de instrucción aumenta la velocidad de su intérprete. Cada aplicación de Android ejecuta su propio proceso con su propia instancia en la máquina virtual Dalvik.
- Los archivos son ejecutados en el formato, “.dex”, el cual minimiza el uso de la memoria y el del microprocesador. La máquina virtual está basada en registros y ejecuta clases compiladas por el compilador del lenguaje Java que fueron transformados en el formato “.dex”, por una herramienta incluida en la máquina virtual denominada “.dx”. Dalvik VM se encuentra



por sobre el sistema operativo Linux y este último se encarga de las funciones subyacentes como son los procesos hilos (thread) y el manejo de memoria de bajo nivel.

- Android está basado en el kernel de sistema operativo Linux de la versión 2.6 y le confía la gestión de memoria, de procesos, de pila de protocolos de red y del modelo del dispositivo. El núcleo actúa como una capa de abstracción entre el hardware y el resto de la pila de software.
- El modelo de seguridad de Android es efectivo en la restricción de los accesos a los datos de las aplicaciones. Características del modelo:
  - A cada aplicación se le asignará un único usuario y grupo de Linux.
  - Las aplicaciones se ejecutan utilizando su identificador único en un proceso dedicado dentro de la máquina virtual.
  - Cada una de las aplicaciones tiene un espacio de almacenamiento dedicado en */data/data* que solo puede ser accedido por la aplicación.

No obstante, la infraestructura digital de Android brinda mecanismos para que las aplicaciones puedan compartir datos. Por ejemplo, un desarrollador puede incluir soporte para proveedores de contenido dentro de la aplicación, permitiéndole compartir datos con otras aplicaciones. El programador controla que datos serán expuestos a otras aplicaciones. Durante la instalación de la una aplicación, un usuario puede controlar si permitirá o no que una aplicación tenga acceso a un proveedor de contenido (SMS/MMS, contactos, calendario, Facebook, Gmail.)

### *Estructura del sistema de archivos en Android*<sup>(3)</sup>

El sistema de archivos YAFFS2 (Yet Another Flash File System) es reciente y usado ampliamente en los dispositivos Android. Fue diseñado específicamente para la memoria Flash NAND, soporta enlaces duros, simbólicos y tuberías.

La organización de los datos en una estructura física de una memoria Flash NAND es manejada por el dispositivo de tecnología de memoria MTD (Memory Technology Device). La organización es en 128 bloques, que consisten en fragmentos de 2048 bytes de datos seguidos de 64 bytes de datos de reserva u OOB (Out Of Band) utilizados para guardar metadatos del disco y del sistema de archivo. Los grupos de fragmentos se combinan para formar un bloque borrado, generalmente de 64 fragmentos. Los fragmentos pueden tener datos o un encabezado. El encabezado contiene información

sobre el nombre del archivo, tamaño, fecha y hora de creación, identificador del padre. La información de los fragmentos también se guarda en el espacio de reserva. La combinación de la información del espacio de reserva y el encabezado son necesarios para construir la estructura de archivos y directorios.

Datos- Fragmentos- Paginas(2048 bytes)	Reserva u OOB (64 bytes)
--	--------------------------

De los 64 bytes de la reserva u OOB, la distribución es la siguiente:

ID Fragmento	ID Encabezado	Byte	Nro. de Secuencia	ECC	Bloque	Datos
<b>4 bytes</b> (Si es 0 es entrada de directorio, si es >1 es dato y posición).	<b>4 bytes</b> (0 si no se utiliza)	Numero de bytes $2^n$ , utilizados por el fragmento 2048=Lleno	<b>4 bytes</b>	<b>3 bytes</b> Código de Corrección de Errores para etiquetas (tags) <b>24 bytes</b> Código de Corrección de Errores de datos	<b>1 byte</b> Estado del Bloque (dañado)	<b>1 byte</b> Estado de datos (dirty-inválida)

Estructura del encabezado (entrada del directorio)

Identificador del Objeto	Entero
Checksum	2 bytes
Nombre de archivo	255 bytes
Modo: protección, directorio, archivo, enlace simbólico.	4 bytes
Identificador del usuario propietario	4 bytes
Identificador del grupo propietario	4 bytes
Fecha y hora de acceso- <i>atime</i>	4 bytes
Fecha y hora de última modificación de datos - <i>mtime</i>	4 bytes
Fecha y hora de último cambio – <i>ctime</i>	4 bytes
Tamaño de archivo- <i>filesize</i>	Entero si es del tipo <i>little endian</i> , convertir a

	hexadecimal o decimal, cero si es carpeta.
Equivalente a identificador de objeto para enlaces duros.  Alias, si es un enlace simbólico o acceso directo.	Entero

La estructura de archivo se puede visualizar en el archivo *mtd* del directorio */proc* y puede ser la siguiente dependiendo del fabricante:

- mtd0: 00040000 00020000 “misc” – misceláneas
- mtd1: 00500000 00020000 “recovery” – recuperación
- mtd2: 00280000 00020000 “boot” – inicio o arranque
- mtd3: 04380000 00020000 “system” – datos del sistema
- mtd4: 04380000 00020000 “caché”
- mtd5: 04ac0000 00020000 “userdata” – datos del usuario

El área de reserva OOB puede ser un problema al momento de montar el sistema de archivo YAFFS2 para su análisis y para el uso de herramientas de análisis de fragmentos. Se pueden utilizar herramientas para remover los espacios de reserva o un simple programa.

El paquete de herramientas de desarrollo de Android contiene aplicaciones de utilidad para la recolección y análisis forense de los dispositivos, como así también el propio sistema operativo Linux sobre el cual funciona Android. En la computadora de informática forense es recomendable que el perito instale el paquete de herramientas de desarrollo de Android. En el laboratorio el perito podrá practicar el uso de las herramientas de recolección análisis que se encuentran en el paquete de desarrollo y luego crear un emulador de un dispositivo Android.

Los dispositivos Android contienen gran cantidad de información para recolectar y analizar, a saber:

- Mensajes de texto (SMS/MSM).
- Contactos.
- Registros de llamadas.
- Mensajes de correo electrónico.
- Mensajería instantánea.
- Coordenadas GPS.

- Fotografías y videos.
- Historial de web.
- Historial de búsquedas web.
- Directivas de manejo o conducción.
- Redes sociales: Facebook, Twitter, etc.
- Archivos guardados en el dispositivo.
- Música.
- Citas en la agenda.
- Información financiera.
- Información de comercio electrónico.
- Historial de compras en línea.
- Archivos compartidos.

Las aplicaciones en Android se pueden guardar en forma interna o externa. El almacenamiento externo se realiza en la tarjeta SD (Secure Digital) o tarjetas SD emuladas. El almacenamiento interno es controlado por las aplicaciones de Android. Al instalarse una aplicación ya sea descargada desde el sitio de Android o incorporada de fábrica, se guarda internamente información en el subdirectorio */data/data* con el nombre de la aplicación a continuación de nombre del paquete. Dentro del directorio */data/data* existe un número de directorios estándar que se encuentran en varias aplicaciones, como así también los directorios de control de los desarrolladores de aplicaciones.

El sistema Android provee a los desarrolladores de cinco métodos para almacenar los datos en el dispositivo, estos es muy importante para los peritos en las etapas de recolección y análisis de los datos. Los datos no volátiles se guardan tanto en la tarjeta SD como en la memoria Flash NAND o en la red (cloud). Los métodos son:

- Preferencias compartidas: permite al desarrollador guardar pares de claves de tipo de datos primitivos en el formato XML (variables booleanas, verdadero-falso, puntos flotantes, enteros, cadena de caracteres en UTF-8, etc.).
- Almacenamiento interno: datos de estructuras más complejas de los desarrolladores se guardan en subdirectorios en */data/data*, que les permite controlar el tipo de archivo, nombre y ubicación. Son todos aquellos archivos que no están en *lib*, *cache*, *databases* o *SHard\_prefs*. Las

aplicaciones utilizan el directorio *app\_* y *files* para guardar datos. El directorio *app\_* contiene varios subdirectorios y archivos de formato desconocido (cach\_r.m).

- Almacenamiento externo: en la tarjeta SD con la estructura de archivos FAT32, para facilitar su montaje y lectura.
- SQLite: gestor de base de datos.
- Red, documentación de los desarrolladores que utilizan paquetes como java.net, android.net.

El perito podrá encontrar otra área de análisis en el sistema operativo estándar de Linux, los archivos de registro de eventos del núcleo o kernel del sistema operativo, inicio y depuración del sistema. El núcleo de Linux es la capa de abstracción de bajo nivel que le permite tener acceso al hardware del dispositivo. La función del núcleo es fundamental en el desempeño del dispositivo de Android y por lo tanto el perito debe verificar a través del comando *dmesg* las actividades del núcleo del sistema operativo.

El dispositivo Android posee dos memorias RAM volátil y Flash NAND no volátil. La memoria RAM se utiliza para cargar, ejecutar y manejar las partes importantes del sistema operativo, las aplicaciones o datos (claves, claves cifradas, nombres de usuario, datos de aplicaciones, datos de proceso y servicios).

La memoria Flash NAND es utilizada para guardar sistemas de archivos, datos del usuario.

### Referencias

<sup>(1)(2)(3)</sup>: Darahuge, María Elena, Arellano González, Luis E. “Manual de Informática Forense II. (Prueba Indiciaria Informático Forense)”. Ed. Errepar. Primera Edición. Año 2012.

# **CAPÍTULO 5**

## ***ASPECTOS***

### ***PROCEDIMENTALES***

#### ***DEL ANÁLISIS***

##### ***FORENSE DE***

###### ***SMARTPHONES***

### Introducción

En este capítulo introducimos una serie de consideraciones procedimentales inherentes a la actuación forense sobre telefonía móvil. Esta recopilación es un intento de unificación de criterios, recuperando aportes desde distintas fuentes y sobre distintas etapas del ciclo de vida del examen forense. Los aspectos detallados no pretenden bajo ningún concepto, ser excluyentes o acabados.

### Principios rectores durante la recolección de la prueba

En primer lugar recuperamos las indicaciones que la RFC 3227 efectúa acerca de aspectos a considerar en el momento de recabar pruebas. Estas recomendaciones son generales, a nivel de pericia informática, por lo que pueden ser aplicables puntualmente a los smartphones.

- Respetar la Política de Seguridad del sitio y adherir al manejo apropiado de incidentes y de personal de aplicación de la Ley.
- Capturar una imagen lo más exacta del sistema como sea posible.
- Mantener notas detalladas. Estas deben incluir fechas y horas. Si es posible generar una transcripción automática. Notas y capturas de pantalla deben ser firmadas y fechadas.
- Notar la diferencia entre el sistema y el reloj UTC. Para cada fecha y hora previstas, indicar si se emplea el tiempo UTC o el local.
- Estar preparado para testificar (quizás años más tarde), ser capaz de exponer todas las acciones que se tomaron y en qué momento. Notas detalladas serán vitales en este proceso.
- Minimizar los cambios a los datos en la medida que se van recolectando. No limitarse a los cambios en los contenidos, se debe evitar la actualización de archivos o los tiempos de acceso al directorio.
- Eliminar las vías externas para el cambio.
- Al enfrentarse a la dicotomía entre recolección/análisis, lo que se debe hacer primero es la recolección, y el análisis luego.
- Los procedimientos deben ser aplicables. Como en cualquier aspecto de la política de incidentes, los procedimientos deben ser testeados para garantizar la viabilidad, especialmente en una crisis. Si es posible, los procedimientos



deben ser automatizados, por razones de velocidad y precisión. Ser metódico.

- Por cada dispositivo, un enfoque metódico debe ser adoptado, el cual continúe con la línea adoptada en el procedimiento de recolección. La velocidad generalmente es crítica, por lo que frente a un número de dispositivos que requieren ser examinados sería apropiado dividir la labor entre el equipo de trabajo para recolectar las pruebas en paralelo.
- Proceder desde lo más volátil a la menos volátil.
- Hacer una copia a nivel de bits del sistema. Si se desea efectuar un análisis forense, debe hacerse una copia a nivel de bits para tal propósito, ya que el análisis seguramente alterará los tiempos de acceso de los archivos. Evitar hacer pruebas forenses sobre la copia de la evidencia.

#### *Orden de volatilidad*

Para continuar, citamos las consideraciones acerca del orden de volatilidad que la RFC 3227 efectúa. En la recolección de pruebas se debe proceder de la más a la menos volátil. Para ilustrar este concepto, se presenta un ejemplo de orden de volatilidad para un sistema típico.

- Registros, caché.
- Tabla de enrutamiento, caché arp, tabla de procesos, estadísticas del kernel, memoria.
- Archivos de sistema temporales.
- Disco.
- Loggeo remoto y monitoreo de datos es de interés para el sistema en cuestión.
- Configuración física, topología de la red.
- Medios de archivado.

#### *Cosas a evitar*

La RFC presenta un listado de “Cosas a evitar”, a nuestro entender, breve pero muy interesante, debido a que es demasiado fácil destruir evidencia inadvertidamente. Los ítems incluidos son:

- No apagar hasta que haya concluido la recopilación de pruebas. Muchas pruebas se pueden perder y es posible que el atacante haya alterado los scripts/servicios del inicio/apagado para destruir las pruebas.
- No confiar en los programas en el sistema. Ejecutar las aplicaciones para colección de evidencia desde medios protegidos adecuadamente.
- No ejecutar programas que modifiquen el tiempo de acceso de los archivos del sistema.
- Al retirar las vías externas para el cambio, tener en cuenta que desconectar o filtrar desde la red puede desencadenar "deadman switches" que detectan cuando están fuera de la red y proceden a borrar pruebas.

### *Privacidad*

En relación a la privacidad, se hacen las siguientes consideraciones:

- Respetar las normas y directrices de privacidad en la empresa y su jurisdicción legal. En particular, asegurarse que ninguna información recogida junto con las pruebas está al alcance de alguien que normalmente no tendría acceso a esta información. Esto incluye acceso a los archivos de log (que pueden revelar patrones de comportamiento de usuario) como así también archivos de información personal.
- No entrometerse en la vida privada de personas sin una fuerte justificación. En particular, no recopilar información de áreas a las que normalmente no se tiene acceso a menos que se tenga una indicación suficiente que hay allí un incidente real.
- Asegurarse de que se tiene el respaldo de la empresa y su normativa para ejecutar los procedimientos necesarios para reunir las pruebas de un incidente.

### *La prueba informática*

En cuanto a lo legal, se indica que la prueba informática debe ser:

- Admisible: debe ajustarse a ciertas normas jurídicas antes de que se pueden presentar ante un tribunal.
- Auténtica: debe ser posible enlazar la evidencia al incidente de forma positiva.

- Completa: debe contar con toda la historia y no sólo una perspectiva particular.
- Fiable: no deben existir dudas acerca de la forma en que la prueba fue recogida y manipulada, a fin de no arrojar dudas acerca de su autenticidad y veracidad.
- Creíble: debe ser fácilmente comprensible y creíble por un tribunal.

### *Proceso de recolección*

En referencia al proceso de recolección, la RFC hace una serie de salvedades. La primera salvedad indica que los procedimientos de recolección deben ser lo más detallados posible. Como es en el caso de los procedimientos de manejo de incidentes, estos deben ser inequívocos, y deben reducir al mínimo la toma de decisiones necesarias durante el proceso de recolección.

Por su parte, los métodos utilizados para recopilar pruebas deben ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos utilizados, y estos métodos deben haber sido testeados por expertos independientes.

#### Pasos de la recolección:

1. ¿Dónde están las pruebas? Listar los sistemas que participan en el incidente y de los que se recogerán las pruebas.
2. Establecer lo que se considera pertinente y admisible. Ante la duda es preferible recolectar de más a que falten pruebas.
3. Para cada sistema, obtener lo relevante según el orden de volatilidad.
4. Eliminar las vías externas que permitan efectuar cambios.
5. Según el orden de volatilidad, recoger las pruebas con herramientas.
6. Registrar el grado de sincronización del reloj del sistema.
7. Preguntarse qué más podría ser evidencia relevante a medida que se avanza en el proceso de recolección.
8. Documentar cada paso.
9. No olvidar a las personas involucradas. Registrar quienes estaban presentes, que estaban haciendo, que observaron y la forma en que reaccionaron.
10. Cuando sea posible se debe considerar generar checksums y firmar criptográficamente la evidencia recolectada, para de esta manera facilitar la preservación de la cadena de custodia. Durante este proceso no se debería alterar la evidencia.

### *Cadena de custodia*

En alusión a la cadena de custodia, se indica que las pruebas deben ser estrictamente garantizadas y la cadena de custodia debe estar claramente documentada. El perito debe ser capaz de describir claramente la manera en la se encontraron pruebas, cómo estas fueron manejadas y todo lo que a ellas le sucedió.

Las siguientes acciones deben ser documentadas:

- ¿Dónde, cuándo y por quién/es fue/ron descubiertas las pruebas recogidas?
- ¿Dónde, cuándo y por quién/es fue/ron manejadas y examinadas las pruebas?
- ¿Quién tuvo custodia de las pruebas, y durante qué período? ¿Cómo fueron almacenadas?
- ¿Cuándo las pruebas cambiaron de custodia?, el momento y la forma en que ocurre la transferencia.

En cuanto al archivo de pruebas, se recomienda que si es posible, se deberían usar archivos específicos para este tipo de medios. El acceso a las pruebas debe ser muy limitado/restricto, y estar claramente documentado. A su vez, debe ser posible detectar accesos no autorizados.

### *Herramientas*

Para finalizar, la guía indica que el perito debe tener los programas que necesite para hacer acopio de pruebas y medios forenses de sólo lectura. El experto debe tener preparado un conjunto de herramientas para cada uno de los sistemas operativos que maneja, antes de tener que utilizarlo.

El conjunto de herramientas debe incluir lo siguiente:

- Un programa para examinar los procesos.
- Programas para examinar el estado del sistema.
- Un programa para hacer copias bit a bit.
- Programas para la generación de checksums y firmas.
- Programas para la generación de imágenes del núcleo básicas y su posterior examen.
- Scripts para automatizar la recopilación de pruebas.

Los programas en su conjunto de herramientas deben estar estáticamente enlazados, y no debería requerir el uso de cualquier librería distinta de las de sólo lectura. Se debe

estar preparado para brindar testimonio de la autenticidad y fiabilidad de las herramientas que se utilicen.

### *Protocolo de actuación para Pericias Informáticas*

Continuando esta aproximación procedimental desde lo general hacia lo específico que en este capítulo presentamos, nos resulta relevante recuperar aspectos descriptos en el “Protocolo de Actuación para Pericias Informáticas” del Poder Judicial de la Provincia de Neuquén, redactado por el Dr. Gómez, debido a la claridad y pertinencia con que se presentan los conceptos y por ser, al momento de redacción del presente trabajo, el único protocolo en su especie que existe por escrito y es de carácter público a nivel nacional.

### *Pericias sobre telefonía móvil en el marco de la informática forense*

Para comenzar, vamos a citar el encuadre que el protocolo presenta acerca de la pericia sobre telefonía celular como parte de la especialidad de informática forense. Las pericias sobre telefonía celular forman parte de la actividad pericial informática en lo que refiere a extracción de evidencia digital. Estas pericias sobre telefonía celular deben ser practicadas por un profesional de grado en Ciencias Informáticas.

En cuanto a la aplicación de metodología de informática forense, la actividad pericial informática sobre telefonía celular no se diferencia en demasía de cualquier otra fuente de evidencia digital, por tal motivo se deben respetar las cuatro fases principales, las cuales son:

- Identificación de las fuentes de evidencia digital
- Preservación de la evidencia digital
- Análisis forense
- Presentación de los resultados de la pericia informática.

El origen de las pericias sobre telefonía celular (Mobile Forensics) como parte de la especialidad de Informática Forense data de aproximadamente el año 1984, año en el que el FBI y otras agencias de investigación y apoyo a la Justicia comenzaron a desarrollar programas de especialización para facilitar el análisis de evidencia digital.

En la actualidad la especialidad de Informática Forense se extiende a todas las áreas donde exista evidencia digital para ser presentada en carácter de prueba científica en el marco de un proceso judicial.

A continuación se detallan ciertas particularidades propias de la especialidad pericial informática sobre teléfonos celulares:

1. En el mercado existe una inmensa variedad de modelos de teléfonos celulares, con sistemas operativos propietarios, sistemas de archivos embebidos, así como también con disponibilidad de aplicaciones, servicios y periféricos. Para análisis de estos dispositivos se requiere conocimiento especializado en informática forense, a fin de contar un mayor número de opciones para dicho análisis.
2. El perito informático debe contar con la mayor cantidad posible de técnicas y herramientas forenses, y aplicarlas en función de su experiencia, debido a la creciente cantidad de modelos de teléfonos celulares existentes en el mercado.
3. Los teléfonos celulares están diseñados para comunicarse con la red de telefonía celular y con otras redes de datos mediante networking, vía Bluetooth, Infrarrojo y/o Wi-Fi. La mejor forma de preservar los datos del teléfono celular es aislarlo de las redes cercanas, en la medida en que esto sea posible.
4. Los teléfonos celulares pueden contar con diversas funcionalidades de almacenamiento de información digital e incluso sincronizar información con almacenamientos de datos online. Resulta necesario aplicar más de una herramienta forense para extraer datos de un teléfono celular y sus dispositivos de almacenamiento asociados.
5. Resulta esencial verificar la precisión de los datos extraídos desde estos dispositivos utilizando, o complementando, las técnicas con más de una herramienta forense, ya que existen situaciones en las que las herramientas forenses utilizadas para extraer la información digital pueden tener incompatibilidades o bien emitir reportes con información errónea.
6. El volumen de información digital contenido en los celulares continúa en aumento diariamente pese a que la cantidad de datos almacenados por éstos es pequeña, si se la compara con la capacidad de almacenamiento de información digital que tienen las computadoras.
7. Los tipos de datos contenidos en los teléfonos celulares y la forma en que éstos son utilizados está en evolución constante. La popularidad de los llamados teléfonos inteligentes hace que ya no sea suficiente la extracción

de agendas de contactos, históricos de llamadas, mensajes de texto, fotografías digitales, entradas de agenda personal, notas y otros archivos multimedia. Muchas aplicaciones instaladas en dichos dispositivos deben ser analizadas, ya que pueden contener información sensible como contraseñas, datos de geolocalización o históricos de navegación en Internet.

8. Las formas de extraer datos desde los teléfonos celulares podrían variar dependiendo de las técnicas que se utilicen para ello. Dependiendo de la finalidad y profundidad con la que se requiera determinada información en el marco de una investigación judicial podrían requerirse solamente algunos datos del teléfono celular o bien una extracción completa del sistema de archivos embebido y/o de la memoria física del teléfono.

Al igual que en otras actividades periciales de informática forense, el celular es una fuente de evidencia digital sobre la que aplican procedimientos operativos estándares (SOPs). Los buenos SOPs no deben contener o mencionar el nombre del hardware/software, ya que ello requiere de la experiencia del perito informático a la hora de seleccionar la herramienta de informática forense que le ofrece los mejores resultados para el caso.

#### *Cuestiones procedimentales*

En el caso que el tiempo lo permita, se debería realizar, previo al allanamiento, una investigación minuciosa con el objeto de identificar con precisión la ubicación y características técnicas generales de los elementos a secuestrar por medio de inteligencia policial.

Para aquellos casos en el que se involucren procedimientos judiciales en empresas o instituciones de gran envergadura, se procurará obtener información, a priori, tendiente a conocer las características generales de la infraestructura tecnológica y hardware existente en el lugar del hecho.

La actuación profesional del Perito es principalmente una actividad de laboratorio y de asesoramiento científico al operador judicial que es responsable de la investigación penal.

La pericia informática conlleva tiempos elevados de trabajo y no es posible realizarla sobre grandes cantidades de elementos. Debe evitarse el secuestro masivo de elementos informáticos, en especial CDs, DVDs, los que sólo han de ser enviados a

peritaje únicamente si se tienen presunciones con un alto grado de verosimilitud de poseer la evidencia buscada.

Recuperamos a continuación lo más relevante del listado de actividades a realizar durante el allanamiento:

1. Se deben separar las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Si es una empresa, se debe identificar al personal informático interno (administradores de sistemas, programadores, etc.) o a los usuarios de aplicaciones específicas que deban someterse a peritaje. Se debe dejar registrado el nombre del dueño o usuarios del equipamiento informático. Siempre que sea posible obtener contraseñas de aplicaciones y dejarlas registradas en el acta de allanamiento.
2. Se debe fotografiar, si es posible, todos los equipos informáticos antes de moverlos o desconectarlos, y realizar una toma fotografía completa del lugar donde se encuentren los equipos informáticos. Además tomar fotos de las pantallas de las computadoras, si están encendidas. Excepcionalmente, si se debiera inspeccionar los equipos informáticos o material tecnológico en el lugar del hecho, puede ser conveniente realizar una filmación o bien una descripción del trabajo que se lleva a cabo ante los testigos.
3. Evitar tocar el material informático sin uso de guantes descartables. Dependiendo el objeto de la investigación, el teclado, monitores, mouse, CDs, DVDs, etc., pueden ser utilizados para análisis de huellas dactilares, ADN, etc.
4. Si los equipos están apagados deben quedar apagados, si están prendidos deben quedar prendidos y consultar con un especialista la modalidad de apagado (En caso de no contar con asesoramiento, proceder a apagarlos desenchufando el cable de corriente desde el extremo que conecta al gabinete informático).
  - a. Si los equipos están apagados, desconectarlos desde su respectiva toma eléctrica y no del enchufe de la pared.
  - b. Si son notebooks o netbooks es necesario quitarles la o las baterías y proceder a secuestrar los cables y la fuente de alimentación.
5. Identificar si existen equipos que estén conectados a una línea telefónica, y en su caso el número telefónico para registrarlo en el acta de allanamiento.



6. Impedir que nadie realice búsquedas sobre directorios o intente ver la información almacenada en los dispositivos ya que es posible alterar y/o destruir evidencia digital (esto incluye intentar hacer una “copia” sin tener software forense específico y sin que quede documentado en el expediente judicial el procedimiento realizado).
7. Identificar correctamente todo el material tecnológico a secuestrar:
  - \*Siempre debe preferirse secuestrar únicamente los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadoras, notebooks y discos rígidos externos). Respecto a DVD, CDs, pendrives, etc., atento a que pueden encontrarse cantidades importantes, debe evitarse el secuestro de este material si no se tiene una fuerte presunción de hallar la evidencia en estos medios de almacenamiento.
  - \*Rotular el hardware que se va a secuestrar con los siguientes datos:
    - i. Para computadoras, notebooks, netbooks, celulares, cámaras digitales, etc.: N° del Expediente Judicial, Fecha y Hora, Número de Serie, Fabricante, Modelo.
    - ii. Para DVDs, CDs, Pendrives, etc: almacenarlos en conjunto en un sobre antiestático, indicando N° del Expediente Judicial, Tipo (DVDs, CDs, Pendrives, etc.) y Cantidad.
  - \*Cuando haya periféricos muy específicos conectados a los equipos informáticos y se deban secuestrar, se deben identificar con etiquetas los números de los cables para indicar dónde se deben conectar. Fotografiar los equipos con sus respectivos cables de conexión etiquetados.
8. Usar bolsas especiales antiestática para almacenar discos rígidos y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.
9. Precintar cada equipo informático en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas. Es responsabilidad del personal policial que participa en el procedimiento el transporte sin daños ni alteraciones de todo el material informático hasta que sea peritado.
10. Resguardar el material informático en un lugar limpio para evitar la ruptura o falla de componentes. No deberán exponerse los elementos secuestrados a

altas temperaturas o campos electromagnéticos. Los elementos informáticos son frágiles y deben manipularse con cautela.

11. Mantener la cadena de custodia del material informático transportado. Es responsabilidad del personal policial la alteración de la evidencia antes de que sea objeto de una pericia informática en sede judicial. No se podrá asegurar la integridad de la evidencia digital (por lo tanto se pierde la posibilidad de utilizar el medio de prueba) si el material informático tiene rotos los precintos al momento de ser entregado, siempre que no esté descripta en el expediente judicial la intervención realizada utilizando una metodología y herramientas forenses por profesionales calificados.

#### *Etiquetas de seguridad para dispositivos informáticos*

Introducimos a continuación un resumen del “Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos” redactado por el Dr. Gómez para el Poder Judicial de la Provincia de Neuquén, que continúa la línea procedimental presentada en los párrafos anteriores.

Las etiquetas son empleadas con el propósito de mantener la cadena de custodia de los elementos probatorios, desde su secuestro hasta la finalización del proceso judicial, a fin de garantizar la autenticidad e integridad de la evidencia. Es imposible atribuir responsabilidades por el faltante de elementos si no se identifica y asegura el material que se envía a peritaje "desde el momento del allanamiento". Estas etiquetas de seguridad evitan fallas en el procedimiento de secuestro/transporte de los elementos probatorios.

Las etiquetas de seguridad deberán ser entregadas al Fiscal o al Oficial actuario de la Policía al momento de expedir una orden de allanamiento (en una cantidad razonable a la magnitud del procedimiento). El instructivo sugiere adjuntar al acta de allanamiento una copia de la “Guía operativa para el secuestro de tecnología informática”.

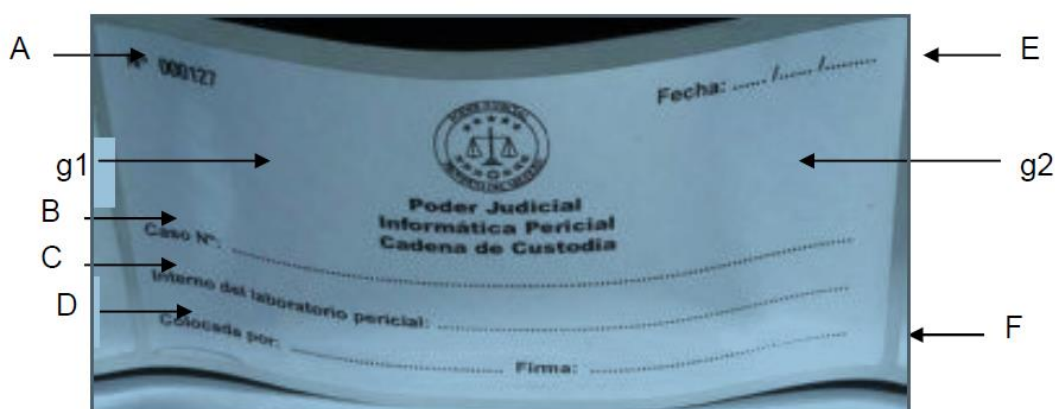
Durante el procedimiento judicial, las etiquetas serán colocadas por el personal policial en todos aquellos lugares que permitan la apertura de un equipo informático, bloqueando cualquier conector de energía eléctrica o que permita el acceso al dispositivo. El personal policial registrará en el acta de allanamiento todos los números de serie de las etiquetas de seguridad utilizadas.

Al finalizar el procedimiento, deberán reintegrarse al organismo judicial las etiquetas de seguridad que no hayan sido utilizadas, las que serán resguardadas por un funcionario para usos posteriores.

Una vez que los objetos secuestrados ingresen al laboratorio pericial, se realizará una inspección general, dejando constancia de cualquier alteración o ausencia de etiquetas de seguridad.

Finalizada la pericia, se colocarán nuevas etiquetas de seguridad, detallando los números de serie en el dictamen y se remitirán los secuestros a la dependencia de origen.

Formato de la etiqueta:



A: Número de serie: Identificador único e irrepetible que debe registrarse al colocar la etiqueta de seguridad en un dispositivo informático (se detalla en el acta de allanamiento, oficio elaborado por un funcionario judicial o dictamen del perito).

B: Número de Expediente-Datos del Juzgado o Fiscalía-Carátula. Opcional: Lugar donde se encuentra el objeto.

C: Código para uso interno del Laboratorio Pericial (no completar).

D: Nombre y apellido del responsable que colocó la etiqueta de seguridad.

E: Momento en que se realizó el procedimiento judicial. Formato: dd/mm/aaaa

F: Firma del responsable que colocó la etiqueta de seguridad.

g1 y g2: Espacios opcionales para la firma de testigos.

#### *Procedimiento aplicable a telefonía móvil*

Este protocolo incluye un detallado procedimiento para pericias informáticas sobre telefonía celular, cuyas actividades/etapas citamos a continuación. Se incluyeron al

protocolo original algunas especificaciones que para nuestro criterio son relevantes, sin embargo el esquema no fue alterado.

1. Verificar que el requerimiento judicial cumpla las pautas establecidas en el apartado d) del Protocolo de Actuación para Pericias Informáticas (“Del requerimiento judicial”).

*“Cuando sea requerido, el Perito evacuará las consultas previas de los operadores judiciales para eliminar ambigüedades y definir el alcance de los puntos de pericia en lo que respecta a los servicios de informática forense.*

*Conforme lo prescripto por el Código Procesal Penal y Correccional, sólo se podrán requerir informes periciales cuando para descubrir o valorar alguna evidencia sea necesario poseer conocimientos especiales en informática forense. Se debe proveer toda la información necesaria para realizar la tarea pericial, de manera clara y precisa.*

*El oficio con los puntos de pericia deberá enviarse desde el organismo requirente indefectiblemente junto con el material probatorio que será sometido a análisis forense. En dicho oficio deberán constar los números de serie de las etiquetas que resguardan el material probatorio, y que fueran detalladas en el acta de allanamiento.”*

*“Sólo se realizarán pericias que involucren la utilización del hardware y software para informática forense y aquellas que requieran la experticia de un profesional. Quedan excluidas del servicio de pericias informáticas toda tarea administrativa o técnica que no sea propia de la disciplina (tareas de transcripción de texto o simplemente dactilográficas, tareas de ordenamiento de información o cruzamiento de datos, tareas de impresión, tareas de escucha, tareas de filmación, elaboración de copias simples conocidas como backups o de resguardo de dispositivos de almacenamiento de información digital).*

*En función a la metodología de trabajo establecida para la actividad pericial informática, no se realizan backups sino que se generan “imágenes forenses” de los dispositivos que contienen información digital (copia bit-a-bit de la evidencia digital – en un formato propietario del software forense utilizado- únicamente a los efectos de realizar sobre ella el análisis forense). La imagen forense es el resultado de un procedimiento metodológico que sirve únicamente para prevenir una posible mala praxis del perito, evitando la contaminación de la prueba. Un backup –por sí mismo- es un procedimiento invasivo que altera la evidencia digital y no conserva información digital oculta o remanente que es de especial utilidad para la pericia informática.”)*

2. Priorizar el caso conforme los criterios detallados en el apartado e) del Protocolo de Actuación para Pericias Informáticas (“De la priorización de casos urgentes”).

*(“Únicamente se establecerá prioridad en pericias nuevas sobre aquellas que estén en lista de espera cuando se trate de causas con personas detenidas, debiendo ello ser explícitamente ser indicado en el oficio con el requerimiento judicial.*

*Asimismo, tienen prioridad aquellas causas judiciales por delitos que prevean penas severas por tratarse de bienes jurídicos protegidos de suma relevancia, como la vida o la integridad sexual con autores ignorados, en los que el paso del tiempo ponga en riesgo el devenir de la investigación.*

*En caso de tener dos pericias informáticas con el mismo nivel de urgencia, se dará trámite por orden de ingreso.*

*El especialista podrá brindar una estimación del tiempo requerido para el inicio de la pericia en función de la capacidad operativa disponible, las pericias en trámite y aquellas que estén en lista de espera, conforme las estadísticas propias de la actividad.”)*

3. Dar ingreso al material probatorio siguiendo los lineamientos del apartado del Protocolo de Actuación para Pericias Informáticas (“Del traslado y recepción del material secuestrado”).

*(“...Se cotejará la existencia de los precintos sobre los secuestros y la correcta identificación de los elementos enviados a peritaje. En caso de detectarse la alteración o ausencia de precintos de seguridad, se dejará constancia. Cada una de las personas que haya trasladado los elementos probatorios deberá dejar registrada su intervención con los medios que se establezcan.”)*

4. Determinar si el teléfono celular está encendido o apagado.

- a) Si está apagado, debe quedar apagado. Observación: Si el teléfono está apagado y se lo conecta al cargador es como si se lo hubiera encendido. Por esta razón se recomienda esperar hasta que se pueda iniciar el dispositivo en el modo de recuperación o en modo a prueba de fallos para la recolección de datos y en esta situación conectarlo al cargador.

- b) Si está encendido debe ser aislado de la red de telefonía celular lo antes posible con la opción que se estime apropiada, dentro de lo posible mantener la batería cargada y manipularlo lo menos posible. Se recomienda no apagar el equipo por la posibilidad de que se pierdan datos ya sea porque la batería se

agotó o porque ocurrió alguna pérdida de señal de la conexión con la red telefónica. Los datos de carácter temporal se perderán con el apagado del equipo. Al encenderlo, es posible que el dispositivo tenga una clave de acceso y por consiguiente el acceso al celular será restringido.

- i) Configurando el modo “Avión” en el teléfono celular, si lo permite. En el Modo Avión el celular no puede enviar o recibir llamadas telefónicas, mensajes de texto, mensajes con imágenes o mensajes de video; el usuario no podrá navegar por internet o utilizar los dispositivos de Bluetooth. El resto de las aplicaciones siguen en funcionamiento (reproductor de música, juegos, agenda, etc.) y pueden seguir siendo utilizadas. En los dispositivos en general, se debe oprimir el botón de apagado y seleccionar “Modo Avión”. Otro modo es seleccionar “Menú” de la pantalla inicial, luego “Configuración” o “Ajustes”, luego la opción “Redes Inalámbricas” o “Wireless Networks”, y luego aparece la opción “Modo Avión”.
- ii) Colocándolo en una caja de Faraday
- iii) Encendiendo un inhibidor de señal en cercanía del teléfono celular.
- iv) Envolviéndolo con tres o más capas de papel de aluminio
- v) Apagando el teléfono y retirando la batería.
- vi) Si el dispositivo es de tipo GSM remover la tarjeta SIM, acción que deshabilita de forma efectiva todos los celulares de voz, SMS y transmisión de datos. No desactiva las redes inalámbricas. No funciona en dispositivos que no sean GSM, incluyendo los teléfonos CDMA (Code Division Multiple Access, Acceso Múltiple por división de Código) o iDEN (Integrated Digital Enhanced Network, Red Mejorada Digital Integrada) y tecnología inalámbrica creada por Motorola.
- vii) La suspensión de la cuenta con el proveedor del servicio de la red inalámbrica celular, deshabilita de manera efectiva todos los celulares de voz, SMS y transmisión de datos, pero requiere la autorización del juez.

Según el tipo de dispositivo, evitar tocar la pantalla táctil.

5. Obtener información sobre el modelo del teléfono celular y planificar la estrategia para la extracción de evidencia digital
  - a) Identificar la tecnología general del teléfono celular
  - b) Localizar cables, drivers y determinar el software o hardware forense a utilizar para la pericia informática. La selección de herramientas forenses para una pericia informática sobre telefonía celular depende de diversos factores, como el nivel de detalle requerido en los puntos de pericia, el modelo de teléfono celular en cuestión y la presencia de otras funcionalidades de almacenamiento externo del dispositivo
  - c) Determinar funcionalidades del teléfono celular y posibles datos almacenados en el mismo.
  - d) Si el teléfono celular no tiene puerto de datos, no se cuenta con el cable de datos, o no existe software o hardware forense disponible para dicho modelo, se registra esta situación
6. Consultar las especificaciones técnicas del teléfono celular y sus capacidades de almacenamiento de datos. Se recomienda los sitios web [www.phonescoop.com](http://www.phonescoop.com) o [www.mobileforensicscentral.com](http://www.mobileforensicscentral.com)
7. Preservar y analizar las fuentes de evidencia digital siguiendo las pautas prescriptas en el Protocolo de Actuación para Pericias Informáticas (“Del análisis forense”)

*“Todo el proceso forense está conducido por una metodología de trabajo para el manejo de evidencia digital. Durante el desarrollo de una pericia se utilizan procedimientos operativos estándares con un control de calidad previo realizado en el laboratorio pericial.*

*El Perito trabaja con un equipo profesional, con funciones específicas asignadas y una organización interna, tanto administrativa como profesional. Las distintas actividades están segmentadas y pueden separarse, permitiendo un análisis autónomo y específico, sin perjuicio de su unión respecto a un resultado. Existe una clara distinción de roles dentro del laboratorio, a saber: asistente técnico, perito informático auxiliar y perito informático oficial. Se considera la capacitación interna para llevar adelante la actividad forense, la idoneidad y la responsabilidad asignada, y el nivel jerárquico conforme experiencia y experticia. La definición del alcance y líneas de investigación forense, así como la elaboración de dictámenes queda a cargo de los peritos de mayor jerarquía y experiencia.”)*

- a) Tarjeta de Memoria Externa
  - i. Realizar una imagen forense con la herramienta de informática forense apropiada.
  - ii. Extraer la evidencia digital que resulte relevante conforme los puntos de pericia que hayan sido indicados.
- b) Tarjeta SIM
  - i. Generar una SIM clonada o leer la información digital de dicho dispositivo utilizando un lector de SIM protegido contra escritura.
  - ii. Si el SIM está bloqueado por PIN, se deja constancia o se utiliza el PUK en caso de estar disponible.
  - iii. Si el SIM no está bloqueado, se extrae la información digital relevante al caso.
- c) Equipo de telefonía celular.
  - i. Aislar el dispositivo de la red de telefonía celular previamente a la extracción de información digital y si es posible, durante todo el proceso.
  - ii. Realizar una extracción física de la memoria del teléfono celular o bien una extracción lógica utilizando todas las herramientas forenses apropiadas, tanto de hardware como de software
  - iii. Verificar los resultados obtenidos
    - a. Que los datos de salida tengan el formato adecuado al tipo de dato asociado.
    - b. Que las fechas y horas sean consistentes
    - c. Que todos los datos requeridos pudieron ser extraídos:
      - 1. Mediante comparación con datos obtenidos desde el teléfono celular
      - 2. Utilizando más de una herramienta forense y comparando resultados.
      - 3. Validando mediante valores hash distintos artefactos digitales del teléfono celular.
- 8. Documentar los resultados en un reporte informático forense
- 9. Elaborar el dictamen para dar respuesta a los puntos de pericia informática haciendo referencia a la evidencia digital detallada en el reporte informático



forense, siguiendo las pautas establecidas en el apartado h) del Protocolo de Actuación para Pericias Informáticas (“De la presentación del dictamen”)

10. Remitir el dictamen junto a los elementos probatorios siguiendo los lineamientos de apartado i) del Protocolo de Actuación para Pericias Informáticas (“De la remisión del material secuestrado”)

*(“Una vez finalizada la pericia, se remitirá el dictamen y el material secuestrado al organismo de origen. Los elementos analizados deberán ser resguardados con los medios adecuados para preservar la integridad y la autenticidad de la evidencia digital.”)*

*Los elementos probatorios que contengan evidencia digital deberán resguardarse hasta finalizar el proceso judicial, siendo imprescindible su conservación ya que permite a futuro -y si fuera necesario- repetir o ampliar la pericia.”)*

El perito informático debe aplicar los conocimientos especializados sobre la materia y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional.

Algunos de los documentos de referencia que se utilizan en el Laboratorio Pericial Informático para las pericias informáticas sobre telefonía celular.

- NIST(2007), Guidelines on Cell Phone Forensics, <http://csrc.nist.gov/>
- ACPO & 7Safe (2008), Guide for Mobile phone seizure and examination. Good Practice Guide for Computer-Based Electronic Evidence, <http://www.7safe.com/>
- SWGDE (2013), SWGDE Best Practices for Mobile Phone Forensics, <https://www.swgde.org/>
- Ayers, R., Dankar, A. & Mislán, R. (2009). Hashing Techniques for Mobile Device Forensics. Small Scale Digital Device Forensics Journal, 1-6.
- Brothers, S. (2011). How Cell Phone "Forensic" Tools Actually Work - Cell Phone Tool Leveling System. DoD Cybercrime Conference. 2011. Atlanta, GA
- Kessler, G. (2010). Cell Phone Analysis: Technology, Tools, and Processes. Mobile Forensics World. Chicago: Purdue University.
- Mislán, R.P., Casey, E., & Kessler, G.C. (2010). The Growing Need for On-Scene Triage of Mobile Devices. Digital Investigation, 6(3-4), 112-124

- Murphy, C. (2009). The Fraternal Clone Method for CDMA Cell Phones. Small Scale Digital Device Forensics Journal, 4-5.
- Murphy, C. (2010), Digital Forensics Magazine, <http://digitalforensicsmagazine.com/blogs/?p=80>
- Punja, S & Mislán, R. (2008). Mobile Device Analysis. Small Scale Digital Device Forensics Journal, Vol. 2, No. 1, 2-4.

### Recolección en Smartphones Android

En lo que resta del capítulo nos vamos a detener puntualmente en los dispositivos inteligentes que poseen Android. Esta sección fue elaborada en base al “Manual de Informática Forense II” de Darahuge y Arellano González. El manual propone un enfoque desde herramientas de código abierto. Actualmente en el Poder Judicial de la Provincia de Córdoba en lo que respecta a telefonía móvil no se emplean herramientas de este tipo, todo el software y hardware es licenciado y forense. En el próximo capítulo nos focalizamos en este tipo de herramientas.

#### *Elementos a recolectar*

1. Tipo y versión del sistema operativo.
2. Llamadas realizadas (fecha, hora, duración.).
3. Llamadas recibidas (fecha, hora, duración.).
4. Último número marcado (LDN \_ Last Dialed Number).
5. Lista de contactos.
6. Mensajes de texto.
7. Fotografías.
8. Archivos.
9. Archivos borrados.
10. Espacio desperdiciado.
11. Videos.
12. Agenda.
13. Correo electrónico.
14. Tonos de timbre (ringtones) personalizados, los cuales pueden ser identificados por un testigo permitiendo ubicar a alguien en un determinado lugar.
15. Ubicación, establece la ubicación física de una persona o su dirección de traslado o viaje.

16. Tarjeta SIM, contiene un procesador con memoria no volátil, se utiliza como un dispositivo de almacenamiento de información relacionada con el suscriptor, incorporada a la red global de celulares GSM. En la tarjeta se puede obtener:
- i. Identificador de área local, identifica donde está ubicado actualmente el celular. Este valor permanece almacenado en la SIM luego de pagado el celular. Es útil para identificar cual fue la última ubicación donde se utilizó el celular.
  - ii. Número de serie, se puede obtener sin tener el PIN (Personal Identification Number) e identifica al SIM mismo.
  - iii. Numero de cliente, se refiere al IMSI (International Mobile Subscriber Identity), que es el número de identificación del cliente que permitirá, junto con la ayuda del proveedor de servicio, identificar al cliente propietario del celular.
  - iv. Número de teléfono del celular. Se refiere al MSISDN (Mobile Subscriber Integrated Services Digital Network).

#### *Recolección de información de la tarjeta SIM*

- Mensajes de Texto: existe un espacio en la tarjeta que mostrara los últimos doce mensajes enviados. Los celulares almacenan los mensajes en memoria. La mayoría utiliza la memoria de la tarjeta SIM primero antes de usar la memoria interna.
- Mensajes Borrados: similar al borrado de archivos en un disco rígido, el primer byte es configurado en cero. Esto significa que los mensajes borrados pueden recuperarse, excepto el primer byte mientras no se sobre escriba con nuevos mensajes.
- Guía de Teléfonos. La mayoría de los celulares tiene la capacidad de almacenar un mínimo de 100 números marcados con su respectivo nombre asociado.
- Últimos números marcados. La mayoría de las tarjetas almacenan aproximadamente los últimos cinco números marcados en la tarjeta SIM. No obstante, la mayoría de los celulares almacenan muchos más en la tarjeta interna de memoria del celular.

*Procedimiento para la duplicación de los dispositivos USB de almacenamiento (UMS-USB-Mass Storage) en dispositivos Android*

Los dispositivos Android puede tener una tarjeta digital externa de seguridad (SD-Secure Digital) o una tarjeta multimedia embebida (eMMC- Embedded MultiMediaCard) que permite almacenar gran cantidad de información para los usuarios. Este almacenamiento existe porque los datos de las aplicaciones del usuario guardados en `/data/data` están separados por razones de privacidad y seguridad.

La copia de fotos, música y video, archivos de oficina, etc., entre un dispositivo Android y la computadora se realiza a través de la gran capacidad de almacenamiento de las particiones FAT y resulta más flexible para el usuario. Los datos sensibles quedan protegidos y los archivos portables quedan accesibles al usuario. El procedimiento recomendado es efectuar la duplicación sin remover del dispositivo las tarjetas SD y eMMC, utilizando el comando `dd` (`dc3dd`, del Departamento de Defensa- Centro del Ciber Crimen).

1. Crear una máquina virtual con el sistema operativo Linux,
2. Descargar, descomprimir, compilar e instalar el programa `dc3dd`.
3. Desactivar la configuración de auto montaje de los dispositivos.
4. Conectar el bloqueador de escritura por hardware a la computadora de informática forense y conectar el dispositivo móvil con Android al bloqueador de escritura.
5. Determinar los dispositivos de almacenamiento o interfaces USB que son reconocidos por el sistema operativo:

`#dmesg`

La información mostrada en el registro del kernel es la siguiente: en el caso de teléfonos inteligentes muestra tres interfaces USB:

- CD-ROM para la instalación de dispositivos.
  - eMMC dispositivo UMS.
  - Tarjeta SD y dispositivo UMS.
6. Ejecutar nuevamente el comando `dmesg`:

`#dmesg`.

El resultado mostrará la diferencia en los dispositivos de almacenamiento: `/dev/sdb` es de 8 GB, es decir la eMMC, y la de 2 GB es la tarjeta SD en `/dev/sdc`.

7. Al adquirir la imagen del dispositivo, a través de un script, o utilizando el comando `dd` o el comando `dc3dd`.

El comando efectúa múltiples archivos de 2 GB; Hash MD5 y SHA1 de la imagen y crea un archivo de registro (log).

El perito podrá modificar los parámetros acorde al dispositivo.

En el caso de que las aplicaciones (apps) se encuentren instaladas en la tarjeta SD, los datos estarán encriptados y no se podrán leer; no obstante, si la tarjeta no está montada en la computadora de Informática Forense, los archivos desencriptados `.apk` montan en `/mnt/sec`. Si se deben analizar los archivos `.app` y `.apk`, el perito tendrá que realizar una copia de cada uno de ellos.

8. Registrar, documentar y/o capturar pantallas con la información requerida.

### *Procedimientos para la recolección lógica en dispositivos Android*

Las técnicas de recolección lógica extraen la información que se encuentra almacenada o asignada. La forma de obtenerla es accediendo al sistema de archivos y le ofrecen al perito no solo la facilidad para la recolección de datos, sino que también obtienen una cantidad de información considerable para la posterior etapa de análisis acorde a la requisitoria pericial.

La recolección lógica en Android no requiere el acceso al dispositivo como usuario root. La opción de Depuración USB (USB Debugging) se utiliza con fines de desarrollo para copiar datos entre la computadora y el dispositivo, instalar aplicaciones en el dispositivo sin preguntar y ver los registros de eventos, por lo tanto debe estar habilitada.

Para la extracción lógica de datos se pueden utilizar diferentes técnicas:

#### I. Comando `adb`

Es una herramienta del paquete de desarrollo de Android con Licencia Pública General (GNU GPL – Genral Public License) de línea de comando que permite comunicarse con una instancia del emulador de Android o con el dispositivo directamente; es una aplicación del tipo cliente-servidor.

La herramienta obtiene información de manera recursiva del dispositivo y la copia en la estación de trabajo de Informática Forense. Si se tiene acceso al dispositivo Android como usuario root se está ejecutando una ROM personalizada, el servicio que se ejecuta de `adb` en el dispositivo sólo funciona con permisos del intérprete de comandos o Shell, por lo que información relevante no se puede recolectar.

No obstante, se puede acceder a otros archivos. Si se intenta copiar archivos de los cuales el usuario del Shell no tiene permisos, simplemente no se copiarán.

Copiar los archivos desde el dispositivo con el comando *adb*, en el caso de poseer los privilegios suficientes para el acceso desde el Shell. Si no se tienen permisos de root, se puede acceder a ciertos archivos de importancia como aplicaciones no encriptadas, a la mayor parte del directorio */tempfs* que puede contener datos de usuario (historial de navegador web) e información del sistema en los directorios */proc*, */sys* y otros directorios que tengan acceso de lectura.

Registrar, documentar y /o capturar pantallas con la información requerida.

## II. Resguardos

Una herramienta muy difundida para realizar resguardos o backup es Rerware My Backup Pro: resguarda los datos utilizando el proveedor de contenidos y el directorio */data/data*, en el caso de que el dispositivo tenga permisos de acceso de root. Esta aplicación funciona también en Windows Mobile, Blackberry y Symbian OS. Las opciones que tiene el usuario para realizar resguardos es guardar la información en la tarjeta SD y en el servidor de Rerware. La herramienta efectúa el resguardo en forma local en la tarjeta SD en un único archivo SQLite. La aplicación puede resguardar:

Archivos de instalación de aplicaciones (si el teléfono tiene acceso de usuario root, incluye APK, data y Enlaces de comercios o tiendas).

- Contactos.
- Registros de llamadas.
- Marcadores de navegador web.
- SMS.
- MMS
- Configuraciones del sistema.
- Pantalla de inicio.
- Alarmas.
- Diccionarios.
- Calendarios
- Lista de reproducción de música.
- Aplicaciones de terceros integradas.

Android recientemente ha desarrollado una aplicación de manejo de resguardos que se integra al resto de las aplicaciones; el resguardo es manejado por Android y Google.

Esto permite al usuario un resguardo continuo de sus aplicaciones guardándolo en la red (cloud) en un servidor de almacenamiento remoto, con el fin de ofrecerle a un usuario un punto de restauración en el caso de que cambie de dispositivo o pérdida de datos.

El perito deberá conocer que tipos de resguardos existen para luego analizar el contenido de la tarjeta SD, así como también, si es posible, la computadora o notebook del usuario.

### III. Herramienta AFLogical

La herramienta AFLogical se distribuye en forma libre para los organismos de gobierno y seguridad, previo registro e identificación en el sitio de la herramienta.

La aplicación está desarrollada por Viaforensics y utiliza las mismas técnicas que los productos comerciales de telefonía forense. El programa permite extraer la información almacenada y compartida de los proveedores de contenido (SMS, MMS, contactos, calendario, Facebook, Gmail, etc.). AFLogical aprovecha la arquitectura de los proveedores de contenido para acceder a los datos almacenados en el dispositivo.

Se debe habilitar la opción de Depuración de USB para utilizar la herramienta AFLogical para la extracción de datos. El formato del resguardo es en CSV (Valor Separado por Comas – Comma Separated Value) y un archivo info.xml, el cual brinda información detallada del dispositivo y de las aplicaciones instaladas. La herramienta puede resguardar los siguientes proveedores de contenido:

- Marcadores del navegador web.
- Búsquedas en el navegador web.
- Calendario.
- Asistentes del calendario.
- Eventos de calendario.
- Propiedades extendidas de calendario.
- Registro de llamadas.
- Contactos.
- Extensiones de contactos.
- Grupos de contactos.
- Organizaciones de contactos.
- Teléfonos de contactos.
- Configuración de contactos.
- Discos externos (imágenes, pre visualizaciones, video).

- Mensajería instantánea (cuentas, charlas, mensajes, invitaciones, proveedores, configuración de los proveedores en la mensajería instantánea).
- Almacenamiento interno (imágenes, pre visualizaciones, video).
- Mapas.
- MMS.
- Notas.
- Gente eliminada.
- Almacenamiento de teléfono.
- Historial de búsquedas.
- SMS.
- Charlas de mensajerías instantánea.
- Actividades sociales.

#### *Procedimientos para la recolección física en dispositivos Android*

La recolección física permite obtener datos que han sido eliminados e información obsoleta de archivos. Las técnicas de recolección física en Android pueden ser por:

Hardware: métodos que conectan hardware al dispositivo o físicamente extraen los componentes del dispositivo móvil. El equipamiento requerido y su respectiva capacitación suelen ser muy costosos:

- Las técnicas para verificar y probar los cables e interconexiones en los circuitos impresos en la placa (PCB – printed circuit board) de celulares o equipos inalámbricos responde al estándar de la IEEE 1149.1 (Standard Test Access Port and Boundary Scan Architecture) denominado JTAG (Join Test Action Group). Requiere de conocimientos específicos y solo se puede realizar en un laboratorio con los instrumentos adecuados y la autorización judicial correspondiente. El estándar efectúa pruebas de acceso a los puertos (TAP- Test Access Port) que permiten el ingreso a la unidad central de procesamiento (CPU). Las señales que se prueban en los dispositivos móviles pueden ser:
  - TDI (prueba de entrada de datos)
  - TDO (prueba de salida de datos)
  - TCK (prueba de reloj)
  - TMS (prueba de selector de modo)



- TRST (prueba de reinicio). Es opcional.

Esta técnica realizada de la manera correcta permite la descarga de memoria Flash NAND y re ensamblado y funcionamiento normal del equipo sin pérdida de datos.

- La técnica de remoción de la tarjeta de memoria Flash NAND se puede utilizar para recuperar datos en los dispositivos dañados y elude la configuración de protección de acceso al dispositivo por contraseña. El procedimiento es destructivo y generalmente es muy difícil volver a conectar la memoria Flash NAND al circuito impreso de la placa y que dispositivo vuelva funcionar correctamente. Por lo tanto solo es recomendable en los casos en el que el dispositivo se encuentre dañado y no se vuelva a utilizar.

Software: técnicas que se ejecutan como programas en el dispositivo con acceso de root y obtienen una imagen física de todas las particiones de datos. Las ventajas sobre las técnicas de hardware son las siguientes:

- Facilidad para su ejecución.
- Generalmente, proveen acceso al sistema de archivos y permiten una copia completa de todos los archivos lógicos simplificando posteriormente el análisis de la información.
- Reduce el riesgo de daño del dispositivo o de la pérdida de datos.

Esta técnica requiere el acceso como usuario root al dispositivo y en Android no está habilitado en forma predeterminada, por lo tanto al cambiar los privilegios de acceso se producen modificaciones en el dispositivo. El procedimiento de acceso como usuario root varía según el fabricante y versión de Android y del Kernel o del núcleo del sistema operativo Linux. Por consiguiente, resulta ser una técnica con muchos obstáculos y agobiante para el perito.

Los tipos de acceso como usuario root pueden ser:

- Temporales, alcanzado por un programa del tipo explotación (aplicación que aprovecha la situación para tomar ventaja de esta, en este caso de acceso como usuario root y control total sobre el dispositivo) y que no sobrevive sino se reinicia el equipo. El demonio *adb* no se ejecuta como root en este caso.

- Acceso total a través de una ROM personalizada o modificada o un programa exploit de root persistente. El demonio *adb* se ejecuta como root mientras que la mayoría de los programas de root persistentes no lo tienen.
- Modo de recuperación alcanzado por el acceso a una partición recuperada o a una parte de la ROM personalizada o modificada. En este modo el demonio *adb* se ejecuta como root de la misma forma que lo hacen la mayoría de las particiones de recuperación modificadas.

Para el perito es preferible el acceso temporal como root o el acceso a través del modo de recuperación. La implementación de estas técnicas debe practicarse previamente en el laboratorio para evitar el daño o pérdida de datos en el dispositivo.

### *Etapas de Análisis de datos*

La mayoría de las herramientas y técnicas que se utilizan para el análisis de celulares en particular y las que se aplican en Informática Forense son válidas también en los dispositivos Android. Las herramientas a utilizar pueden ser de código abierto, de libre disponibilidad o productos comerciales o comandos del propio sistema operativo Linux.

Procedimiento para el análisis del núcleo del sistema operativo Linux

Registros de Eventos o sucesos del Núcleo

- I. En la estación de trabajo de telefonía forense, conectarse al dispositivos con USB Debugging habilitado, ejecutar el comando *dmesg*, no requiere permisos administrativos. El resultado extraído muestra información acerca de la fecha y hora, del hardware, actividades del dispositivo en el inicio del sistema y del núcleo del sistema operativo. Si el dispositivo no ha sido iniciado recientemente, la información del arranque del dispositivo ya no está disponible.
- II. Analizar la información en la línea de los mensajes de depuración del sistema y de las aplicaciones con el comando *logcat*. El resultado muestra el registro en línea de todas las tareas que se realizan en el dispositivo. Se puede obtener información de latitud y longitud, información de fecha y hora, detalle del uso de las aplicaciones, etc. Cada mensaje comienza con una letra que indica:
  - V: verbose, detallado y de menor prioridad.
  - D: debug, depuración.
  - I: information, información.
  - E: error.

- F: fatal.
  - S: silent, silencioso y de mayor prioridad donde no aparece nada escrito.
- III. Analizar en línea de las conexiones del teléfono móvil con el sistema GSM, utilizando el comando *logcat*. La información puede ser de interés para el perito ya que muestra los datos sobre:
- Fecha y hora de los eventos en formato Unix Epoch.
  - Comando AT utilizados por el celular para comunicarse.
  - Mensajes SMS: receptor, tamaño, fecha y hora.
  - Red y datos de la ubicación.
  - Información del proveedor de servicio.
- IV. Analizar la información en línea de los eventos utilizando el comando *logcat*. Se puede observar las acciones INSERT y SELECT en las bases de datos, por ejemplo en la *mmssms.db* en donde se almacenan los mensajes de texto.
- V. Analizar la información de los servicios, memoria, identificadores de proceso (PID), base de datos, cuentas de acceso a redes sociales, correos electrónicos, fecha y hora y otros elementos del sistema con el comando *dumpsys*.
- VI. Analizar la información del estado del sistema con el comando *dumpstate*. El resultado muestra la información por secciones que en su mayoría son obtenidas del pseudo directorio de procesos */proc*. El perito puede analizar en forma individual cada uno de los subdirectorios y archivos del directorio */proc* o analizar las secciones del comando *dumpstate*.
- VII. Analizar la información del estado del sistema con el comando *bugreport* que efectúa una combinación de los comandos *logcat*, *dumpsys* y *dumpstate* en un solo comando.
- VIII. Registrar, documentar y/o capturar pantallas con la información requerida.

Referencias:

<sup>(1)</sup>Darahuge, María Elena, Arellano González, Luis E. “Manual de Informática Forense II. (Prueba Indiciaria Informático Forense)”. Ed. Errepar. Primera Edición. Año 2012.

# **CAPÍTULO 6**

## ***ANÁLISIS DE HERRAMIENTAS FORENSES LICENCIADAS***

### Introducción

En este capítulo haremos foco en determinados aspectos del proceso de recolección, adquisición y posterior análisis de datos. Como adelantamos en el capítulo anterior, se presentan y comparan una serie de herramientas (hardware y software) de tipo forense y licenciadas.

La disponibilidad de herramientas de software forense para equipos móviles es considerablemente distinta a la de las computadoras personales. Mientras que las computadoras personales difieren de los teléfonos móviles desde una perspectiva de hardware y software, sus funcionalidades progresivamente se van haciendo más parecidas. Podemos mencionar que existen tanto herramientas de software forense (ya sean comerciales como open source) como herramientas de software no forense creadas para la administración del dispositivo, testing y diagnóstico. Las herramientas forenses típicamente se diseñan para la adquisición de datos tanto del dispositivo como del UICC sin alterar el contenido, y el posterior cálculo de un hash para garantizar la integridad de los datos adquiridos. Tanto las herramientas forenses como las no forenses usualmente utilizan los mismos protocolos y técnicas para comunicarse con el dispositivo. Sin embargo, las herramientas no forenses suelen permitir tráfico bidireccional irrestricto de información y omiten el cálculo de hash para asegurar la integridad. En la práctica, los especialistas suelen trabajar con una serie de herramientas tanto forenses como no forenses según lo amerite el caso.

La brevedad de los ciclos de vida de estos tipos de dispositivos obliga a los proveedores de herramientas a que continuamente actualicen las aplicaciones para proveerles a los examinadores soluciones forenses. La tarea de los fabricantes es destacable, sin embargo, existe un retraso entre la introducción de un nuevo smartphone en el mercado y la adecuación de las herramientas forenses a este. A su vez, existen en funcionamiento dispositivos móviles antiguos que también deben ser soportados, lo que hace que el escenario sea de creciente complejidad.

### Tipos de extracción

Consideramos relevante recuperar una taxonomía de las distintas formas de recolectar datos desde un dispositivo móvil. Esta clasificación no es bajo ningún punto de vista exhaustiva, simplemente recuperamos a nuestro criterio, las categorías válidas para la posterior comparación de herramientas.

*Extracción Manual:* generalmente se utiliza cuando no existen elementos compatibles para la extracción de la evidencia, se emplea como último recurso ya que altera de manera irreversible la prueba. Suele ser necesaria en teléfonos fabricados recientemente, cuando aún no existe actualización del software forense que soporte el equipo. Este método involucra la visualización directa de los datos almacenados en el smartphone. Para visualizar el contenido en la pantalla es necesaria la manipulación de botones, teclado y/o pantalla táctil. En este nivel de extracción es imposible recuperar información borrada. Si existe un volumen considerable de datos, una extracción manual puede consumir una gran cantidad de tiempo, por otra parte, puede suceder que inadvertidamente se modifiquen, borren o reescriban datos. Esta técnica requiere que los examinadores forenses realicen una grabación de cada una de las pantallas que se van visualizando al momento de la recolección, empleando el teclado (físico o pantalla táctil) y las funcionalidades del sistema operativo y las distintas aplicaciones. Este tipo de recolección no suele ser viable cuando la pantalla está dañada o ausente, al igual que los botones o el teclado. Se debe considerar también que el dispositivo puede estar configurado en un lenguaje desconocido para el investigador, dificultando la navegación por el menú.

*Recolección Lógica:* las técnicas de recolección lógica extraen la información que se encuentra almacenada o asignada. La forma de obtenerla es accediendo al sistema de archivos. La conectividad entre el dispositivo móvil y la estación de trabajo forense se obtiene o bien mediante cables o de forma inalámbrica. El examinador debe ser consciente acerca de las implicancias de seleccionar un tipo específico de conectividad, debido a que los distintos tipos de conexiones y sus protocolos asociados pueden resultar en la modificación de los datos originales (por ej. Mensajes de texto no leídos) o en diferentes cantidades o tipos de información extraída. Las herramientas de extracción lógica comienzan enviando una serie de comandos sobre la interfaz establecida desde la computadora hasta el dispositivo móvil. El dispositivo móvil responde basado en la solicitud del comando. La respuesta se envía a la estación de trabajo y es presentada al examinador con el fin de que este pueda elaborar reportes.

*Recolección Física:* permite obtener datos que han sido eliminados e información obsoleta en el sistema de archivos. La extracción física implica el copiado de bit por bit de la memoria flash completa del dispositivo móvil. Este método de extracción no sólo permite la adquisición de los datos intactos, sino que también de los datos ocultos y eliminados. Los datos eliminados pueden ser recuperados de varios niveles: el primer

nivel es el del sistema de archivos. Durante el proceso de reconstrucción del sistema de archivos, es posible, en muchos casos, recuperar los archivos eliminados. El segundo nivel es la recuperación de información eliminada de archivos de bases de datos. En algunos archivos de bases de datos que se pueden encontrar en los teléfonos inteligentes, es posible recuperar registros eliminados, como entradas de registros de llamadas, contactos, mensajes, etc. Los tipos de datos soportados obtenidos por medio de la extracción física incluyen a las contraseñas intactas y eliminadas, aplicaciones instaladas, Geotags, información de ubicaciones, archivos multimedia como fotos tomadas y vídeos grabados por el usuario, ubicaciones de GPS, correos electrónicos, chats, entre otros.

### Descripción de herramientas

#### UFED Touch Ultimate <sup>(1)</sup>

A continuación presentamos la herramienta UFED (Dispositivo Universal de Extracción Forense) Touch Ultimate, debido a que es instrumento principal para realizar los análisis forenses en el marco de la DACTI, como así también en otros poderes judiciales de la República Argentina.

Esta herramienta está diseñada para obtener datos de tarjetas SIM y teléfonos móviles que operan con tecnología GSM, TDMA y CDMA. UFED proporciona la capacidad de conectarse a través de un cable, Bluetooth o LrDA. La terminal UFED contiene un SO embebido con pantalla táctil, cables de datos para varios fabricantes y un lector de tarjetas SIM protegido contra escritura.

Fundada en 1999 por un equipo de profesionales con amplia experiencia en las áreas de telecomunicaciones y telefonía móvil, Cellebrite es una compañía global reconocida por sus avances tecnológicos en la industria móvil. Más de 20.000 UFEDs han sido desplegadas en fuerzas policiales y del orden público y agencias de seguridad en todo el mundo. Cellebrite es una filial de entera propiedad del Sun Corporation, una empresa japonesa que cotiza en bolsa.

El UFED Touch Ultimate permite la extracción, decodificación, análisis y generación de informes de datos móviles. Realiza la extracción física, lógica, del sistema de archivos y contraseñas de todos los datos (aunque hayan sido eliminados) del más amplio rango de dispositivos, que incluye teléfonos antiguos y comunes, teléfonos inteligentes, dispositivos GPS portátiles, tablets y teléfonos con chipsets de manufactura china.



UFED tiene como punto favorable una gran cobertura de modelos telefónicos, pero como toda herramienta de informática forense tiene limitaciones y no excluye la aplicación de otras técnicas especializadas y herramientas de informática forense durante la realización de una pericia informática sobre dispositivos de telefonía celular.

Esta herramienta permite desbloquear algunos modelos de teléfonos celulares que hayan sido protegidos con una contraseña, pero no tiene capacidad de desbloquear las protecciones de la tarjeta SIM mediante el uso del PIN. En estos casos se puede intentar hacer una clonación de la tarjeta SIM para acceder a la evidencia digital contenida en la memoria interna del dispositivo, pero si no es posible conocer a priori el PIN o el PUK se pierde la posibilidad de extraer la información digital del SIM.

Se incluyen a continuación una galería de imágenes disponible en el sitio oficial de la herramienta.





Con hardware propietario, una batería integrada, una interfaz de usuario intuitiva y una pantalla táctil, el UFED Touch Ultimate acelera el proceso de las investigaciones, cumpliendo con las demandas de la industria del análisis forense de dispositivos móviles. En la página web del fabricante se encuentra disponible el listado de equipos soportados por la herramienta.

La solución UFED Touch Ultimate viene con una gama de aplicaciones:

- UFED Physical Analyzer – La aplicación avanzada de decodificación, análisis y generación de informes
- UFED Phone Detective – Para una identificación instantánea de teléfonos móviles
- UFED Reader – Permite al personal autorizado compartir información con otras personas

Haremos mención también al UFED Touch Logical del mismo fabricante, que constituye una solución integral de análisis forense de dispositivos móviles para personal de intervención inmediata. Éste permite una extracción lógica rápida y

simplificada de los datos probatorios de una amplia variedad de dispositivos móviles. Está específicamente diseñado para el análisis forense de dispositivos móviles, provee las herramientas necesarias para extraer rápidamente la tarjeta SIM y la memoria de un dispositivo en un procedimiento de campo o en el laboratorio, de forma adecuada desde el punto de vista forense.

### XRY Complete <sup>(2)</sup>

El XRY es una aplicación de software diseñada para Windows, que permite realizar extracción forense de datos de manera segura, sobre una variedad de dispositivos móviles. Es una solución forense basada en el software pero incluye todo el hardware necesario para recuperar datos de estos dispositivos.

Existen básicamente 3 versiones:

- XRY Logical: según el proveedor, eficiente en el 80% de los casos. Proporciona una interfaz intuitiva y fácil de usar para analizar una amplia gama de teléfonos móviles mediante un proceso de examen protegido, para recuperar los datos de una manera segura desde el punto de vista forense. Permite crear un informe en minutos a prueba de manipulación, que se puede personalizar según las necesidades del usuario
- XRY Physical: permite ir a lo profundo del dispositivo, para extraer información borrada o protegida. Es un paquete de software para la recuperación física de datos. El volcado de memoria para cada dispositivo individual es una compleja estructura de datos, por lo que desde XRY han desarrollado esta herramienta para facilitar la lectura de la información.
- XRY Complete: es la solución integrada que combina los beneficios de la versión Logical y Physical.

A continuación y a modo ilustrativo, incluimos imágenes disponibles en la página del proveedor, en particular de la herramienta Complete.



Todas las versiones de XRY son desarrolladas por Micro Systemation AB, una compañía que cotiza en el mercado de valores sueco, creada en 1984. Desde el año 2003 la compañía solo se ha enfocado en el desarrollo de soluciones digitales de alta calidad para aplicaciones forenses que permitan el análisis de dispositivos móviles tales como teléfonos celulares, smartphones, dispositivos GPS y tablets que usen sistemas operativos móviles.

### Oxygen Forensic Suite <sup>(3)</sup>

Oxygen Forensic Suite es la herramienta desarrollada por Oxygen Software. La compañía (radicada en los Estados Unidos) está dedicada a desarrollar soluciones forenses que cubran la mayor cantidad de dispositivos que corran bajo Android, iOS, Blackberry, Windows Phone y Symbian, entre otros. A diferencia de las dos herramientas que presentamos anteriormente, Oxygen es meramente una solución de software, no incluye en ninguna de sus versiones complementos de hardware.

La herramienta está disponible en 3 versiones:

- Oxygen Forensic Suite 2014 Analyst: versión licenciada, que incluye las funcionalidades de unificar contactos, rooting del SO Android, listar aplicaciones instaladas, estadísticas, generación de línea de tiempo con el comportamiento del usuario, entre otros.
- Oxygen Forensic Passware Analyst: versión licenciada que complementa al Analyst y permite la recuperación de contraseñas.
- Oxygen Forensic Suite 2014 Standard: esta versión se puede descargar gratuitamente del sitio del proveedor, previo registro y aprobación de la solicitud de descarga. Las funcionalidades que ofrece son bastante pobres y

limitadas en comparación a las ofrecidas por las versiones licenciadas. Es apenas una demo que permite obtener una primera aproximación al comportamiento de las versiones licenciadas.

Análisis comparativo

Se presenta a continuación un análisis comparativo de las herramientas descritas. Para elaborar el cuadro se tomó como base el análisis presentado por el NIST en su “Guidelines on Mobile Device Forensics”. Por otra parte, se incluyeron aportes desde la documentación oficial de las tools. Se procuró incluir la mayor cantidad de categorías descriptivas sobre las cuales se contara con información.

	UFED Touch Ultimate	XRY Complete	Oxygen Forensic Suite Analyst 2014
SO donde corre la aplicación	Windows	Windows	Windows
Gama de dispositivos soportados (SO/fabricante)	Amplia	Amplia	Amplia
Soporta adquisición lógica del UICC	Si	Si	No
Soporta la clonación de la tarjeta SIM	Si	Si	No
Nivel de adquisición	Lógica y Física	Lógica y Física	Lógica
Tipo/s de red/es de telefonía móvil que soporta	GSM, CDMA, iDEN/TDMA	GSM, CDMA, iDEN/TDMA	GSM, CDMA
Permite realizar análisis de los datos adquiridos	Si. Incluye visor hexadecimal y visor de texto.	Si. Incluye visor hexadecimal. Comparador de	Si. Favoritos, incluye visor hexadecimal y

	Permite la recuperación de datos borrados y el parseo de datos físicos.	distintas adquisiciones. Permite la recuperación de datos borrados, de puntos GPS del Google Earth y el parseo de datos físicos.	visor de texto incluido. Permite la recuperación de datos borrados, de la clasificación de archivos, del visor de imágenes y del visor de otros archivos. Permite el parseo de los datos físicos.
Generación de reportes	Si (DOC, XLS, Hoja de cálculo de Open Document, CSV, HTML, PDF, XML)	Si (DOC, XLS, Open Office, XML, Google Earth). Permite exportar a CD/DVD.	Si (CSV, HTML, RTF, PDF, XLS, XML)
Soporta el análisis de imágenes adquiridas con otras herramientas	Si	No	No
Soporta análisis de dispositivos de manufactura china	Si	Si	Si
Incluye hardware para la	Si	Si	No

conectividad con el dispositivo			
Algoritmos de hash	MD5, SHA-2	No especificado en la documentación	MD5, SHA1, SHA2, GOST R34.11-94, CRC, HAVAL.
Documentación sobre el producto y la empresa proveedora	Aceptable	Aceptable	Pobre

Referencias:

- (1) <http://www.cellebrite.com/es>
- (2) <https://www.msab.com/xry>
- (3) <http://www.oxygen-forensic.com>



# **CAPÍTULO 7**

## ***CASO PRÁCTICO***

### Consideraciones previas

En este apartado incluimos a modo ilustrativo un proceso de extracción lógica y de análisis de datos realizado sobre un Samsung S4 mini (GT-i9190) sobre el cual corre un Android 4.2.2 con la herramienta Oxygen Forensic Suite 2014 Estándar. Las herramientas comerciales del tipo de las presentadas en el capítulo anterior son onerosas y destinadas a fuerzas de seguridad, por lo que las demos y versiones de pruebas son muy restringidas en cuanto al acceso. La elección de la herramienta se basó básicamente en la viabilidad de la experiencia, Oxygen Estándar fue la única versión de prueba de un producto licenciado que se pudo conseguir de manera gratuita (previo registro y justificación en el sitio del proveedor), que permitía extraer una imagen desde dispositivos con Android. Se obtuvo también el Physical Analyzer 3.9 de UFED, pero al ser una versión demo solo era posible realizar imágenes de dispositivos con iOS, lo que hizo imposible que utilizáramos la aplicación. La herramienta XRY directamente no habilita ningún tipo de descarga en su sitio oficial.

Se analizó también la viabilidad de emplear herramientas open source (tales como AFLogical), pero las mismas fueron descartadas debido a que se deben emplear técnicas invasivas en el dispositivo para poder utilizarlas, como por ejemplo, instalar agentes. Así mismo, el resultado obtenido mediante Oxygen se vio limitado también debido a que no se contaba con acceso root en el aparato y se decidió no intervenir en la “prueba” instalando apps y haciendo modificaciones permanentes. Se procuró durante toda la experiencia seguir los lineamientos de trabajo observados en la Policía Judicial de la Prov. de Córdoba, lo cuales indican minimizar la manipulación de evidencia y prevalecer el resguardo de la misma.

En este punto vale la aclaración de que se estuvo en tratativas con la DACTI para realizar pruebas en su equipamiento (UFED Touch Ultimate y XRY Complete). Lamentablemente dicho requerimiento no fue autorizado por las autoridades de la Dirección.

A pesar de las restricciones que caracterizaron la experiencia, esta fue satisfactoria y permite ejemplificar de manera práctica varios de los conceptos presentados.

A continuación se detallan cada una de las actividades que se realizaron y los resultados que se obtuvieron. Algunos datos sensibles/privados fueron sombreados, lo que no impide bajo ningún concepto analizar la utilidad de la herramienta.

### *Dispositivo a analizar*

#### Samsung S4mini (GT-i9190)

- Dimensiones: 61,3 x 124,6 x 8,94 mm
- Peso: 107 gramos
- Sistema operativo: Android Jelly Bean 4.2.2
- Procesador: Dual Core 1,7 GHz
- Memoria RAM: 1,5 GB
- Memoria Interna: 8 GB (5 GB accesible al usuario)
- Memoria Expansible: 2 GB microSD
- Ranuras de tarjeta SIM: 1 ranura
- Tipo de la tarjeta SIM: micro SIM
- Pantalla: 4,3" capacitiva multitouch
- Cámara principal: 8 megapíxeles
- Batería: 1900 mAh
- Industria argentina



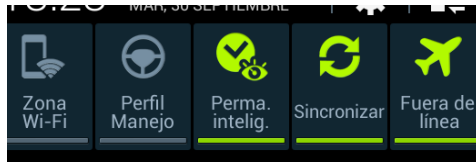
### *Conectividad*

La conectividad entre la estación de trabajo y el dispositivo se realizó mediante un cable de datos USB – micro USB que viene de fábrica con el dispositivo.



### Preparación del dispositivo para la extracción

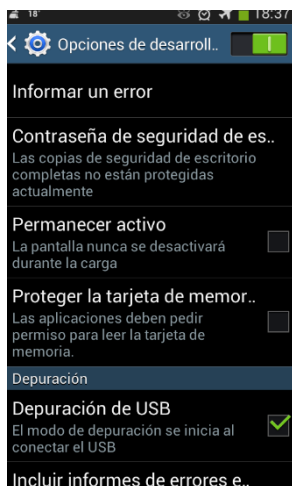
1. Verificar el estado de la batería del equipo, la cual debe estar cargada.
2. Seleccionar la opción Fuera de línea (modo vuelo).



3. Activar el modo desarrollo; ir a Configuración, Más, Acerca del dispositivo, hacer clic 7 veces en Número de Compilación, con el fin de habilitar el modo de desarrollo.



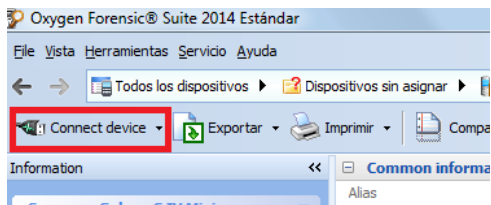
4. Se debe activar la depuración USB: volver al Configuración, ir a Opciones de desarrollador, activar Depuración de USB.



Cabe aclarar que para realizar la experiencia se trabajó sobre un dispositivo sin patrón de bloqueo. En el caso que el dispositivo hubiera estado bloqueado, herramientas adicionales deberían haber sido empleadas, sin garantía de poder acceder al mismo.

## Extracción lógica

- a) Ejecutar la herramienta Oxygen Forensic Suite 2014 Estándar.
- b) Conectar por medio del cable USB - micro USB el dispositivo móvil con la estación de trabajo.
- c) Clickear connect device



A continuación se ejecuta el siguiente asistente:



La aplicación va efectuando una serie de recomendaciones que van guiando el proceso.

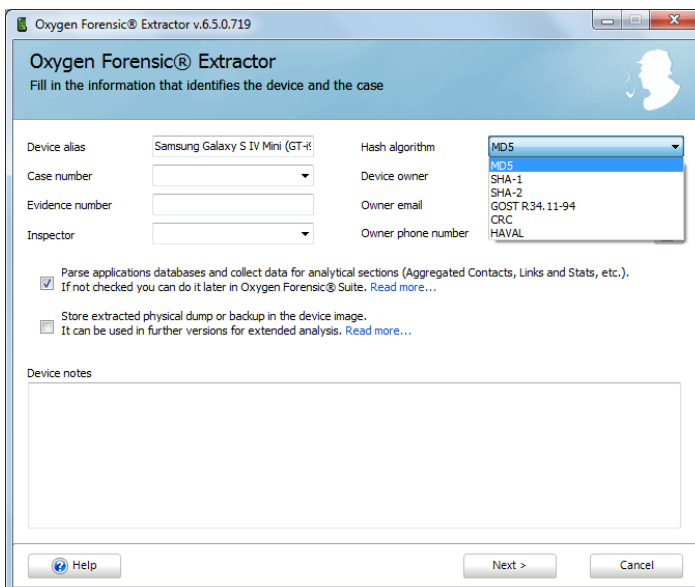


Cuando la aplicación detecta el dispositivo, indica el éxito de la operación mostrando el modelo, IMEI, versión de hardware y de software.



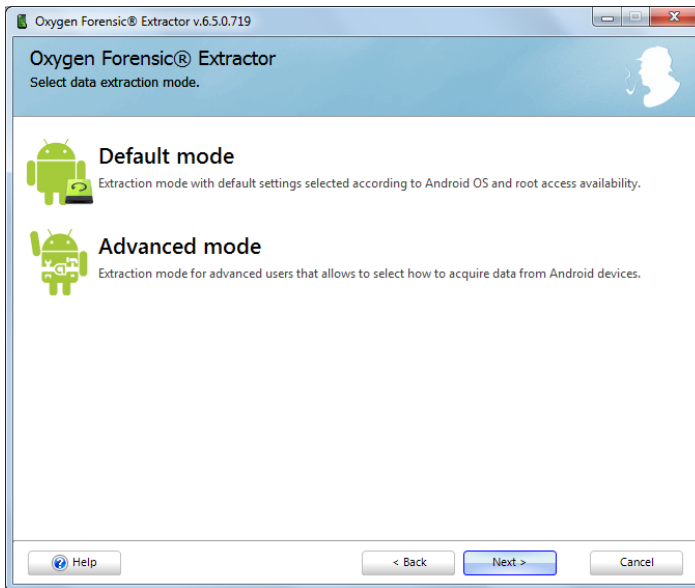
Para comenzar con la extracción de datos es necesario seleccionar *Next*.

Es requerido por la herramienta seleccionar el algoritmo de hash que se desea utilizar para la posterior comprobación de la integridad de los datos.

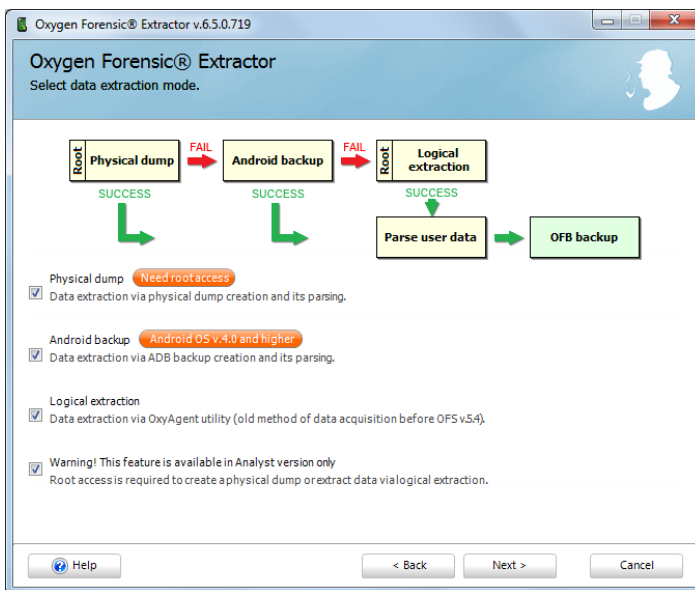


Se seleccionó MD5.

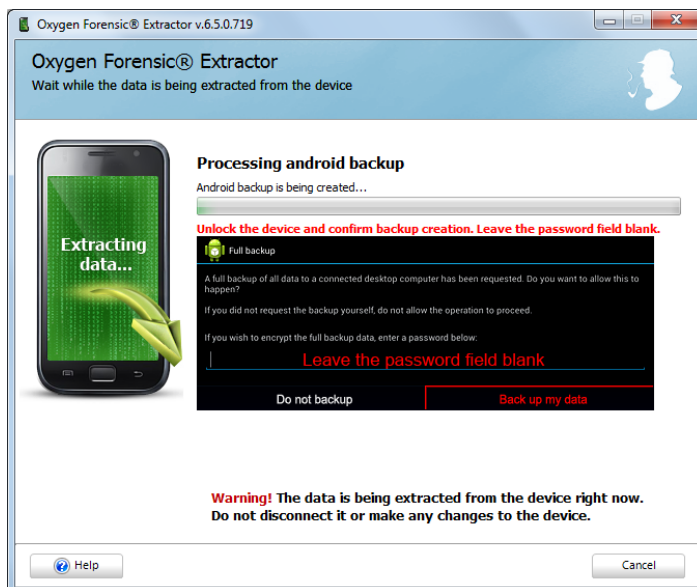
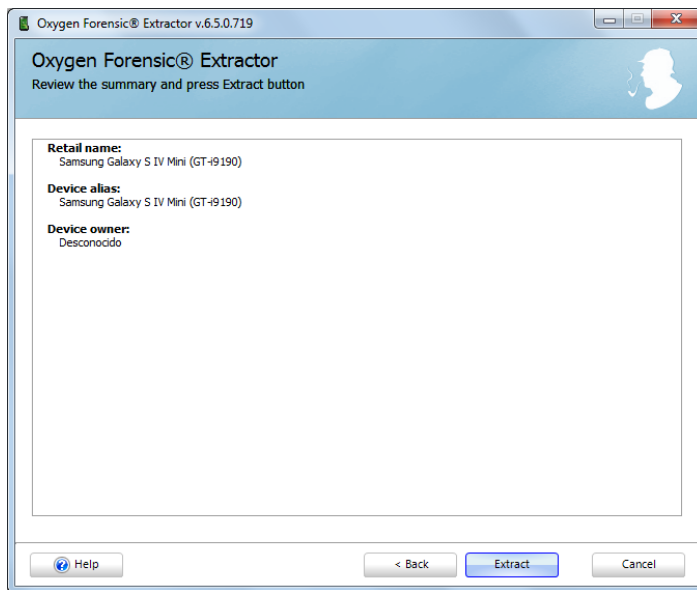
Acto seguido, la herramienta permite escoger entre dos modos de extracción: el modo default y el modo avanzado (que permite al usuario escoger de qué modo se van a adquirir los datos).



Se seleccionó modo avanzado. El aplicativo muestra la siguiente pantalla, donde se seleccionó como alternativas volcado físico (es necesario contar con acceso de root), backup de Android (para v.4.0 y superior) y extracción lógica.

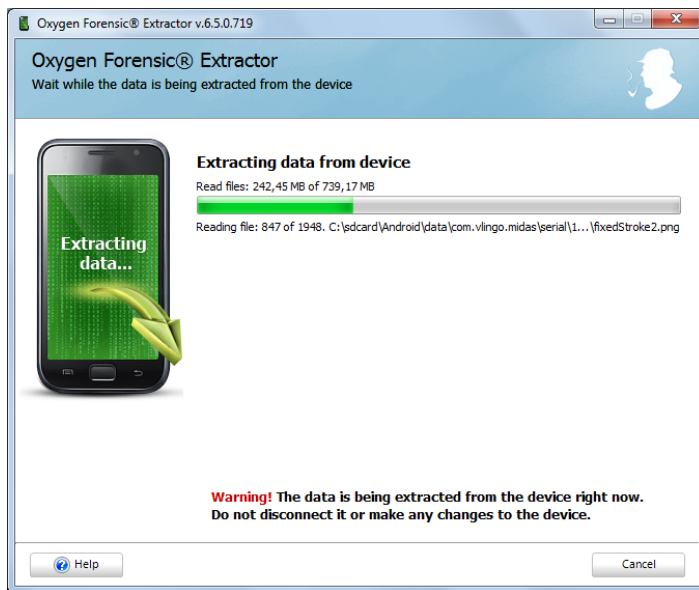


Luego de seleccionar *Next* se visualizó la siguiente pantalla, que permite revisar los datos de la extracción que se va a realizar. Se hizo clic en *Extract* y comenzó el proceso de extracción en sí mismo.



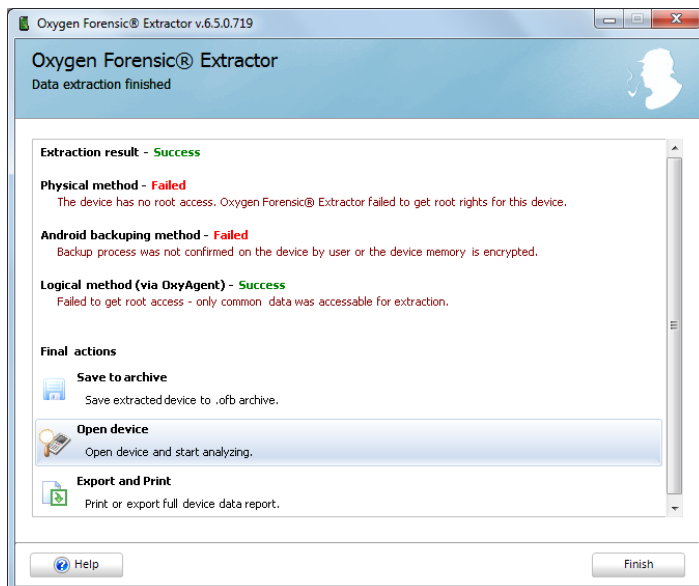
La operación puede llevar varios minutos. La aplicación fue emitiendo distintos mensajes de advertencia sobre la manipulación del dispositivo. Se recomienda no desconectar o efectuar ningún cambio sobre el aparato para no interrumpir el proceso de extracción.



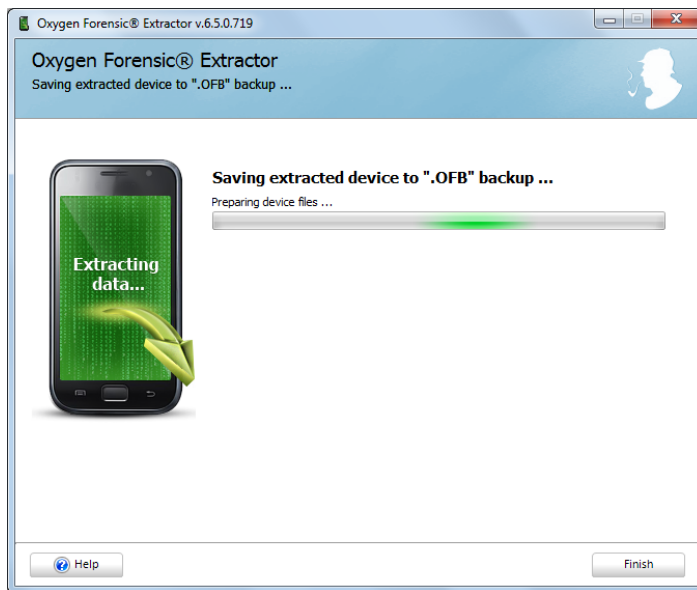


Se visualizó una barra de progreso de la extracción.

Cuando terminó la extracción, se pudo observar el resultado de la misma. La extracción fue exitosa, sin embargo se falló en el volcado físico debido a que no existían permisos de root en el dispositivo, tampoco fue exitoso el backup Android debido a que la memoria del dispositivo estaba encriptada. Finalmente, solo se pudo hacer la extracción mediante el OxyAgent, de la cual solo se obtuvieron datos comunes, ya que no se contaba con acceso de tipo root. Posteriormente, se pudo abrir el resultado de la extracción para realizar el correspondiente análisis.



Los datos extraídos fueron almacenados en un archivo de extensión “.OFB” .

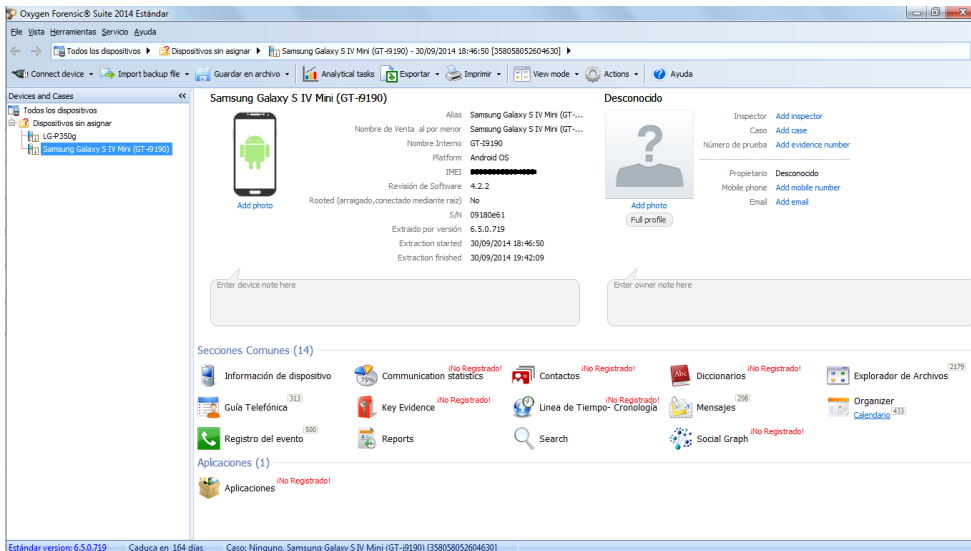


Una vez finalizada esta etapa, la información ya estaba disponible para el correspondiente análisis.

### *Resultados de la extracción lógica*

A continuación presentamos los datos que se pudieron obtener mediante el proceso de extracción lógica descrito en el apartado anterior.

Esta pantalla presenta los datos que pudieron adquirirse. En el apartado *Secciones Comunes* se pueden observar una serie de iconos con la inscripción “¡No Registrado!” que indica que esa información no está disponible en la versión Estándar. Iremos presentando una a una las secciones que cubre la licencia, exhibiendo los resultados obtenidos y en el caso de ser posible, contrastándolos con los resultados de la extracción manual.



## 1. Información del dispositivo

Common information	
Alias	Samsung Galaxy S IV Mini (GT-I9190)
Nombre de Venta al por menor	Samsung Galaxy S IV Mini (GT-I9190)
Fabricante	N/A
Nombre Interno	GT-I9190
Platform	Android OS
IMEI	████████████████████
Revisión de Software	4.2.2
Rooted (arraigado, conectado mediante raíz)	No
IMSI	N/A
S/N	09180e61
Network Information	
Operador	N/A
Red	N/A
Modo de Red	N/A
Estado de Red	N/A
Información de ancho de banda de la Red	N/A
Acceso a la Red	N/A
MCC	722
MNC	310
Identificación del Teléfono Móvil	N/A
LAC	N/A

El IMEI es concordante con el que figura interior del aparato, el resto de los datos indicados son también coincidentes con la información que provee el dispositivo.

## 2. Guía Telefónica

#	Foto	Contacto	Internet	Teléfonos	Grupos llamantes	Origen de Datos	Último contactado	MD5 Hash
1		437013@discussion.openxava.p.r.e.s.f.net	E-mail: 437013@discussion.o...					53e26aa27e8dc43265b966a2b4343075
2		Aa				WhatsApp		fc0f52c5ee6add37472831f660237472
3		AA Institucional	E-mail: institucional@aa.edu.ar					f6e80edb1956d3332ba80391070ffa5
4		acaduc@gmail.com	E-mail: acaduc@gmail.com					19d2bd9e3c2966a54746d6ea3b6c6438
5		agencia.cordobajoven@gmail.com	E-mail: agencia.cordobajove...					cfacfece6602a5f649ad1c70e40e53a5
6		Aguilera Mildred	E-mail: mildredaguilera@hot...					449f8e12bba9d260871c08086ff941c3
7		Agustin Hassanet		Mobile: 3519408316		primary.sim_account_...	Device time: 17/08/2014 ... UTC: 18/08/2014 1:33:02	41d8519660fcd9baf781d0776e2790c5
8		al Cliente Atencion	E-mail: atencioncliente2@...					0b611d2bc19a9aed2a820988909c7747
9		Alemania Willyto	Instant messenger: +4915234176737@...	Mobile: +4915234176737		WhatsApp		dd485e02da368976004874b4bcd947
10		Almada David	E-mail: david.almada@wee...					94a46e345a8b784cd54881dc10ce0256
11		Ana Trabajo		Mobile: +5493516799078		primary.sim_account_...	Device time: 29/07/2014 ... UTC: 29/07/2014 21:37:19	36222ec2bde4c442f6e9dbb673ec320
12		Anita		Mobile: +5493519958279		primary.sim_account_...	Device time: 21/09/2014 ... UTC: 21/09/2014 21:56:21	aad9f43cc257d395395042a346e4131
13		Anita	Instant messenger: 5493519958279@...	Mobile: +5493519958279		WhatsApp		e58bfca4c9f98e3e78343e73bb5e3ce
14		Arcanio Laureano	E-mail: larcanio@gmail.com					5f54601f741fad671454db5d863cd78
15		areainformaticado.unc.edu.ar	E-mail: ...					244011c230c5c1d4240d493c1c611c0d

La aplicación permite visualizar una tabla que presenta la siguiente información:

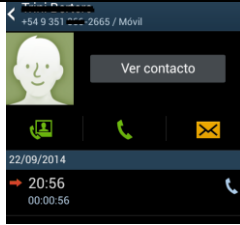
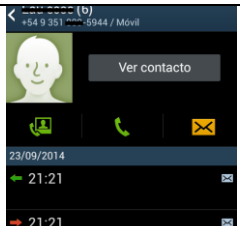
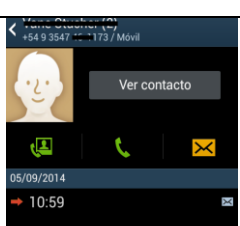

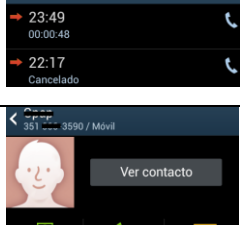
- Foto: en el caso de que el contacto esté asociado a alguna imagen, es posible visualizar la misma.
- Contacto: alias con el que el contacto fue agendado en el dispositivo.
- Internet: en el caso de que el contacto posea dirección de correo electrónico, es factible visualizarla.
- Teléfonos: en el caso de que el contacto posea número telefónico, es posible visualizar el mismo.
- Grupos llamantes
- Origen de datos: primary.sim.account\_name (para los contactos del SIM), [xxx@gmail.com](#) (para los contactos de la cuenta de Gmail primaria del dispositivo), [yyy@gmail.com](#) (para los contactos de la cuenta de Gmail secundaria del dispositivo), WhatsApp (para los contactos que poseen dicha aplicación), vacío (para los contactos almacenados en el teléfono).
- Ultimo contactado: en el caso de estar disponible, brinda la fecha y hora en formato del dispositivo y UTC, del último contacto efectuado.
- MD5 Hash

Datos obtenidos con Oxygen agrupados según su origen versus datos obtenidos mediante extracción manual.

Origen	Total Oxygen	Total Manual	Porcentaje recuperado
SIM	61	61	100%
<a href="#">xxx@gmail.com</a>	198	198	100%
<a href="#">yyy@gmail.com</a>	6	6	100%
WhatsApp	42	42	100%
Teléfono	6	6	100%
Todos	313	313	100%

La aplicación fue capaz de recuperar el 100% de los contactos que figuran en la guía telefónica del dispositivo. Sin embargo, debido a que se realizó una extracción de tipo lógica, no fue posible recuperar datos borrados por el usuario.

A continuación tomamos a modo ilustrativo 5 contactos y contrastamos la fecha y hora de último contacto provista por Oxygen versus la información disponible en el dispositivo. Los contactos fueron seleccionados al azar.

Número telefónico	Último contacto Oxygen	Último contacto Dispositivo
351xxx2665	Device time: 22/09/2014 20:57:19 UTC: 22/09/2014 23:57:19	
+549351xxx5944	Device time: 23/09/2014 21:21:06 UTC: 24/09/2014 0:21:06	
+5493547xxx173	Device time: 05/09/2014 10:59:56 UTC: 05/09/2014 13:59:56	
351xxx3591	Device time: 29/09/2014 23:50:41 UTC: 30/09/2014 2:50:41	
351xxx3590	Device time: 28/09/2014 22:31:55 UTC: 29/09/2014 1:31:55	

Podemos observar que solo se encontraron discrepancias a nivel de minutos ( $\pm 2$  min) entre los datos obtenidos mediante Oxygen y los datos extraídos directamente dispositivo.

### 3. Registro del Evento

Event information	Full Event Log	Answered calls	Missed calls	Dialed calls	Remote party	Contact name	Call duration	MD5 Hash
<b>Event information</b> <b>Maria Teresa</b> Type: Voz Direction: (Llamada saliente) Duration: 00:00:48 Time stamp: Device time: 29/09/2014 20:49:01 UTC: 29/09/2014 23:49:01 MD5 Hash: df2ee6730a0a0e6d1f28d553dac52cd4						Maria Teresa	00:00:48	df2ee6730a0a0e6d1f28d553dac52cd4
<b>Relevant Contact</b> <b>Maria Teresa</b> No photo Phones: Mobile: [redacted] Internet: Instant messenger: [redacted]@s.whatsapp.net						Maria Teresa		08e99e518ef6c0fce49259e176681c2d
<b>Evidence note</b> Enter a note for the evidence						Colorada		67bd543d69:0abfe2d8f8ff5c6e1d105
						Casa	00:00:49	2f3a10fe260aad2b3c9a5c32ce38652087
						Maria Teresa		3cd8d5112c874a245435ac19d79cd306
						Max	00:02:03	b352d69d14365ffbd8d87d1bf735f0e4
						Max		b389c00ea7:3a1ca43c32ce38657881
						Max		32a0fb4c3833326e21a244e54497dc
						Maria Teresa	00:00:16	1ab0219b3c0f23f6b734a506ba6d67e
						Grap	00:01:00	ad3c3718a58bc40925a27c5b58d8b339
						Grap		efcab559e029ddeb20fdae436679f90
						Grap		a6cf07e66d3f94e29305c46a45382c5
						Grap	00:01:34	66070658f79271fa1fd2ec2867d1a92a
						Grap		01c588ca198327101db63cce1920cfb3
						Grap		09862587b4b1064455a437ba638011b9

La aplicación permite visualizar una tabla que presenta la siguiente información:

- Dirección: saliente, entrante, perdida
- Tipo: voz
- Time stamp: fecha y hora en formato tanto del dispositivo como UTC.
- Interlocutor remoto: número telefónico del interlocutor.
- Contacto: en caso de que el interlocutor este agendado en el dispositivo.
- Duración de la llamada: en caso de que la misma haya sido concretada.
- MD5 Hash

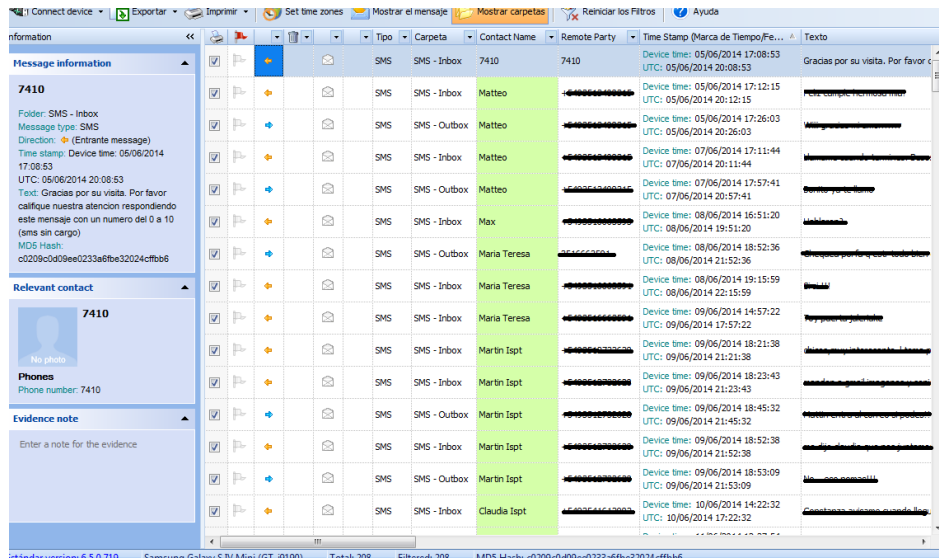
Datos obtenidos con Oxygen agrupados según su dirección versus datos obtenidos mediante extracción manual.

Dirección	Total Oxygen	Total Manual	Porcentaje
Salientes	214	214	100%
Entrantes	200	200	100%
Perdidas	86	86	100%
Total	500	500	100%

La aplicación fue capaz de recuperar el 100% de las llamadas que figuran en el registro del dispositivo. Sin embargo, debido a que se realizó una extracción de tipo lógica, no fue posible recuperar datos borrados por el usuario. Cabe destacar que solamente se pudieron visualizar las llamadas efectuadas a partir del 12/08/2014 (tanto

con Oxygen como desde el dispositivo), siendo que el aparato se comenzó a utilizar el 05/06/2014.

#### 4. Mensajes



En la sección mensajes, es posible visualizar tanto las características del mismo como su contenido. La tabla de mensajes presenta la siguiente información:

- Tipo: SMS, MMS
- Carpeta: bandeja de entrada, bandeja de salida y borradores, tanto para SMS como para MMS.
- Nombre del contacto
- Interlocutor remoto: número telefónico del contacto
- Time stamp: fecha y hora tanto del dispositivo como UTC
- Texto: contenido del mensaje

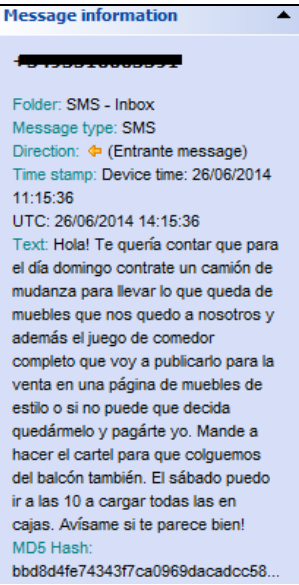
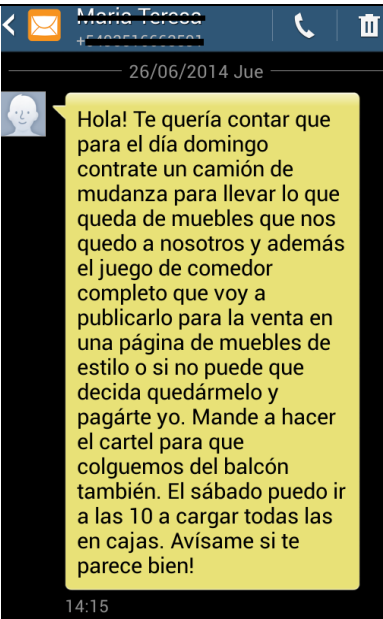
Mensajes recuperados con Oxygen agrupados según su carpeta versus mensaje obtenidos mediante extracción manual.

Carpeta	Total Oxygen	Total Manual	Porcentaje
Bandeja de entrada SMS	113	113	100%

Bandeja de salida SMS	92	92	100%
Borradores SMS	1	1	100%
Bandeja de entrada MMS	2	2	100%
Total	208	208	100%

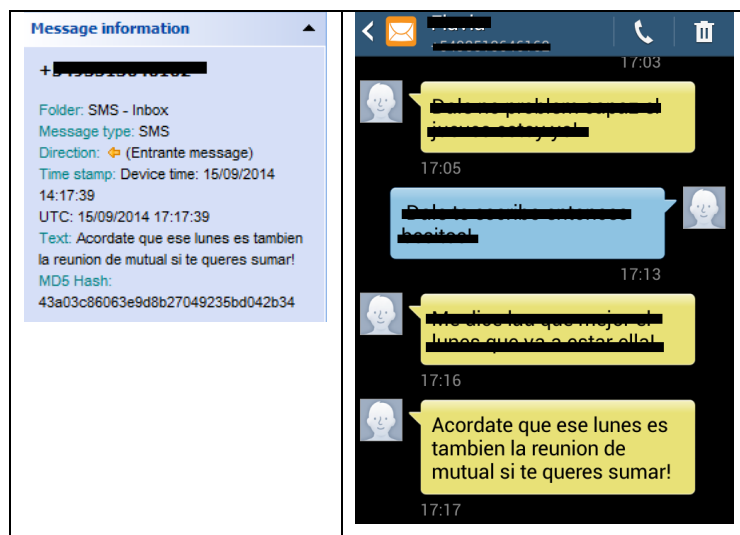
La aplicación fue capaz de recuperar el 100% de los mensajes que figuran en las distintas carpetas del dispositivo. Sin embargo, debido a que se realizó una extracción de tipo lógica, no fue posible recuperar mensajes borrados por el usuario.

A continuación tomamos como muestra 5 mensajes y contrastamos el contenido de los mismos provisto por Oxygen versus la información disponible en el dispositivo. Los mensajes fueron seleccionados al azar.

Mensaje Oxygen	Último contacto Dispositivo
 <p>Message information</p> <p>Folder: SMS - Inbox  Message type: SMS  Direction: (Entrante message)  Time stamp: Device time: 26/06/2014 11:15:36  UTC: 26/06/2014 14:15:36  Text: Hola! Te quería contar que para el día domingo contrate un camión de mudanza para llevar lo que queda de muebles que nos quedo a nosotros y además el juego de comedor completo que voy a publicarlo para la venta en una página de muebles de estilo o si no puede que decida quedármelo y pagárte yo. Mande a hacer el cartel para que colguemos del balcón también. El sábado puedo ir a las 10 a cargar todas las en cajas. Avisame si te parece bien!  MD5 Hash:  bbd8d4fe74343f7ca0969dacadcc58...</p>	 <p>María Teresa</p> <p>26/06/2014 Jue</p> <p>Hola! Te quería contar que para el día domingo contrate un camión de mudanza para llevar lo que queda de muebles que nos quedo a nosotros y además el juego de comedor completo que voy a publicarlo para la venta en una página de muebles de estilo o si no puede que decida quedármelo y pagárte yo. Mande a hacer el cartel para que colguemos del balcón también. El sábado puedo ir a las 10 a cargar todas las en cajas. Avisame si te parece bien!</p> <p>14:15</p>



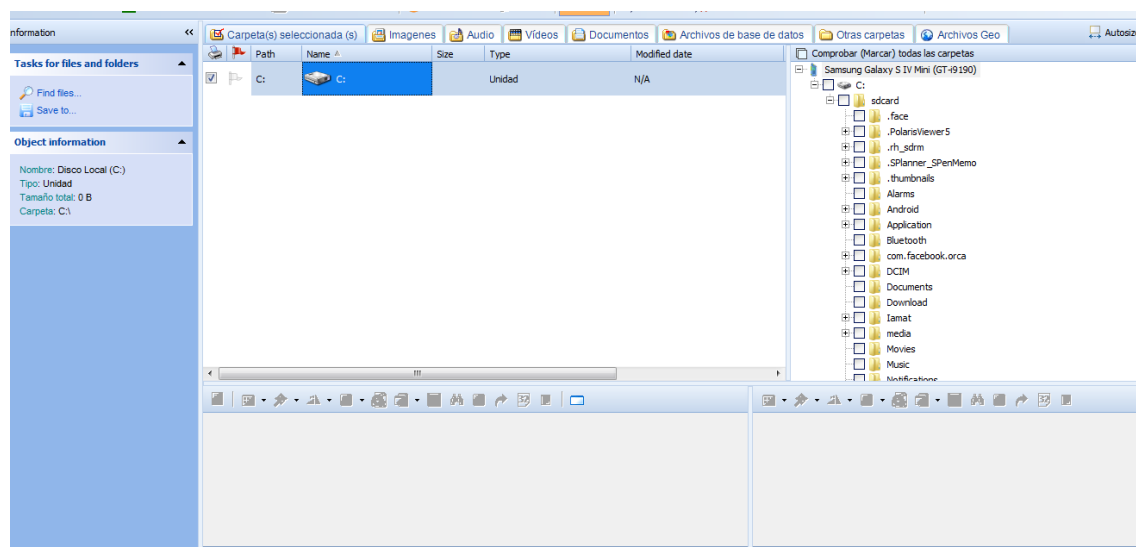
<p><b>Message information</b></p> <p><b>7410</b></p> <p>Folder: SMS - Inbox  Message type: SMS  Direction: (Entrante message)  Time stamp: Device time: 18/07/2014 10:10:12  UTC: 18/07/2014 13:10:12  Text: Claro agradece tu llamado. Por favor califica nuestra atencion respondiendo este mensaje con un numero del 0 al 10 (sms sin cargo).  MD5 Hash:  aa803ae9e4fd3ace7cefca8cf8238bf</p>	<p>05/06/2014 Jue</p> <p>20:08</p> <p>18/07/2014 Vie</p> <p>13:10</p>
<p><b>Message information</b></p> <p>+5499548888555</p> <p>Folder: SMS - Inbox  Message type: SMS  Direction: (Entrante message)  Time stamp: Device time: 24/07/2014 16:27:48  UTC: 24/07/2014 19:27:48  Text: brown entre 27 y cAseros  MD5 Hash:  faa37e31b2f14fd25cbdc9d4dodd0385</p>	<p>24/07/2014 Jue</p> <p>19:24</p> <p>19:27</p>
<p><b>Message information</b></p> <p>+549954888555</p> <p>Folder: SMS - Inbox  Message type: SMS  Direction: (Entrante message)  Time stamp: Device time: 05/09/2014 16:04:22  UTC: 05/09/2014 19:04:22  Text: Hola a todos! Mañana desde las 10 a las 18hs en la casa de españa. Entre rios 40 hay un encuentro gratis, de practicas escolares innovadoras. Reenvien al que no esta en la lista. Gracias. Los espero. Abrazos!  MD5 Hash:  40fcdab8a18a727dda91985022c99f...</p>	<p>10:07</p> <p>05/09/2014 Vie</p> <p>19:04</p>



Como podemos observar, los mensajes coinciden en contenido y fecha. En particular, el horario de los mensajes provisto por Oxygen en formato UTC coincide con el horario provisto por el dispositivo.

### 5. Explorador de Archivos

Presenta una interfaz de navegación de archivos al estilo Microsoft Windows.



A medida que vamos desplazándonos por las solapas de la sección superior, es posible visualizar características y contenido de los distintos tipos de archivos que fueron recuperados.

Oxygen Forensic Suite 2014 Estándar

File Vista Herramientas Servicio Ayuda

Todos los dispositivos Dispositivos sin asignar Samsung Galaxy S IV Mini (GT-I9190) - 30/09/2014 18:46:50 [358058052604630] Explorador de Archivos Criterios de filtro ...

Connect device Exportar Imprimir Exportar a Google Earth Set time zones Arriba Visor Filtros Reset Filters Vistas Tipo, Clase Ayuda

Information

Carpeta(s) seleccionada (s) Imágenes Audio Vídeos Documentos Archivos de base de datos Otras carpetas Archivos Geo

Tasks for files and folders

Find files... Save to...

Object information

Nombre: +54 9 351 666-3594  
 20140611\_011151.jpg  
 Tipo: Imagen JPEG  
 Tamaño: 33,89 KB  
 Modificado: Device time: 10/06/2014 22:11:00  
 UTC: 11/06/2014 1:11:00  
 MD5 Hash: a571c519c8d1e2a090108e1a04c25...  
 Carpeta: C:\sdcard\WhatsApp\Media\WhatsApp Profile Photos  
 Geo posicionamiento: Esta foto no tiene geo posicionamiento información

Exif information

No hay información EXIF

Path	Name	Size	Type	Modified date
C:\sdcard\...	+54 9 351 666-359...	33,89 KB	Imagen JPEG	Device time: 10/06/2014 22:11:00 UTC: 11/06/2014 1:11:00
C:\sdcard\...	1200.png	7,50 KB	Imagen PNG	Device time: 19/07/2014 15:16:00 UTC: 19/07/2014 18:16:00
C:\sdcard\...	1200.png	12,97 KB	Imagen PNG	Device time: 16/09/2014 22:21:00 UTC: 17/09/2014 1:21:00
C:\sdcard\...	1200.png	13,09 KB	Imagen PNG	Device time: 07/09/2014 22:48:00 UTC: 08/09/2014 1:48:00
C:\sdcard\...	1402031265307.jpg	14,68 KB	Imagen JPEG	Device time: 05/06/2014 23:07:00 UTC: 06/06/2014 2:07:00
C:\sdcard\...	1402094051046.jpg	14,83 KB	Imagen JPEG	Device time: 06/06/2014 16:34:00 UTC: 06/06/2014 19:34:00
C:\sdcard\...	1402094051120.jpg	8,91 KB	Imagen JPEG	Device time: 06/06/2014 16:34:00 UTC: 06/06/2014 19:34:00
C:\sdcard\...	1402094051219.jpg	8,00 KB	Imagen JPEG	Device time: 06/06/2014 16:34:00 UTC: 06/06/2014 19:34:00

Some filters are applied. Not all files can be shown.  
 Filtering by extension (Imágenes) Help

Mode: Image Zoom: Fit No hay selección

Estándar version: 6.5.0.719 Samsung Galaxy S IV Mini (GT-I9190) Total: 936 objects (-1 B) Seleccionado: +54 9 351 666-3594 20140611\_011151.jpg MD5 Hash: a571c519c8d1e2a090108e1a04c25c9a

Oxygen Forensic Suite 2014 Estándar

File Vista Herramientas Servicio Ayuda

Todos los dispositivos Dispositivos sin asignar Samsung Galaxy S IV Mini (GT-I9190) - 30/09/2014 18:46:50 [358058052604630] Explorador de Archivos Criterios de filtro ...

Connect device Exportar Imprimir Exportar a Google Earth Set time zones Arriba Visor Filtros Reset Filters Vistas Tipo, Clase Ayuda

Information

Carpeta(s) seleccionada (s) Imágenes Audio Vídeos Documentos Archivos de base de datos Otras carpetas Archivos Geo

Tasks for files and folders

Find files... Save to...

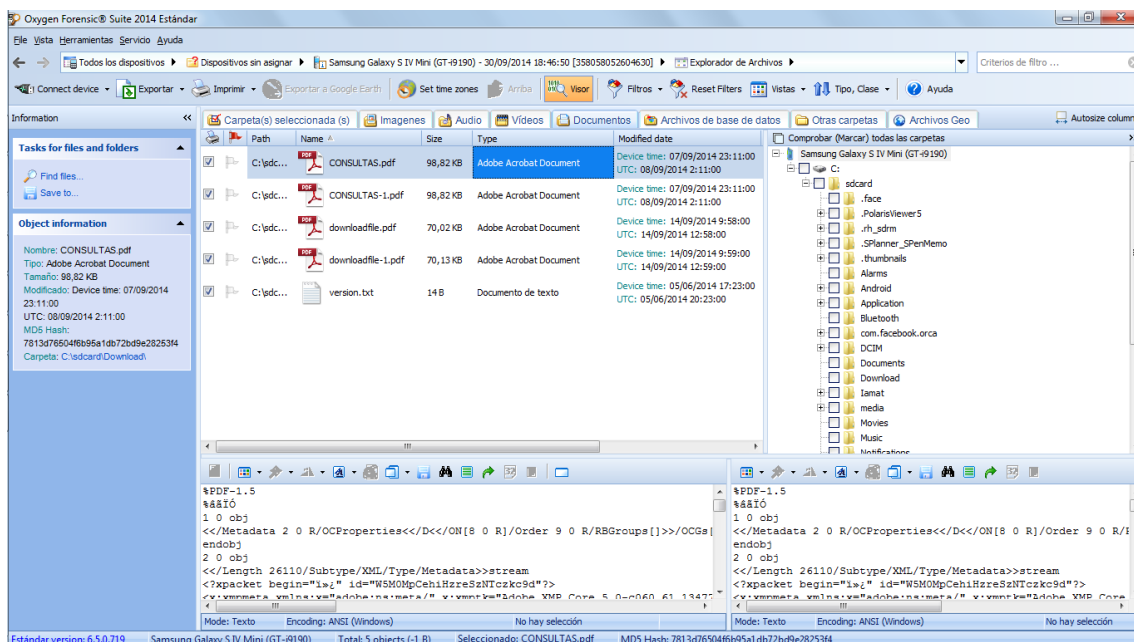
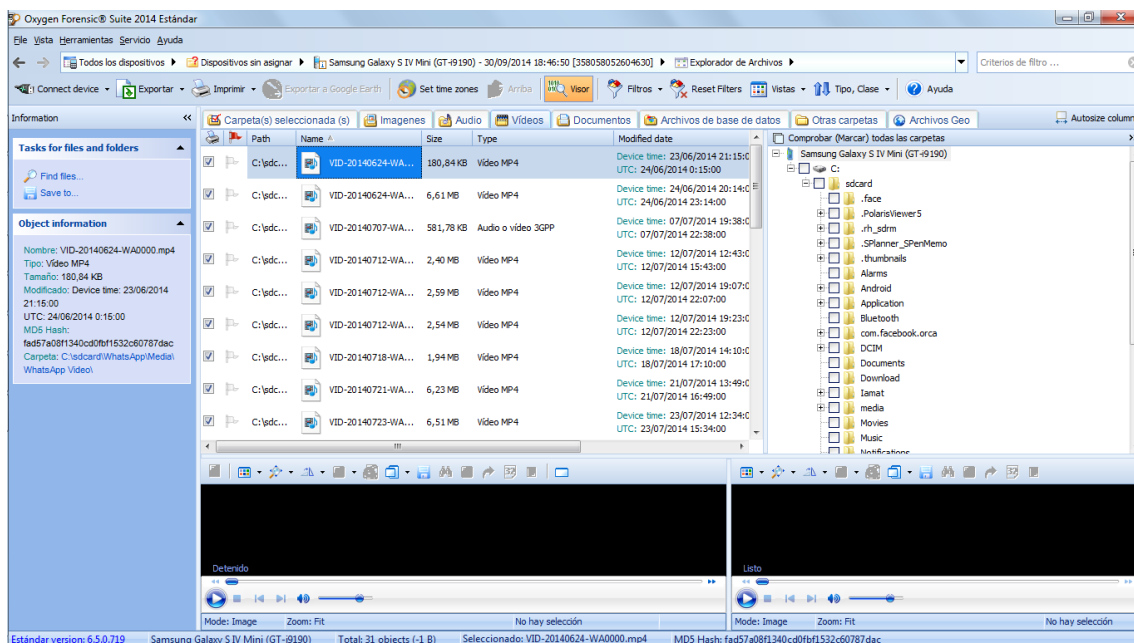
Object information

Nombre: 188bb3c948c50114db125713034b...  
 Tipo: Audio ADTS  
 Tamaño: 0 B  
 Modificado: Device time: 16/09/2014 22:40:00  
 UTC: 17/09/2014 1:40:00  
 MD5 Hash: 188bb3c948c50114db125713034b...  
 Carpeta: C:\sdcard\WhatsApp\Media\WhatsApp Voice Notes\201438

Path	Name	Size	Type	Modified date
C:\sdcard\...	00d1052b36703b...	0 B	Audio ADTS	Device time: 20/07/2014 10:15:00 UTC: 20/07/2014 13:15:00
C:\sdcard\...	049fba3d87aa2e...	0 B	Audio ADTS	Device time: 26/09/2014 23:37:00 UTC: 27/09/2014 2:37:00
C:\sdcard\...	051736061697767...	0 B	Audio ADTS	Device time: 26/08/2014 21:10:00 UTC: 26/08/2014 21:10:00
C:\sdcard\...	09202660708428...	0 B	Audio ADTS	Device time: 29/07/2014 13:11:00 UTC: 29/07/2014 16:11:00
C:\sdcard\...	0934e085ee3a16e...	0 B	Audio ADTS	Device time: 26/08/2014 18:31:00 UTC: 26/08/2014 21:31:00
C:\sdcard\...	0cb2e2bfac958e5f...	0 B	Audio ADTS	Device time: 22/07/2014 16:54:00 UTC: 22/07/2014 19:54:00
C:\sdcard\...	15885709a9f3033a...	0 B	Audio ADTS	Device time: 28/08/2014 8:42:00 UTC: 28/08/2014 11:42:00
C:\sdcard\...	188bb3c948c5011...	0 B	Audio ADTS	Device time: 16/09/2014 22:40:00 UTC: 17/09/2014 1:40:00
C:\sdcard\...	19868884fd0a49f3...	0 B	Audio ADTS	Device time: 20/09/2014 16:43:00 UTC: 20/09/2014 19:43:00

Mode: Image Zoom: Fit No hay selección

Estándar version: 6.5.0.719 Samsung Galaxy S IV Mini (GT-I9190) Total: 117 objects (-1 B) Seleccionado: 188bb3c948c50114db125713034b55a.1.aac MD5 Hash:



Presentamos el conteo de los objetos recuperados

Tipo	Objetos recuperados
Imágenes	936
Audio	117
Video	31
Documentos	5
Archivos de base de datos	1
Otras carpetas	858

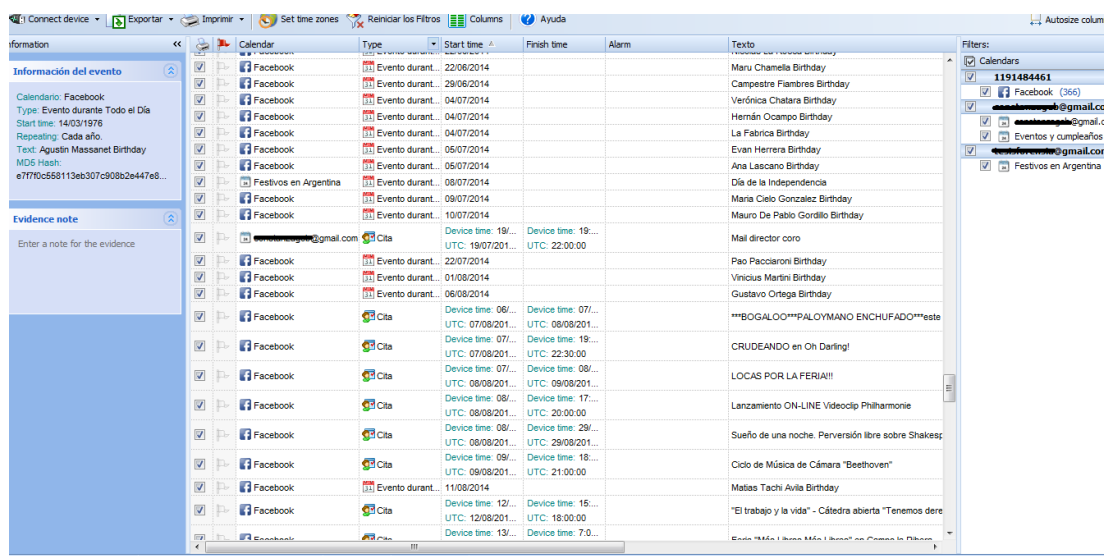
Archivos de geolocalización	0
Total	1948

Debido al gran volumen de información almacenado en la tarjeta de memoria, vamos a analizar cinco carpetas seleccionadas al azar, en particular vamos a contrastar el contenido de las mismas provisto por Oxygen versus la información disponible en el dispositivo.

Carpeta	Total Oxygen	Total Manual	Porcentaje Recuperado
sdcards/WhatsApp/Media/WhatsApp Images/Sent	84	84	100%
sdcards/Download	5	5	100%
sdcards/media/audio/notifications	1	1	100%
sdcards/WhatsApp/Databases	9	9	100%
sdcards/Sounds	11	11	100%

Como podemos ver, en los casos considerados, coincide la cantidad de objetos recuperados por Oxygen con los existentes en el dispositivo. Adicionalmente, se compararon los contenidos y el resultado fue satisfactorio.

## 6. Organizer



La tabla de eventos del calendario permite visualizar:

- Calendar: el nombre del origen del evento, como por ejemplo, Facebook, festivos en Argentina, Gmail, etc.
- Tipo: cita o evento durante todo el día.
- Hora de comienzo
- Hora de finalización
- Alarma
- Contenido
- Nota
- Ubicación
- Recurrencia: por ejemplo, cada año.
- MD5 Hash

Presentamos los resultados obtenidos en cuanto a objetos recuperados por Oxygen versus los objetos recuperados de forma manual.

Origen	Objetos Oxygen	Objetos Manual	Porcentaje
Facebook	366	366	100%
Eventos y cumpleaños de contactos de xxx@gmail.com	5	5	100%
Fechas festivas en la Argentina desde yyy@gmail.com	62	62	100%
Total	433	433	100%

### Conclusiones

Consideramos que el resultado de la experiencia fue satisfactorio. Se operó siguiendo los lineamientos que indican las guías de buenas prácticas analizadas en apartados anteriores. Fue posible extraer la información del dispositivo de manera simple, amigable y segura gracias a la herramienta empleada. Se analizaron los resultados provistos por Oxygen mediante el contraste con el resultado de una extracción manual. Las muestras brindaron concordancia entre los objetos en el dispositivo y los recuperados por la herramienta. Como era de esperarse, mediante el

proceso de extracción lógica no fue posible rescatar objetos borrados, lo cual en un escenario judicial sería imprescindible.

Consideramos que Oxygen es una buena herramienta, intuitiva y eficaz, que debe ser complementada con al menos, otra aplicación que permita la extracción física de datos.

# **CAPÍTULO 8**

## ***ESTADO DEL ARTE***



### Introducción

En este capítulo se presenta una recopilación de 3 entrevistas llevadas a cabo entre los meses de agosto y septiembre del 2014 en las oficinas de la Policía Judicial citas en la Ciudad de Córdoba, de las cuales participaron:

- El Sr. Fiscal de Instrucción Dr. Enrique Gavier
- El Ing. Arsenio Antonio Cardone
- El Ing. Gustavo José Guayanes
- El Ing. Luciano Paquali

Todos ellos, miembros del Poder Judicial de la Provincia de Córdoba.

En las mismas, se abordaron distintos aspectos de la temática de la Informática Forense aplicada a smartphones. A continuación presentamos la información, a nuestro criterio, más relevante discutida durante esos encuentros.

### Sobre la DACTI

La Dirección de Análisis Criminal y Tecnología de la Información, es producto de una reestructuración de la Ley Orgánica del Ministerio Público, publicada en el Boletín Oficial el 30 de abril del 2014. Esta Dirección obtiene y analiza los datos fácticos suficientes para poder establecer el comportamiento criminal, fijar el mapa del delito, diseñar políticas de persecución criminal y todo otro dato que procure la optimización de la investigación penal.

El Director de Análisis Criminal y Tecnologías de la Información tiene a su cargo la elaboración de informes, estudios y estadísticas criminales y presta la colaboración que le requieran los Fiscales de Instrucción, otros magistrados o funcionarios judiciales u otras áreas del Poder Judicial o del Ministerio Público, con conocimiento del Director General de Policía Judicial y autorización del Fiscal General.

La Dirección de Análisis Criminal y Tecnologías de la Información cuenta con personal con formación académica en las áreas y especialidades que la conforman y se integra con las áreas que determinen los reglamentos que dicte y la organización que establezca el Fiscal General, quien las podrá modificar o ampliar cuando las necesidades del servicio así lo requieran.

### *Sobre protocolos y guías de buenas prácticas*

Actualmente, en el marco de la Provincia de Córdoba no existe protocolo escrito alguno de manejo de evidencia digital. Los lineamientos de trabajo se basan principalmente en la RFC 3227 y en la ISO/IEC 27037:2012. Esta normativa fue tomada como base con el fin de poder interactuar con otras fuerzas. Se destaca la labor que se está llevando a cabo en el proyecto PURI. Las autoridades de la DACTI realizan análisis comparativos periódicos entre las directivas de trabajo interno y todo protocolo o reglamentación nueva que surja y sea aplicable. Se procura elaborar un compendio de normas ya existentes permeables a incorporar buenas prácticas y metodologías nuevas que vayan surgiendo.

### *Sobre el convenio de Budapest*

Las autoridades consideran que aún hay mucho trabajo para realizar, sobre todo en lo que respecta a la extra territorialidad de los delitos, y en especial respecto a minoridad, ya que según el país, cambia la reglamentación.

Actualmente Argentina está de invitada en el convenio, tiene voz pero no voto.

Las situaciones de cooperación internacional se han dado básicamente en relación a pornografía infantil. Este tipo de causas vienen de Interpol, ellos detectan que hay tráfico a través de sistemas que tienen almacenamiento en la nube, por ejemplo Gmail, Hotmail, etc.; donde mandan imágenes pornográficas, que luego son detectadas en el tráfico de un correo electrónico a otro. En la mayoría de los países está penado la distribución, no la tenencia de este tipo de material. Cuando ellos detectan que se está distribuyendo, se inicia una causa que desde Interpol viene a la Justicia Federal y de allí, al Poder Judicial de Córdoba. Generalmente la causa ya viene resuelta en el sentido de que ya saben lo que hay que buscar, que imágenes se transfirieron y que direcciones IP participaron, cual es el domicilio físico de estas IPs, etc. entonces lo que hace Policía Judicial es ir concretamente a buscar esas imágenes a esa dirección y hacer un allanamiento.

### *El escenario a nivel nacional*

En cuanto a la situación interprovincial, se debe rescatar que existen grandes similitudes en referencia a los lineamientos de trabajo, sin embargo, cada provincia adapta estos a su realidad y necesidad. Sería óptimo que existiera alguna normativa que unifique criterios y estandarice los procedimientos. Córdoba es una provincia fuerte en

materia de análisis forense de tecnologías informáticas, a tal punto que vienen a tomar capacitaciones desde todo el país.

Difieren entre provincias principalmente, los Códigos Procesales Penales.

Con respecto a la Provincia de Bs. As. y Policía Federal existen ciertas discrepancias en referencias a los códigos procedimentales y las acciones resultantes, por ejemplo en esas jurisdicciones, cuando necesitan un dictamen contratan un perito, según la disponibilidad económica y la importancia de la causa es el tipo de perito que se contrata. Por su parte, los técnicos de Córdoba son empleados de planta permanente de la provincia, y están en condiciones de efectuar tanto informes técnicos como dictámenes.

La etapa investigativa requiere una forma de trabajo y cuando se avanza a la etapa judicial, se repite todo el procedimiento nuevamente. Hay jurisdicciones que solo actúan en la etapa del juicio, en cambio en nuestra provincia los peritos también trabajan en la instrucción penal preparatoria, etapa más fuerte del ciclo de vida judicial.

#### *Sobre la cadena de custodia*

En referencia puntual a la cadena de custodia existen protocolos escritos que están siendo revisados. Cabe destacar que solo en el fuero de narcotráfico y a partir del año 2012 se aplica con rigurosidad la cadena de custodia, procurando la no nulidad de la prueba. En este fuero se usan envoltorios convenientes, stickers, en cada etapa un precintado para que se garantice inviolabilidad y fichas de trazabilidad para asegurar que todos los procesos sean reversibles y permitir que los abogados defensores puedan acceder a las pruebas. En los demás fueros, este aspecto no se maneja con tanta rigurosidad. La principal diferencia procedimental entre el fuero de narcotráfico y lo demás fueros, es que en casos de estupefacientes la ficha de traza (que indica fecha, hora, operador que intervino, firma) está constantemente adherida al dispositivo, mientras que en los demás fueros, se deja constancia en actas de la manipulación de la prueba.

#### *Sobre el análisis forense de telefonía móvil*

Existen dos áreas de trabajo bien diferenciadas: equipos de computación y dispositivos móviles, ambas utilizan distintas oficinas y distintos elementos. Hasta el plan de inversión de cada área es distinto. En el caso de dispositivos móviles la inversión ha sido significativa, cada elemento de hardware o software es muy oneroso,

mucho más que para la parte informática. Por cada valija de se calcula un costo aproximado de \$40.000 dólares norteamericanos. Este tipo de equipamiento solo se vende a fuerzas legales. La versión comercial (forPC) no me permite acceder a la misma información que la valija para fuerzas de seguridad, por ej. La versión forPC no permite hacer extracción física, que permite buscar elementos borrados.

En el caso de dispositivos móviles los sistemas operativos no están demasiado estandarizados, no siempre se cuenta con herramientas que soporten al mismo. Por esto, se dan situaciones que no dejan otra alternativa que usar técnicas de trabajo de cuidado y proceder a la extracción manual. Siempre se procura que el dispositivo no sea interactuado por redes externas, por este motivo, es que se los aísla. Sucede en ocasiones que aun habiendo aplicado software y hardware forense el resultado no es satisfactorio, en cuyo caso hay que indefectiblemente hacer relevamientos manuales para extraer archivos multimedia.

En algunos casos, se ha tenido que proceder a efectuar la imagen con alguna herramienta open source. Sin embargo y en general, lo que no se puede extraer por medio de métodos forenses, tiene puramente valor indiciario, ya no unívoco. En nuestro sistema no existe lo que se llama prueba legal, sino que se rige por el concepto de libertad probatoria, que implica que cualquier hecho se puede probar de cualquier manera en la medida que sea lícito y que no sea en violación a las garantías constitucionales. Después, las pruebas serán valoradas según la sana crítica. En el caso de contar con una sola prueba y esa prueba es de procedencia dudosa, no es suficiente. Si hay varias pruebas, en cambio, se converge a una única conclusión.

En materia de elección de herramientas, se intenta analizar la relación costo/beneficio de usar una u otra, es importante a su vez, pautar una metodología de trabajo por una cuestión de tiempos. Generalmente la evidencia cuando aparece, aparece. Es raro encontrar a último momento del análisis alguna prueba relevante. A veces se confrontan los resultados entre herramientas y metodologías para verificar que el negativo sea negativo y a su vez, que no estemos en presencia de falso positivos. En el caso de los dispositivos móviles generalmente lo que no se pudo encontrar con una herramienta licenciada, raramente encuentre con otra más económica o libre. Por la particularidad de estos dispositivos, existen complicaciones entre los fabricantes de herramientas y los fabricantes de dispositivos: los dispositivos se han hecho para hablar por teléfono, no para ser analizados con técnicas forenses. Hay alta heterogeneidad de sistemas operativos en dispositivos móviles, baja normalización. No se le puede exigir

al fabricante del aparato que guarde información por las dudas, por que potencialmente se pueda usar en una causa.

#### *Sobre el registro fotográfico*

No se toma registro fotográfico alguno sobre dispositivos móviles. Si se toma registro manual cuando se nota alguna anomalía en el aparato (ej. Pantalla rota). Muchas veces, los imputados intentan destruir el aparato, pisándolo por ej., sin embargo todavía es posible obtener la información. La fotografía solo se usa para mostrar una situación en particular o para realizar un análisis comparativo (fotografía como elemento documental). En la mayoría de los casos, se apela a la descripción minuciosa, a tal punto que si ponemos en comparación dos teléfonos iguales es posible identificarlos unívocamente. También se identifican por IMEI, tanto físico como electrónico.

#### *Cuestiones procedimentales*

1. Para ingresar a un domicilio es necesario contar con una orden de allanamiento, que es solicitada por una fiscalía y emitida por un juzgado de control, quien autoriza a violar las garantías constitucionales de la privacidad de domicilio.
2. Con respecto a los celulares no se hace un análisis en el lugar del allanamiento, sino que se lo secuestra y se lo lleva a los depósitos de la Policía Judicial.
3. Una vez que se determinó que se va a secuestrar el celular, como primera medida se procede a apagarlo, embalarlo y precintarlo con un precinto de color blanco, que tiene una numeración y doble oreja, donde una de las orejas se corta y se registra en el acta de allanamiento. Al realizar este procedimiento se labra una acta donde se indica quien interviene en el allanamiento, las personas que lo llevan a cabo y que otras organizaciones u oficiales de justicia hay en el momento del allanamiento. Generalmente quienes llevan a cabo los allanamientos son integrantes de la Policía de Córdoba y de la Policía Judicial, como asesores para la parte técnica. En ocasiones suelen concurrir otras secciones de Policía judicial, como por ejemplo química, huellas y rastros, etc.; dependiendo de la naturaleza del

hecho. Todo esto queda mencionado en la orden, como así también porque se secuestra el dispositivo.

4. En ocasiones existe un pedido puntual de secuestro del celular y a veces no, todo depende de la vinculación que el dispositivo tenga con la causa. De acuerdo a esto es la medida que se toma de secuestrarlo o no. Cuando existe la duda de hacerlo o no, se consulta a quien lleva adelante la causa que generalmente es la fiscalía de instrucción.
5. Cuando se secuestra el dispositivo móvil se lo aísla. Se lo apaga y se lo coloca en una bolsa, no en una bolsa de Faraday por cuestiones presupuestarias. Para preservar la cadena de custodia se utiliza la bolsa, el precinto, y en causas comunes, no interviene la ficha de traza, la cual solo se aplica en narcotráfico.
6. Una vez secuestrado, no se procede al sellado de los conectores del celular, porque la bolsa en la que está contenido no se abre nunca y controla que ningún precinto este violado.
7. La acción del secuestro es llevada a cabo por el área administrativa de Policía de Córdoba. La labor de Policía Judicial es brindar los lineamientos técnicos generales a los policías administrativos, como por ejemplo, que se retire la batería del celular. Se hace constar en acta el estado del dispositivo, si tiene la pantalla rota, si esta rayado, etc. La prueba es trasladada al depósito de la fiscalía y después se lo envían a policía judicial para hacer el análisis. El dispositivo viene con un oficio en el cual está descripto la información que se solicita.
8. La urgencia de los casos va marcando el ritmo de la investigación. Si llega una causa mucho más urgente, se deja la actual y se atiende a la urgente. En general se consideran como urgentes casos donde por ejemplo, existan personas detenidas.
9. Junto con el dispositivo, al laboratorio llega un oficio donde el fiscal indica que necesita, otras veces se solicita toda la información disponible en el equipo. En general se extrae todo, y se le transfiere al fiscal solo lo que él solicitó. Entonces, para agilizar el trabajo, se extrae todos los datos posibles, contemplando que quizás en etapas posteriores necesiten otra información además de la indicada en el oficio.

10. Una vez en el laboratorio, se extrae el teléfono de la bolsa donde está guardado. A veces se tiene conocimiento acerca del modelo puntual, otras veces no. En caso de no tenerlo, dentro del teléfono existe una etiqueta que indica cual es el modelo. No se emplean guantes.
11. Ya en posesión técnico, lo primero que se hace es retirar la tarjeta SIM y colocar el dispositivo en Modo Avión.
12. La herramienta utilizada para llevar a cabo los análisis es el UFED Touch Ultimate.
13. En primer lugar, se efectúa la imagen de la SIM. El UFED solo lee chips comunes, se necesita adaptador para mini y micro SIM. La herramienta extrae registro de últimas llamadas, mensajes y contactos almacenados en el chip.
14. Posteriormente se procede a hacer la imagen de la memoria del dispositivo, siempre procurando que el equipo no tome señal con la red de telecomunicaciones.
15. Cuando el equipo está bloqueado mediante un patrón o una contraseña y ninguna herramienta logra desbloquearlo, sucede que no se puede hacer ninguna extracción ni física, ni lógica. En casos así, se realiza una extracción manual, donde se debe corromper el PIN, lo que produce modificación de la prueba. En estas situaciones, lo importante es que si se modifican los datos, esto quede debidamente asentado por escrito. Para el caso de Android hay herramientas ADB del SDK para desarrolladores que permiten conectar el dispositivo a través de un Shell, a la computadora y realizar operaciones sobre el mismo. Existen otras herramientas para monitorear todo lo que se va haciendo en paralelo, de esta manera se puede tener registro de las operaciones que se van efectuando en tiempo real. Para iPhone existe la aplicación Jailbreak que funciona de manera análoga al root de Android, permitiendo obtener la cadena de privilegios para saltar un patrón o un PIN.
16. Si el celular está dañado, como última instancia se podría usar la técnica chip off (que en Córdoba no se aplica). Si el teléfono está quemado, directamente ya no se puede actuar.

17. No existe una diferencia de tratamiento de la evidencia según sistema operativo, se opera en forma semejante en dispositivos con Android, iOS, Symbian, Windows Phone o BlackBerry OS.
18. Para asegurar la integridad de la evidencia se emplea el algoritmo de hash MD5, debido al tamaño de las imágenes, ya que si se empleara otro algoritmo, como SHA-2, el tiempo del cálculo del hash sería mucho mayor. La evidencia se preserva en dos ejemplares idénticos al hasheado, se trabaja con un solo ejemplar de la imagen, siempre con la réplica del elemento original.
19. El archivo que contiene la imagen se abre con la herramienta Logical Analyzer de UFED. En ocasiones también se emplea el Physical Analyzer del mismo proveedor, que permite hacer Data Carving. No es lo mismo pedir una sábana a un proveedor de telefonía móvil que analizar el aparato, porque el proveedor solo brinda las llamadas que se concretaron, no los intentos. Suele suceder que los delincuentes usan códigos para comunicarse, como por ejemplo, hacerlo sonar 3 veces.
20. La mayoría de la carga de trabajo del personal se aboca a la parte administrativa y no a la técnica. El informe va explicando que y como se obtuvo punto por punto y en lenguaje coloquial. En el dictamen se amplía más aún el grado de detalle. Se estipula en qué momento se hizo la extracción, que técnico fue responsable, la versión del software del equipo, información descriptiva del dispositivo (IMEI etc.), el hash de la extracción, que es UFED, etc. El informe debe ser lo más explícito posible.
21. En referencia a la restitución de los dispositivos, la DACTI una vez que realiza los análisis correspondientes, lo devuelve a la fiscalía que interviene sin ninguna clase de tratamiento. Es la fiscalía quien dispone entregárselo o no al propietario del aparato. Actualmente no existen mecanismos de sanitizado. Se está trabajando en la elaboración de un protocolo de desnaturalización, para reutilización, destrucción o reciclaje. Actualmente la situación de los depósitos es crítica.

¿Quién audita los procedimientos?

Existen tres instancias:



Instancia Penal preparatoria: todavía se desconoce la identidad del supuesto autor, por lo que no hay nadie controlando o auditando los procedimientos, allí solo se recolecta evidencia para llegar a la autoría.

Cuando existe una persona indicada pero no está demostrado que sea el autor, existe la posibilidad que esta parte solicite el control/presencia en el proceso de la pericia.

Ya en los primeros dictámenes, donde se le da el derecho de primera defensa, ahí sí el presunto autor puede proponer un perito de parte.

Como en la DACTI se siguen unos lineamientos bastantes estándares, no hay una manipulación del equipo que exceda lo pertinente al caso. Raramente se ha llegado a la impugnación de la prueba por errores en el manejo técnico de la misma. En cuanto a técnicas y metodologías, se mantiene una cadena de retroalimentación en función de parámetros que se consideran que no han sido actualizados de manera reciente. Se van haciendo adecuaciones y mejoras sobre todo al entorno y a la tecnología.

#### *Sobre la selección de herramientas*

El UFED es el instrumento protagonista debido a que es capaz de realizar adquisiciones físicas, lógicas y de sistema de archivos. En julio de 2014 se ha incorporado una nueva herramienta denominada XRY, lo óptimo sería contar con al menos tres herramientas para poder efectuar un análisis comparativo de los resultados.

A nivel nacional, por ejemplo la Policía Federal está usando UFED y NEUTRINO. La desventaja que tiene UFED es que si no se paga el canon anual el proveedor no entrega actualizaciones y luego empieza a suceder que hay equipos que no están soportados. Hubo un caso en donde se dilató el análisis de la prueba porque no estaba la actualización correspondiente y no se llevó a cabo el procedimiento hasta no tenerla a disposición. En Córdoba el Poder Judicial cuenta con cinco valijas, y el canon es abonado anualmente. De manera adicional, también se adquiere la licencia que soporta chipsets de manufactura china, que cada vez se están haciendo más populares. Se diferencian en que generalmente, tienen otra conectividad, otras fichas. Lo positivo es que todos tienen Android.

Hasta el momento no se han presentado cuestionamientos acerca del UFED. Por lo general los abogados defensores buscan anular la prueba en etapas anteriores al uso de software forense, por ejemplo en actas, en allanamientos, etc.

Quienes redactamos esta tesis tuvimos la posibilidad de observar un análisis forense sobre un dispositivo en particular, un Nokia de la serie Lumia. En el caso analizado el

UFED solo extrajo mensajes de texto (inclusive los borrados por el usuario), las ubicaciones del dispositivo, imágenes, sonido y video. Había mucha información que el mismo UFED no fue capaz de rescatar.

# **CAPÍTULO 9**

## ***DESNATURALIZACIÓN DE LA EVIDENCIA DIGITAL***

### Introducción

En este último capítulo y constituyéndose en instancia previa a la presentación de conclusiones, abordaremos la temática de la desnaturalización de la evidencia digital, como etapa final del ciclo de vida del elemento probatorio. En concreto nos referimos al conjunto de procedimientos aplicables a los diferentes tipos de dispositivos tecnológicos, al momento de ser estos reintegrados a sus propietarios o almacenados en algún depósito fiscal. Actualmente sólo interesa hacer que cese la acción delictiva, por ejemplo en un caso de distribución electrónica de pornografía infantil, pero no se toman medidas tendientes a administrar el material delictivo secuestrado. Siguiendo la línea investigativa del presente trabajo, se hará especial mención a los dispositivos inteligentes con Android.

### Desnaturalización de la evidencia tecnológica <sup>(1)</sup>

La identificación, preservación y trazabilidad de la evidencia (concepto de cadena de custodia), garantizan la intangibilidad de la prueba relacionada a un delito durante el proceso penal para dar base a la acusación o determinar el sobreseimiento de los autores.

La evidencia permanece almacenada en depósitos, acorde a la naturaleza y/o tamaño de los objetos desde el inicio al fin del proceso, independientemente de la resolución. En este punto emerge la primera cuestión a resaltar, estos elementos permanecen olvidados en esos sitios, en estos depósitos, y algunos pocos de ellos son restituidos y/o desnaturalizados (destruidos en el caso de las armas). Tomando como referencia la destrucción periódica de armas de fuego (Art. 10 de la Ley Provincial N° 9.041, Creación del Registro balístico de armas de fuego, cartuchos y proyectiles provenientes de secuestros realizados por la autoridad pública, sancionada el 28/02/2002) y estupefacientes (Art. 30 de la Ley Nacional N° 23.737, Tenencia y tráfico de estupefacientes), presentamos a continuación una propuesta de desnaturalización de material tecnológico vinculado con las TIC's. Esta propuesta fue presentada en el Simposio Argentino de Informática y Derecho del año 2013, por Arsenio Cardone y Gustavo Guayanes, ambos ingenieros miembros del Poder Judicial de Córdoba, en particular de la DACTI.

Para el fin de desnaturalizar evidencia tecnológica los autores contemplan diferentes alternativas, entre las cuales podemos mencionar el reciclado, la reutilización y/o

destrucción, entre otras, considerando que actualmente en Argentina no existe en tal sentido un marco normativo.

En las dependencias que analizan evidencia física y/o lógica relacionada con las TIC's, se observa un incremento gradual año tras año, tanto en la demanda de intervenciones de campo y/o de laboratorio así como en el caudal de ingreso de material por causa judicial. Este hecho es comprobado en las estadísticas de los últimos cinco años, construidas utilizando los registros de los sistemas de información específicos que registran el ingreso y egreso de materiales.

Cada material es identificado, analizado y remitido, por medio de este sistema, a incontables depósitos con asientos en las comisarías de la Policía de la Provincia de Córdoba, depósitos del Poder Judicial de Córdoba en distintos Departamentos o Circunscripciones, un depósito general (según Ley Provincial N° 9.041) en la Primer Circunscripción Judicial - Departamento Capital.

El procedimiento es el siguiente: se extrae el material a ser analizado y una vez que el técnico forense lo procesa, vuelve al mismo depósito u otro que se disponga por parte de la Autoridad Judicial. Esto genera solamente un desplazamiento del volumen ocupado. Además hay que considerar que hay materiales que nunca serán analizados por diversos motivos de la causa a la cual pertenecen y permanecerán en el depósito indefinidamente.

Con el paso del tiempo, al tratarse de equipamiento tecnológico, el mismo se torna obsoleto e inutilizable en la mayoría de los casos, ocupando un espacio físico en los depósitos que se utilizan sin solución.

De tal modo es que surge la propuesta y la necesidad de trabajar en la autorización de la desnaturalización de material tecnológico, tendiente al reciclado de sus partes, su reutilización o destrucción según corresponda teniendo presente procedimientos compatibles con el cuidado del medio ambiente. Para tal fin, es necesario considerar las distintas instancias procesales para otorgar garantías y recaudos legales que correspondan, al tratarse de un acto irrepetible e irreversible.

Se debe tener en cuenta que para instrumentar una medida como la señalada es necesaria la disponibilidad de un sistema de información competente para monitorear el estado final de cada material (evidencia física) y los elementos a considerar para tomar la decisión de desnaturalizar el material hacia su estadio final.

### *Características Generales*

A los fines de establecer límites concretos a esta propuesta de desnaturalización de la evidencia digital, esta se circunscribe a su aplicación en un fuero determinado por la Justicia de la Provincia de Córdoba, específicamente sobre aquellos elementos tecnológicos secuestrados en el marco de causas judiciales ya iniciadas, haciendo especial y principal mención sobre los smartphones.

Estos elementos o dispositivos son los señalados como los más comunes por el momento, sin desconocer la incorporación de nuevos dispositivos tecnológicos producto del crecimiento, avance y asimilación tecnológica.

La chatarra electrónica, los desechos electrónicos, la basura tecnológica, etc. son conceptos globales de la denominada e-waste (basura tecnológica). Este término corresponde a que todos aquellos productos electrónicos mencionados anteriormente, tienen un crecimiento importante por causa de su obsolescencia, el que van adquiriendo con el paso del tiempo, y su tratamiento inadecuado puede producir graves impactos ambientales e inclusive generar daños a la salud.

Estos impactos tanto ambientales como sanitarios son ocasionados principalmente por los deshechos de:

- Mercurio (se lo encuentra en interruptores) que ocasiona daños al cerebro y al sistema nervioso;
- Plomo (presente tubos de rayos catódicos como los monitores, y soldaduras) que produce daños al cerebro y sistema circulatorio;
- Cadmio (se lo encuentra en tableros de circuitos y semiconductores) el que provoca infertilidad;
- Cromo (se lo utiliza en el acero como anticorrosivo) manifiesta problemas en riñones y huesos.

Mientras los smartphones, así como otros elementos tecnológicos, están en funcionamiento, no producen efectos como los mencionados. Cuando caen en desuso, y al mezclarse con la basura se destruyen y esos metales tóxicos se liberan al medio ambiente. Por este motivo se torna primordial favorecer e incentivar la cultura del reciclado de elementos, como el plástico, metales y otros elementos constitutivos.

Para llevar a cabo la desnaturalización de la evidencia física relacionada con las TIC's, se presentan las siguientes consideraciones a tener en cuenta por parte de

aquellas autoridades judiciales responsables en ordenar una medida que contemple la reutilización, reciclado y/o desnaturalización de dicha evidencia:

- Posibilidad de efectuar de manera acabada resguardo y preservación de datos y elementos (evidencia lógica: es aquella evidencia intangible obtenida de la aplicación de técnicas, procesos y herramientas forenses) contenidos en los dispositivos a analizar.
- Posibilidad de poder efectuar de manera parcial resguardo y preservación de datos y elementos (evidencia lógica) contenidos en los dispositivos a analizar.
- Posibilidad de no poder efectuar de manera parcial o total resguardo y preservación de datos y elementos (evidencia lógica) contenidos en los dispositivos a analizar.
- Necesidad de verificar operatividad del dispositivo, situación que determina que el mismo no podrá ser considerado “prescindible”.
- Tratamiento transversal de materiales sin discriminar la figura delictiva.
- Escasas precisiones en cuanto a los elementos relevantes para la causa, pueden determinar que todos los datos contenidos en el dispositivo son importantes, o por el contrario, todos los elementos contenidos en el no revisten interés para la misma.
- Velar por las garantías procesales.
- Resguardar y prever consecuencias o impactos ambientales.

Una decisión relevante que determina si un elemento tecnológico podrá ser desnaturalizado en su último estadio, es establecer si es prescindible o no en el proceso judicial, para lo cual hay que tener en cuenta los aspectos enumerados a continuación.

- 1) Garantizando el resguardo y preservación de los datos:
  - a) Disponer de elementos concretos para establecer el propietario del dispositivo y su posible vinculación a una causa judicial: por un lado, el motivo de establecer el dueño del objeto es a fin de proceder a su restitución, o en caso contrario, definir el destino del material, por otro lado, determinar su vinculación en causas judiciales y su ulterior tratamiento.
  - b) Si es factible efectuar de manera acabada resguardo y preservación de datos y elementos (evidencia lógica) contenidos en los dispositivos a analizar, de esta manera se garantiza evitar la desnaturalización del material original;

considerando la posibilidad de determinar la operatividad del material objeto de prueba, en cuyo caso se debe evaluar si dicha acción provocará la desnaturalización del elemento, en cuya situación debería ordenarse el trabajo como pericia.

- c) Disponiendo de elementos precisos de búsqueda y colaboración de la investigación para el análisis, permite determinar la vinculación e importancia para la causa del elemento bajo estudio y su contenido (en aquellas situaciones donde se efectuó secuestro sin análisis).
- 2) Ante la situación de no poder garantizar el resguardo y preservación de los datos:
    - a) Disponer de elementos concretos para establecer el propietario del dispositivo y su posible vinculación a causa judicial: Por un lado, el motivo de establecer el propietario es a fin de proceder a su restitución, o en caso contrario, definir el destino del material, por otro lado, determinar su vinculación en causas judiciales y su ulterior tratamiento.
    - b) Si no es factible efectuar de manera acabada resguardo y preservación de datos y elementos (evidencia lógica) contenidos en los dispositivos a analizar, se debe disponer de certeza de haber obtenido los elementos necesarios y suficientes vinculados a la causa, garantizando no desnaturalizar el material original; considerando la posibilidad de determinar la operatividad del material objeto de prueba, en cuyo caso se debe evaluar si dicha acción provocará la desnaturalización del elemento, en cuya situación debería ordenarse el trabajo como “pericia”.
    - c) Disponiendo de elementos precisos de búsqueda y colaboración de la investigación para el análisis, permite determinar la vinculación e importancia para la causa del elemento bajo estudio y su contenido; en aquellas situaciones donde se efectuó secuestro sin análisis.

Una vez que se determinó si el objeto es prescindible o no en el proceso penal en que el encuentra secuestrado, las acciones técnicas que se proponen, son tendientes a la reutilización o reasignación de los materiales una vez analizados, con observancia de vinculación a otras causas judiciales del mismo material y aspectos procesales; debiendo tener en cuenta:

- La obtención de réplica del contenido de los dispositivos.



- El relevamiento de datos identificativos de cada elemento y análisis de contenido a fin de determinar el posible propietario del elemento, independientemente de los elementos vinculados a la causa.
- Consulta de datos identificativos de cada elemento con la oficina que corresponde de la Policía de la Provincia de Córdoba, tendiente a establecer causa y propietario del mismo.
- Una vez que la investigación toma conocimiento de los resultados obtenidos en los procesos anteriores, debe determinar el destino y acción a seguir de los materiales prescindibles.
- Desnaturalización (sanitización/flasheo/destrucción/reciclado) de cada elemento prescindible ya analizado.
- Preservación física con remisión al destino de cada elemento que ya fue desnaturalizado.
- Determinación del envoltorio y destino de los elementos destruidos.

Previo a continuar con el desarrollo de la temática presentada, es menester incorporar ciertos conceptos. Definimos como sanitización, en manejo de información confidencial o sensible, al proceso lógico y/o físico mediante el cual se remueve información considerada sensible o confidencial de un medio ya sea físico o magnético, ya sea con el objeto de desclasificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.

La sanitización de un dispositivo móvil se logra por medio del proceso lógico o por medio del proceso físico:

- La sanitización lógica se realiza mediante un borrado seguro, que comprende un conjunto de técnicas que tienen como objetivo volver imposible la recuperación de la información almacenada en el medio magnético por medios digitales. Estos métodos de borrado comprenden usualmente la sobre escritura de ceros y/o unos a nivel de bit en procesos repetitivos.
- La sanitización física requiere de la destrucción del medio físico más allá de condiciones de posible recuperación. Para cada tipo de medio físico existen técnicas herramientas y maquinarias diseñadas para su destrucción.

- El flasheo de un smartphone consiste en cambiar o actualizar el sistema operativo, permitiendo agregar características de funcionamiento al dispositivo. Se puede interpretar también como el “borrado” del sistema operativo y volverlo en condiciones de funcionamiento iniciales o de fábrica.
- La destrucción es la técnica o el método más seguro de borrado. Puede aplicarse a diferentes tipos de medios de almacenamiento desde discos duros y cintas, hasta dispositivos móviles como smartphones. Debe ser realizada por expertos en el tema, y en ambientes especialmente preparados. Algunas técnicas de destrucción controlada son:
  - Trituración
  - Incineración del equipo
  - Aplicación de químicos como ácido
  - Elevación de la temperatura
  - Magnetización
  - Aplicación de altos voltajes por encima de las especificaciones del fabricante, entre otras.

El tiempo estimado de este procedimiento depende principalmente de la técnica utilizada y del grado de seguridad que se desea obtener, ya que un proceso más minucioso toma más tiempo, pero garantiza que la información no será recuperada en un futuro.

En cuanto al reciclado los smartphones son llevados a un lugar específico, denominados puntos limpios. En dichos establecimientos se realiza la clasificación de toda la chatarra electrónica, para luego continuar el camino hacia el destino del reciclaje. Para reciclar un teléfono móvil, se funde el equipo a 1200 °C, con el fin de poder separar los diferentes metales y plásticos que lo componen, y de esta manera poder avanzar en el proceso de reciclado. A esta altura, se separan los elementos contaminantes de aquellos que pueden ser reutilizados. Componentes como plástico, aluminio, cobre o vidrio se procesan para fabricar nuevos productos.

Continuando con el tema de la desnaturalización de la evidencia digital, mencionamos que se ofrecen dos alternativas de implementación de los procesos de desnaturalización de dispositivos tecnológicos.

### 1) Vuelta al depósito

- Si en el oficio de remisión de material no consta la requisitoria de identificación de propietario, se realiza la labor forense habitual.
- Caso contrario, si se solicita la identificación de propietario debe efectuarse las gestiones necesarias con la oficina de gestión pertinente ante las empresas que brindan el servicio de telefonía móvil celular cuando son dispositivos móviles y analizar en procura de individualizar al propietario.
- En el caso de solicitar la identificación de propietario del elemento para analizar, efectuar consulta con oficina correspondiente de la Policía de la Provincia de Córdoba, tendiente a establecer causa y propietario.
- Si al concluir la labor forense habitual, en el oficio de remisión de material no consta la acción que debe realizarse al material ni el destino del mismo, se remitirá al depósito de dónde provino.
- Del mismo modo si se determina efectuar “pericia”, hasta que la misma sea ordenada; repitiendo el proceso desde el primer punto.

### 2) Sin vuelta al depósito

- Si en el oficio de remisión de material no consta la requisitoria de identificación de propietario, se realiza la labor forense habitual.
- Caso contrario, si se solicita la identificación de propietario debe efectuarse las gestiones necesarias con la oficina de gestión pertinente ante las empresas que brindan el servicio de telefonía móvil celular cuando son dispositivos móviles y analizar contenido en procura de individualizar al propietario.
- En el caso de solicitar la identificación de propietario del elemento para analizar, efectuar consulta con la oficina correspondiente de la Policía de la Provincia de Córdoba, tendiente a establecer causa y propietario.
- Si al concluir la labor forense habitual, en el oficio de remisión de material consta la acción que debe realizarse al material y el destino del mismo, se efectuará la desnaturalización

(sanitización/flasheo/destrucción/reciclado); labrando el acta correspondiente.

- Preservación física con remisión al destino de cada elemento desnaturalizado (sanitizado/falseado/reciclado). En el caso del proceso de reciclado se debe efectuar preservación física y remitir al destino que se indique.
- Preservación física masiva de los elementos destruidos con remisión al destino que se indique.
- Cuando se dictamina “pericia”, el material no es sometido al efecto de los dos puntos anteriores y se remite al depósito, hasta que la misma sea ordenada.

A continuación se describen las consideraciones generales a tener en cuenta para el proceso de desnaturalización:

<b>Proceso de Desnaturalización</b>	<b>Ventajas</b>	<b>Desventajas</b>
Sanitización	<p>Imposibilidad de tomar contacto con datos contenidos en el almacenamiento que estaban relacionados a la causa judicial, evitando la minería de datos.</p> <p>Permite la reutilización del espacio de almacenamiento de manera segura, lo que evita el incremento de residuo tecnológico.</p> <p>No genera impacto ambiental.</p>	<p>Es un proceso irreversible.</p> <p>Su reutilización evita la renovación del parque tecnológico.</p>
Flasheo	<p>Imposibilidad de tomar contacto con datos contenidos en el almacenamiento del dispositivo que estaban relacionados a la causa judicial, evitando la minería de datos.</p> <p>Permite la reutilización del</p>	<p>Es un proceso irreversible.</p> <p>Dependiendo del dispositivo, se puede obtener un comportamiento anómalo del mismo.</p>

	dispositivo, bajo ciertas condiciones.	
Destrucción	Reducción del espacio utilizado por la cosa. En el caso de los dispositivos móviles, fomenta la renovación del parque tecnológico.	Es un proceso irreversible. Los residuos generados del proceso de destrucción provocan impacto ambiental. Los residuos demandan un tratamiento particular.
Reciclaje	Reduce el riesgo de impacto ambiental. Permite la reutilización de materiales.	Demanda un tratamiento particular de sus componentes.

### *Equipamiento*

Hasta el momento no hemos mencionado el equipamiento necesario para llevar a adelante un correcto y acabado proceso de desnaturalización.

Si consideramos la opción de sanitización (equipos informáticos con medios de almacenamiento magnético):

- WIPEMASSTER o GIZMODO (para sanitizar discos rígidos)
- Winhex, WipeDriver Pro y/o herramientas para Linux Ubuntu (para sanitizar tarjetas de memoria, discos sólidos y discos rígidos de tamaño y conectores no standard)

Si consideramos la opción de flasheo (dispositivos móviles)

- Cyclone Box para desbloquear, flashear y reparar celulares Nokia.
- Advanced Turbo Flasher (ATF Box), AXE Box, CRUISER Pro Box, AVATOR Box, CYCLONE Box, DREAMBOX SE
- Cajas y dongles para flasheo, reparación y liberación de IMEI y teléfonos celulares. Medusa Box + Pegasus Box.
- BB-BOX.
- UST PRO (cajas de desbloqueo, flasheo y reparación).

- SMART-CLIP+SCARD/UID-BOX NOKIA BB5  
UNLOCK/SETOOL3/ULT-PRO LG/KIT GSM UNLOCK 2008.

Si consideramos la opción de destrucción (medios de almacenamiento ópticos, tarjeta SIM y dispositivos móviles)

- Para el caso de CD/DVD y tarjetas, un destructor de CD's / DVD's y tarjetas.
  - Para el caso de dispositivos móviles:
    - i. Se puede aplicar destrucción de materiales sin reciclado de los mismos, lo que demanda un mecanismo de embalaje para enterramiento hermético sin tratamiento.
    - ii. Se puede aplicar destrucción de materiales con reciclado de materiales, lo que demanda cumplir con ciertas normativas y disponer de un mecanismo de embalaje para enterramiento hermético sin tratamiento.

Si consideramos la opción de Reciclado solo es aplicable a dispositivos que no son de tecnología anterior a GSM.

#### *Borrado seguro de datos para Android*

Al hablar de desnaturalización de la evidencia digital, planteamos en forma general diferentes procedimientos que permiten desvincular la información sensible de los dispositivos y qué hacer con estos una vez que ya no son de utilidad para una causa.

Ahora cuando de borrar información sensible se trata, tenemos que garantizar que realizaremos un borrado seguro de dicha información.

Específicamente para los smartphones con Android existen diferentes técnicas de borrado seguro. El borrado seguro es un procedimiento que nace a partir de la necesidad de eliminar toda aquella información que permanece en el medio de almacenamiento del dispositivo, incluso después de haber sido borrada.

#### Alternativas

- 1) Reseteo de fábrica de Android y formateo memoria microSD (Seguridad muy baja)

Con el dispositivo en nuestro poder, seleccionamos la opción de Privacidad y desde las opciones disponibles elegimos la opción que indica resetear datos de fábrica. Una vez finalizado el reset y cuando el dispositivo tenga de nuevo la configuración de

fábrica, se habrán borrado todos los datos (aplicaciones, configuraciones y caché) almacenados en la memoria interna; sin embargo todo lo almacenado en la tarjeta de memoria permanecerá ahí a pesar del restablecimiento.



Este método posee una seguridad baja, el problema está en que el reseteo de fábrica de Android no es muy sólido. Para ejemplificar este hecho, Avast! (software antivirus de la firma checa AVAST Software) compró en la web 20 móviles Android usados, y utilizó un programa muy simple y de fácil acceso, destinado a la recuperación de datos y restauración de archivos borrados. La cantidad de datos que se recuperaron fue increíble y prueba que un simple borrado desde el dispositivo no es suficiente.

La razón por la que ocurre esto se debe a que la función de borrado en Android no elimina físicamente la información de los módulos de memoria, sino que la marca como libre al sistema operativo, para que pueda reescribir encima de ésta. De forma similar, y con versiones de Android previas a la 3.0, ocurre cuando se formatea el teléfono. Es decir que cuando se borra un archivo, en realidad sigue allí, con la diferencia de que ya no es accesible de forma directa para el usuario.

En resumen, el reseteo de fábrica en Android no realiza un borrado seguro de la información, y un proceso convencional de recuperación forense tiene grandes probabilidades de restaurar una parte significativa del contenido original.

Otro aspecto a tener en cuenta, es que la mayoría de teléfonos Android vienen equipados con una tarjeta microSD que podremos encontrar en algún lugar del mismo. Una opción es transferir todos los datos que contiene la tarjeta a otro dispositivo, ya sea una notebook, disco, o cualquier otro dispositivo que permita almacenar este tipo de información, u otra tarjeta microSD. Para vaciar la tarjeta, se debe conectar el teléfono a una computadora mediante un cable USB y formatearla. Esta acción también puede realizarse desde el propio teléfono. En el icono

de Ajustes seleccionamos almacenamiento en tarjeta y elegimos la opción de Formatear tarjeta SD.

## 2) Encriptar Datos de Smartphones con Android (Seguridad Media)

Actualmente Android ofrece una solución, en sus últimas versiones, que permite someter al smartphone a un proceso de encriptación. A partir de Android 3.0, existe un cifrado para el restaurado de fábrica que se aplica a los dispositivos.



La opción de cifrado se encuentra en la mayoría de teléfonos en el apartado Ajustes, Seguridad, Cifrar dispositivo, Memoria, Encriptación de memoria del teléfono, lo que nos permite establecer una clave antes de formatear la memoria interna.

## 3) Utilizar Herramientas de Borrado Seguro (Seguridad Alta/Muy Alta)

Cuando borramos un archivo, lo que estamos haciendo en definitiva es enviarlo a la papelera de reciclaje. Únicamente cuando se vacía la papelera, el archivo ya no estará visible para el usuario en su sistema operativo. Pero que no esté visible no significa que no se pueda recuperar.

Ejemplifiquemos esta situación: suponemos que tenemos un libro con un índice. Cada página de nuestro libro es un archivo. Lo que hacemos al borrar un archivo es decirle al índice que esa página no es necesaria, con lo cual si quisiésemos escribir en nuestro libro podríamos usarla. Borramos la línea del índice que apunta a esa página. Sólo hemos modificado el índice. Únicamente si escribimos otra vez encima se borraría el contenido de la página. Mientras podríamos leer todas las páginas de nuestro libro secuencialmente y encontraríamos esa página intacta (esto es lo que hacen los programas de recuperación de datos).

El borrado seguro consiste en escribir en esa página información unas cuantas veces, de forma que aunque la recorramos, lo único que veamos sea información sin sentido. En esto es en lo que se basan los métodos de borrado seguro, en sobre escribir nuestro archivo con información, un número determinado de pasadas.



Para introducir los métodos más comunes utilizados en el borrado seguro de información, presentamos la siguiente tabla:

Método de borrado	Definición	Nivel de seguridad
Grado 1 Super Fast Zero Write	Sobre escritura del soporte con un valor fijo (0x00) en cada tercer sector.	Bajo
Grado 2 Fast Zero Write	Sobre escritura del soporte con un valor fijo (0x00) en cada sector.	Bajo
Grado 3 Zero Write	Sobre escritura del soporte con un valor fijo (0x00) en todo el área al completo.	Bajo
Grado 4 Random Write	Sobre escritura del soporte con valores aleatorios. Su fiabilidad aumenta con el número de pasadas.	Medio
Grado 5 Random & Zero Write	Después de sobre escribir el soporte con valores aleatorios, se vuelve a sobre escribir de nuevo con un valor fijo (0x00), sobre escribe con valores aleatorios y termina con escritura de valor cero; este método es más seguro que Zero Write.	Medio
Grado 6 US Navy, NAVSO P-5239-26 – MFM	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con MFM (Modified Frequency Modulation). El método consiste en la escritura de un valor fijo (0xffffffff) sobre el soporte, después un valor fijo (0xbfffffff), y finalmente una serie de valores aleatorios. El área de datos se lee para verificar la sobre escritura. El método suele ser aplicado sobre disquetes.	Medio
Grado 7 US Navy, NAVSO P-5239-26 – RLL	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con RLL (Run Length Limited). Este método aplica la escritura de un valor fijo (0xffffffff) sobre el soporte grabado, un valor fijo (0x27ffffff), y finaliza con valores	Medio

	aleatorios. El área de datos se lee para verificar la sobre escritura. El método es aplicable a discos duros y soportes ópticos como el CD, DVD o el disco BlueRay.	
Grado 8 Bit Toggle	Sobre escritura de toda la zona de datos cuatro veces, primero con el valor (0x00), sigue con el valor (0xff), luego (0x00) y finaliza con (0xff).	Medio
Grado 9 Random Random Zero	Sobre escritura del soporte dos veces con valores aleatorios, una vez más con un valor fijo (0x00). Vuelta a sobre escribir dos veces con valores aleatorios y una última vez con ceros; el método es más seguro que Random & Zero Write.	Medio
Grado 10 US Department of Defense (DoD 5220.22-M)	Este método de borrado fue introducido por el Departamento de Defensa de los EE.UU. (Pentágono) y es conocido como "DoD5220.22-M". El método consiste en la sobre escritura del soporte con un valor fijo determinado una vez (por ejemplo 0x00), seguidamente se escribe su valor complementario (0xff) una vez, y finalmente se repasa con valores aleatorios una vez. El disco se verifica para comprobar la escritura correcta de los valores.	Medio
Grado 11 US Air Force, AFSSI5020	Estándar de las Fuerzas Aéreas de los EE.UU. (US Air Force) AFSSI5020. Este método de borrado primero sobre escribe el soporte con un valor fijo (0x00), después otro valor fijo (0xff), y finalmente un valor aleatorio constante. Se comprueba al menos un 10% del disco para verificar la sobre escritura.	Medio
Grado 12 North Atlantic Treaty Organization - NATO standard	Estándar de borrado de la OTAN (North Atlantic Treaty Organization). Sobre escribe el soporte siete veces. Las primeras seis pasadas son de sobre escritura con valores fijos alternativos entre cada pasada (0x00) y (0xff). La séptima pasada sobre escribe con un valor aleatorio.	Alto
Grado 13	El método fue creado por Peter Gutmann en 1996.	Alto

Peter Gutmann Secure Deletion	Probablemente sea el método de borrado de datos más seguro que existe sin combinación con otros métodos. La sobre escritura del soporte se realiza grabando valores aleatorios cuatro veces sobre cada sector. Seguidamente se sobre escribirá todo el soporte con valores pseudo aleatorios sobre cada sector durante veintisiete pasadas. Para terminar, se escribirán valores aleatorios durante cuatro pasadas sobre cada sector. En total, se realizan treinta y cinco pasadas de sobre escritura.	
Grado 14 US Department of Defense (DoD 5220.22-M) + Gutmann Method	Método de alta seguridad consistente en 35 pasadas, complementables con iteraciones de Mersenne, para agilizar los procesos de borrado seguro mediante la generación de números pseudo aleatorios. Combina el Grado 13 y el 10.	Muy Alto

A modo de síntesis sólo nos remitiremos a nombrar las más utilizadas para realizar un Borrado Seguro. La duración del proceso depende de la técnica aplicada. El borrado de los datos se hace, en la mayoría de los casos mediante sobre escritura de los mismos con diversos valores. Algunos ejemplo de herramientas de este tipo:

- ERASER o Eraser Portable
- Darik's Boot and Nuke SE
- Zilla Data Nuker
- Smart Data Scrubber
- Mareew Free Eraser
- SuperShredder
- Clean Disk Security
- Absolute Shield File Shredder
- AHHB Power Delete
- Simple File Shredder
- Disk Redactor
- EZ Wipe
- UBCD4Win: Ultimate Boot CD for Windows (bootable recovery CD)

- Secure RM (SRM) (Linux)
- Clonar disco duro, con borrado seguro de disco origen - CopyWipe
- Darik's Boot and Nuke
- HDD Low Level Format Tool Free
- Disk Wipe
- Dflabs DIM
- CCleaner
- SDelete

### Consideraciones Jurídicas Legales

Cerrando la presentación de esta temática, no debemos dejar de mencionar algunas consideraciones jurídicas respecto a la desnaturalización de la evidencia digital. A continuación resumiremos algunas reflexiones y derivaciones.

Dichas reflexiones apuntan a la necesidad de implementar un marco legal para reglamentar la desnaturalización controlada de evidencia vinculada a las TIC's, con la finalidad de su reciclado, reutilización y destrucción de material tecnológico ya analizado y considerado prescindible en la causa.

El Código Procesal Penal, Ley N° 8123 de la Provincia de Córdoba, en su artículo 363, establece que en un proceso penal la autoridad penal correspondiente ofrece la posibilidad de incorporar prueba al mismo mediante una notificación de las partes, para que en un término común de diez días, se ofrezcan pruebas, ellas podrán ser de distinta naturaleza, con las consideraciones que correspondan en la aceptación o el rechazo, durante ese período el Ministerio Público y las partes presentarán la lista de testigos y peritos, con indicación del nombre, profesión y domicilio a tales efectos.

De igual manera, en el Art. 210, "...El Tribunal o el Fiscal de Instrucción, si no fuere necesario allanar domicilio, podrá disponer que sean conservadas o recogidas las cosas relacionadas con el delito. Las sujetas a confiscación o aquéllas que puedan servir como prueba. Para ello, cuando fuere necesario, se ordenará su secuestro..." y en el Art. 217 se manifiesta "Devolución. Los objetos secuestrados que no estén sometidos a confiscación, restitución o embargo, serán devueltos, tan pronto como no sean necesarios, a la persona de cuyo poder se sacaron. Esta devolución podrá ordenarse provisionalmente, en calidad de depósito, e imponerse al poseedor la obligación de exhibirlos. Los efectos sustraídos serán devueltos, en las mismas condiciones y según

corresponda, al damnificado o al poseedor de buena fe de cuyo poder hubieran sido secuestrados...”.

En relación a las pericias y según el Art. 239, “Conservación de Objetos. El órgano judicial y los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse. Si fuera necesario destruir o alterar los objetos analizados o hubiere discrepancias sobre el modo de conducir las operaciones, los peritos deberán informar antes de proceder”.

Para la restitución de los objetos secuestrados el C.P.P. de la Provincia de Córdoba, lo trata en los artículos 542 al 545, de ellos el Art. 543 “Cosas Secuestradas. Restitución y Retención. Las cosas secuestradas que no estuvieren sujetas a confiscación, restitución o embargo serán devueltas a quien se le secuestraron. Si hubieran sido entregadas en depósito antes de la sentencia, se notificará al depositario la entrega definitiva. Las cosas secuestradas de propiedad del condenado podrán ser retenidas en garantía de las costas del proceso y de la responsabilidad pecuniaria impuesta”, en el Art. 545 “Objetos no Reclamados. Cuando después de un año de concluido el proceso, nadie acreditare tener derecho a la restitución de cosas que no se secuestraron de poder de personas determinadas, se procederá en la forma establecida en la Ley 7.972 (Ley de destino de los bienes secuestrados en causas penales)”.

Referencias:

(1) Cardone Arsenio Antonio, Guayanes Gustavo José. Material publicado en el “Simposio Argentino de Informática y Derecho, SID 2013”. Año 2013

# **CAPÍTULO 10**

# **CONCLUSIONES**

### Conclusiones

En este capítulo final, y en concordancia con las aspiraciones planteadas al comenzar este trabajo, presentamos una serie de reflexiones, consecuencia del desarrollo principalmente teórico pero con instancias prácticas, que hemos podido llevar adelante.

Las tareas de ayuda a la investigación no necesariamente tienen que ver con los denominados delitos informáticos, sino con la recolección de evidencia digital. Las tareas forenses en general, y las pericias informáticas en particular, requieren de profesionales con conocimientos certificados, y actualizados permanentemente en nuevas técnicas y herramientas.

Recuperamos en esta instancia, los objetivos establecidos al comenzar este proyecto de investigación. Allá por el comienzo nos propusimos en base al estudio de metodologías, protocolos y herramientas de pericia informática de teléfonos inteligentes, extraer conclusiones que aportasen mejoras a los actuales procesos de peritaje ejecutados en el ámbito de la Provincia de Córdoba. En concreto, definimos los siguientes aspectos:

- Analizar teóricamente la normativa a nivel nacional y provincial y su relación con convenios internacionales.
- Investigar una serie de herramientas de forensia de teléfonos móviles inteligentes.
- Realizar el seguimiento de un caso testigo.
- Elaborar propuestas de mejora referidas a la materia.

A esta altura podemos afirmar que estos objetivos han sido concretados de manera satisfactoria. A continuación, desarrollamos las aristas más relevantes de la investigación, en articulación con los objetivos enumerados.

En primer lugar consideramos que el Poder Judicial de la Provincia de Córdoba, en particular la DACTI, está operando en base a lineamientos estándares a nivel mundial, en relación al análisis forense de smartphones. Son evidentes las consecuencias de las inversiones realizadas, tanto en equipamiento como en recursos humanos, que posicionan al Poder Judicial de Córdoba en una situación privilegiada a nivel nacional. Fue claramente acertada la decisión administrativa de crear la Dirección de Análisis Criminal y Tecnologías de la Información, otorgándole una estructura que coadyuve a la consecución de sus fines. Por otra parte, nos parece relevante que todo el software y



hardware empleado al interior de la dirección para el análisis de smartphones sea de tipo forense, garantizando de cierta forma, la calidad de la evidencia.

No obstante, fue posible identificar ciertos aspectos susceptibles de mejora, los cuales introducimos a continuación.

Sería óptimo contar con alguna especie de protocolo escrito en materia de análisis forense informático, en especial, de análisis de dispositivos móviles, al estilo del citado “Protocolo de Actuación para Pericias Informáticas” o del “Protocolo para Pericias Informáticas sobre telefonía celular”, ambos redactados por el Poder Judicial de la Provincia de Neuquén. Los operadores de justicia necesitan un marco que les permita conocer si la metodología utilizada para la obtención de la evidencia digital fue la adecuada. Tenemos conocimiento de que hubo una serie de intentos en este sentido, pero estos fracasaron debido a que el personal de la dirección es escaso en relación a la carga de trabajo asignada. A su vez, estos ensayos pretendieron ser demasiado detallados, extensos y descriptivos, en detrimento de la practicidad. Consideramos en base al material analizado en este trabajo que debe existir cierto balance entre detalle, flexibilidad y pragmatismo, un protocolo debe servir de guía operativa en modo genérico, debido a la naturaleza evolutiva de esta clase de dispositivos. Un documento de este tipo permitiría formalizar la capacitación a nuevos integrantes del equipo de trabajo, estandarizar criterios entre Policía Administrativa y Policía Judicial, sobre todo al momento del secuestro de la evidencia, informar de forma unívoca los procedimientos realizados al interior de la dirección, comparar e intercambiar lineamientos con otras fuerzas de seguridad (Federal, Metropolitana, otras provincias), entre otras ventajas. Distinguimos como carácter de tal protocolo, la actualización en el tiempo, como herramienta dinámica de trabajo. Cabe destacar que no creemos necesaria una redacción desde foja cero, más bien consideramos como base y aporte las guías de buenas prácticas existentes y validadas a nivel internacional, sobre las cuales deberían efectuarse ciertas adecuaciones al panorama local.

Así mismo, pensamos que un protocolo o estándar de las características mencionadas de alcance nacional sería un instrumento muy valioso a la hora de asegurar el adecuado tratamiento de la evidencia digital a lo largo y ancho del país. Tal protocolo debería ser elaborado de manera participativa entre las provincias, con observancia de la adhesión al Convenio de Cibercriminalidad de Budapest.

Es menester resaltar que pudimos observar que los procedimientos y metodologías aplicados al interior de la dirección están en concordancia con respecto a guías de buenas prácticas trascendentes a nivel internacional.

En alusión a la cadena de custodia, en particular al uso de la ficha de traza, estimamos que esta no debiera ser privativa del fuero narcotráfico. No creemos que sea necesaria demasiada inversión económica para implementar esta ficha de seguimiento adherida al dispositivo a lo largo de los distintos fueros, y sería notable el fortalecimiento de la cadena de custodia de la prueba de aplicarse universalmente.

En referencia a la preservación de la integridad de la prueba, pudimos observar que se trabaja con el algoritmo de hash MD5, argumentando cuestiones de rapidez. Según propias palabras de los técnicos de la DACTI, con las sucesivas actualizaciones del equipamiento forense, el uso del tiempo se ha maximizado, en particular, el tiempo de obtención de la imagen del dispositivo se ha reducido notablemente. Es de público conocimiento que este algoritmo es hoy por hoy, altamente vulnerable, por lo que utilizarlo para proteger información tan sensible, es como mínimo, un descuido importante. Proponemos en relación a este aspecto, la utilización de SHA-1 o SHA-2 como algoritmos criptográficos.

Con respecto a las herramientas hardware y software empleadas para llevar a cabo los análisis forenses de smartphones, no estamos en condiciones de efectuar mayores recomendaciones sobre la eficacia de las mismas, debido a la serie de inviabilidades con las que nos topamos al intentar efectuar pruebas comparativas entre las diversas tools disponibles en el mercado. Nos limitamos a indicar que la intención de los miembros de la DACTI de emplear dos o más aplicaciones forenses de distintos proveedores para la obtención y análisis de imágenes es correcta y fortalece la veracidad de los resultados de la pericia. Así mismo, observamos que el sistema UFED es utilizado en conformidad con las indicaciones del fabricante. El único aspecto que atrajo nuestra atención acerca de UFED es que solo cuenta con lector de tarjetas SIM comunes, que hoy por hoy, son las menos usuales. El técnico debe emplear un adaptador para micro o mini SIM, situación no del todo deseable, que debería ser resuelta en los próximos lanzamientos de la herramienta.

En alusión a la desnaturalización de la evidencia tecnológica, caracterizamos de urgente y prioritario el tratamiento que a este tema debe brindarse. La problemática tiene una serie de aristas a considerar, por un lado, el aspecto normativo, por otro, la infraestructura, las cuestiones procedimentales y también, la necesidad de

concientización en la materia. Es preocupación de los mismos integrantes de la DACTI tanto el estado de los depósitos como la falta de tratamiento adecuado que se le da a esta clase de materiales. En primera instancia, debe existir un marco normativo para el tratamiento de esta clase de dispositivos, una vez que finaliza su vida útil como evidencia en un proceso penal. Luego, será necesario contar con un espacio físico e instrumentos adecuados para acondicionar los materiales para su ulterior destino, mediante sanitización, flasheo, destrucción o reciclaje. Todos los procedimientos deben ser debidamente estandarizados y tener como máxima, la protección del medio ambiente y la salud de los seres humanos. A su vez, sería óptimo acompañar esta iniciativa con planes de concientización al interior del Poder Judicial sobre la importancia de cerrar de manera apropiada el ciclo de vida del elemento probatorio.

Como último aspecto a rescatar, creemos que se debería incorporar algún sistema de auditoría interno, que permita realizar un control de calidad sobre el área, en especial sobre procesos y metodologías, que permita contar con información fehaciente para la toma de decisiones de inversión, infraestructura, equipamiento, capacitación a los recursos humanos, entre otros tópicos.

La temática abordada en el presente trabajo tiene alcance potencial para realizar un estudio de mayor envergadura. Los tópicos abarcados están en constante evolución y se constituyen en un área de investigación prioritaria para el esclarecimiento de actividades delictivas, cuya resolución en definitiva, contribuye a la preservación del orden social.