

# MANUAL DE INFORMÁTICA FORENSE II

(Prueba Indiciaria Informático Forense)

**Bases teóricas complementarias.**

**Metodología suplementaria:**  
computación móvil (tablet, celulares,  
iPhone, iPad, iPod, GPS, Mac, imágenes,  
audio, video, Android, CD, DVD)



**INCLUYE  
ACTUALIZACIÓN  
ON-LINE**

**María Elena Darahuge  
Luis E. Arellano González**

Prólogo del Ing. Jorge Omar Del Gener



MARÍA ELENA DARAHUGE  
LUIS E. ARELLANO GONZÁLEZ

# MANUAL DE INFORMÁTICA FORENSE II

(PRUEBA INDICIARIA INFORMÁTICO  
FORENSE)

Bases teóricas complementarias.  
Metodología suplementaria: computación  
móvil (tablet, celulares, iPhone, iPad, iPod,  
GPS, Mac, imágenes, audio, video,  
Android, CD, DVD)

Darahuge, María Elena

Manual de Informática Forense II / María Elena Darahuge y Luis Enrique Arellano González. - 1a ed. - Ciudad Autónoma de Buenos Aires :

Errepar, 2014.

E-Book.

ISBN 978-987-01-1682-0

I. Informática. Informática Forense. I. Arellano González, Luis Enrique

II. Título

CDD 657.4

Manual de informática forense II

Fecha de catalogación: 19/06/2014

ERREPAR S.A.

Paraná 725 (1017) - Buenos Aires - República Argentina

Tel.: 4370-2002

Internet: [www.errepar.com](http://www.errepar.com)

E-mail: [clientes@errepar.com](mailto:clientes@errepar.com)

ISBN: 978-987-01-1682-0

Nos interesan sus comentarios sobre la presente obra:

[editorial@errepar.com](mailto:editorial@errepar.com)

© 2012 ERREPAR S.A.

Queda hecho el depósito que marca la ley 11.723

No se permite la reproducción parcial o total, el almacenamiento, el alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u otros métodos, sin el permiso previo y escrito del editor. Su infracción está penada por las leyes 11.723 y 25.446.

Digitalización: Proyecto451

# ACTUALIZACIÓN ON-LINE

El contenido del presente libro se actualiza por Internet a través de nuestra página web.

Deberá ingresar a [www.errepar.com/libros](http://www.errepar.com/libros).



The screenshot shows a web browser window with the URL <http://www.errepar.com/libros/>. The page features a navigation menu on the left with categories like 'COMPañIA', 'PUBLICACIONES', and 'SERVICIOS'. The main content area displays a featured book: 'EL COMPORTAMIENTO ADMINISTRATIVO' by Herbert A. Simon, with a 'CONÓZCALO AQUÍ' button. Below this, a section titled 'Libros / Servicios Asociados' lists four books with 'INGRESAR' buttons: 'MANUAL DE INFORMÁTICA FORENSE', 'BLANQUEO LABORAL Y PROMOCIÓN Y PROTECCIÓN DEL EMPLEO REGISTRADO', 'CÓDIGO PROCESAL CONTENCIOSO ADMINISTRATIVO DE LA PROVINCIA DE BUENOS AIRES', and 'CONCURSOS Y QUIEBRAS'.

Seleccione la presente obra presionando el botón Ingresar, visualizará la siguiente pantalla:

The screenshot shows the Editorial Errepar website. The browser address bar displays "http://www.errepar.com/libros/". The page header includes the site name and contact information: "Atención al cliente", "011 4370-2002", and "clientes@errepar.com". A navigation menu on the left lists categories like "COMPañIA", "PUBLICACIONES", and "SERVICIOS". The main content area features a book listing for "EL COMPORTAMIENTO ADMINISTRATIVO" by Herbert A. Simon, with a "CONÓZCALO AQUÍ" button. Below this is a section titled "Libros / Servicios Asociados" with a login form for "MANUAL DE INFORMÁTICA FORENSE" by María Elena Darahuge and Luis E. Arellano González. The login form includes fields for "Usuario:" and "Clave:", an "INGRESAR" button, and a "Recordar Contraseña:" checkbox. There are also links for registration and password recovery.

La primera vez que intente consultar el material tendrá que registrarse como usuario, para lo cual se le pedirá que ingrese la clave de de acceso (22462691) y que complete una serie de datos personales.

Tenga presente que es muy importante que ingrese correctamente su dirección de correo electrónico, debido a que allí se le enviará su usuario y contraseña para acceder a los servicios asociados al libro.

Finalmente, presionando el icono correspondiente, tendrá acceso a las actualizaciones de esta obra.

# LOS AUTORES

## **Prof. Ing. María Elena Darahuge**

Licenciada e Ingeniera en Informática.  
Profesora Universitaria en Ingeniería en Informática, UCSA.  
Secretaria Académica del Curso de Experto en Informática Forense, FRA (UTN).  
Profesora Asociada de la materia Sistemas Operativos, UAJFK.

## **Prof. Ing. Luis Enrique Arellano González**

Abogado con orientación Penal, UBA.  
Licenciado e Ingeniero en Informática.  
Profesor Universitario en Ingeniería en Informática y en Criminalística, UCSA.  
Licenciado en Criminalística.  
Perito en Documentología, Balística y Papiloscopía, IUPFA.  
Director del Curso de Experto en Informática Forense, FRA (UTN).  
Profesor Asociado de la materia Sistemas Operativos, UAJFK.

# Índice de contenido

## **Portadilla**

## **Prólogo**

## **Prefacio**

## **Estructura general**

Orientación para la lectura del manual

## **PRIMERA PARTE - TEORÍA**

### **Capítulo 1 - Revisión de conceptos**

La naturaleza pericial de la Informática forense

Confiar en el cargo y no exigir idoneidad

Extrañas dependencias periciales

Comparación de perfiles profesionales

La Informática forense y sus especialidades

El vocablo “prueba”

Prueba documental clásica

Efectos del desconocimiento

Prueba documental informática

Breve guía de recolección de prueba documental informática

### **Capítulo 2 - Las medidas previas, preliminares o prueba anticipada en Informática forense**

Características

Requisitos doctrinarios

Fallo relacionado

### **Capítulo 3 - Revisión jurisprudencial**

Fallos relacionados

La resolución por Cámara

## **Capítulo 4 - Criterios a tener en cuenta**

Las posibilidades de falsificación de mensajes de correo electrónico  
Ejemplo de accionar ante eventualidad previsible  
El uso de formas alternativas de resolución de conflictos  
Tratamiento de residuos informáticos  
La basura ciberespacial  
Los riesgos de contaminarse  
¿Por qué debemos proteger el ciberespacio?  
Inserción legal de la problemática  
División de responsabilidades y tareas

## **Capítulo 5 - La cadena de custodia informático forense**

Cadena de custodia vs. privacidad  
La cadena de custodia en la práctica informático forense

## **Capítulo 6 - El contrato electrónico y la Informática forense**

Características del documento digital  
El contrato digital, como forma de celebración contractual a distancia (entre ausentes)  
El problema de la jurisdicción en el contrato electrónico internacional  
La prueba documental informática en el entorno regional

## **Capítulo 7 - El rol del perito informático forense en el proceso judicial**

Lo que se espera  
Síntesis

## **SEGUNDA PARTE - PROCEDIMIENTOS**

### **Capítulo 8 - Procedimiento de aplicación general para teléfonos celulares**

Etapa de identificación, registro, protección, embalaje y traslado

- Identificación y registro
- Protección del dispositivo
- Posibles estados en que se puede encontrar el dispositivo
- Encendido
- Apagado
- Embalaje y traslado
- Procedimiento para la recolección y protección de información - Elementos a recolectar
- Recolección de información de la tarjeta SIM
- Dispositivos iPhone
  - Sistema de archivos
  - Procedimientos y medidas preventivas para la protección, embalaje y traslado de dispositivos
  - Consideraciones previas
  - Procedimiento para iPhone encendido
  - Pantalla activa: Puede o no tener el código de acceso y la opción auto-bloqueo activa
  - Aislamiento del dispositivo de la red celular e inalámbrica
  - Procedimiento: El dispositivo tiene el código de acceso activado y está bloqueado para responder
  - Procedimiento para la comprobación del estado del código de acceso
  - Procedimiento para la verificación y secuencia del posible borrado remoto (*wipe*)
  - Procedimiento para iPhone apagado
  - Identificación y registro
  - Procedimiento para la identificación de dispositivos iPhones liberados (*jailbroken*)
- Etapas de recolección y adquisición de datos
  - Procedimientos de recolección de datos en dispositivos iPhone e iPad
  - Consideraciones previas
  - Método de recolección física

Procedimiento para la preparación de la duplicación de la memoria Flash NAND

Procedimiento para ejecutar la herramienta iRecovery

Descripción del método de duplicación de la partición de datos de usuario del dispositivo utilizando el método de Jonathan Zdziarski

Ejemplo del método de duplicación en un dispositivo liberado

Método de recolección lógica

Procedimiento para la recolección lógica de dispositivos iPhone

Método de recolección a partir de archivos de resguardo

Procedimiento para la recolección lógica a partir de los archivos resguardados con la herramienta iPhone Backup Extractor

Resguardos encriptados

Procedimiento para la recolección lógica de dispositivo iPhone, iPod táctil e iPad del resguardo efectuado con iTunes

Procedimiento para la recolección en iPhones

Etapa de análisis de datos

Análisis de la primera partición del sistema de archivo de iPhone (liberado)

Consideraciones previas

Análisis de la información adquirida o recolectada de los dispositivos iPhone

Procedimiento para la conversión de los archivos “.plist”

Consideraciones previas

Procedimiento para el montaje de imágenes “.dmg” en Mac

Procedimiento para el montaje de imágenes “.dmg” en Linux

Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux - Recuperación de

- archivos fragmentados
- Consideraciones previas
- Otras herramientas que efectúan la búsqueda de fragmentos de archivos
- Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux - Recuperación de archivos con cadenas de caracteres ASCII
- Consideraciones previas
- Otras herramientas que efectúan la búsqueda de fragmentos de archivos
- Procedimiento para el análisis de las bases de datos de sms con un editor en hexadecimal
- Consideraciones previas
- Procedimiento para el análisis de la estructura de directorios y partición de almacenamiento de datos en iPhone
- Consideraciones previas
- Procedimiento para el análisis de las aplicaciones preinstaladas en iPhone
- Consideraciones previas
- Análisis de la tarjeta SIM del teléfono iPhone
- Revisión de conceptos
- Dispositivos iPod
- Etapa de identificación, registro, protección, embalaje y traslado de dispositivos iPod
  - Procedimiento con el iPod encendido
- Etapa de recolección y adquisición de datos
  - Procedimientos de recolección de datos en dispositivos iPod
  - Consideraciones previas
  - Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh
  - Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh

Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh

Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh

Procedimiento para crear la imagen del dispositivo iPod con una estación de trabajo de Informática forense de Macintosh con el comando dc3dd (<http://sourceforge.net/projects/dc3dd/>)

Observación

Procedimiento para crear la imagen del dispositivo iPod con la herramienta de libre disponibilidad, FTK Imager, Forensic Tool Kit (<http://accessdata.com/support/adownloads>) en una computadora con sistema operativo Windows

Procedimientos sintetizados de recolección en diferentes modelos de iPod

Etapa de análisis de datos

Procedimiento para el análisis del sistema de archivos de iPod

Consideraciones previas

Procedimiento para el análisis del archivo de imagen del dispositivo iPod en una computadora Mac

Consideraciones previas

Síntesis - Lista de control

## **Capítulo 9 - Computadoras Apple Macintosh**

Consideraciones previas

Procedimiento para la preparación de la estación de trabajo de Informática forense Apple Macintosh

Instalación del sistema operativo

Síntesis - Lista de Control

Etapa de recolección y adquisición de datos

Procedimiento de adquisición de una imagen de una computadora Macintosh con una computadora

Macintosh

Consideraciones previas

Secuencia de pasos para la preparación de adquisición de la imagen

Procedimiento alternativo para la adquisición o duplicación de la imagen utilizando un CD de Linux en vivo

Consideraciones previas

Síntesis - Lista de control

Efectuar la imagen de Macintosh a Macintosh

Efectuar la imagen de una computadora dubitada

Macintosh con un CD/DVD de arranque o inicio en vivo

Procedimiento para determinar la fecha y hora en Macintosh

Consideraciones previas

Procedimiento para la recolección de datos de memoria volátil en un sistema desbloqueado

Consideraciones previas

Procedimiento para la recolección de datos de memoria volátil en un sistema bloqueado

Consideraciones previas

Síntesis - Lista de control - Descarga de la memoria volátil

Procedimiento para la recolección de datos en el modo de usuario único (Single User Mode)

Consideraciones previas

Etapa de análisis de datos

Procedimiento para el análisis de la información del inicio del sistema operativo y los servicios asociados

Consideraciones previas

Procedimiento para el análisis del sistema de archivos HFS+ de la imagen recolectada

Procedimiento para el análisis de directorios especiales (*bundle*) en el sistema de archivos HFS+ de la imagen recolectada

Consideraciones previas

Procedimiento para el análisis de archivos de configuración de red  
Consideraciones previas  
Procedimiento para el análisis de archivos ocultos  
Consideraciones previas  
Procedimiento para el análisis de aplicaciones instaladas  
Consideraciones previas  
Procedimiento para el análisis de espacio de intercambio (*swap*) y de hibernación  
Consideraciones previas  
Procedimiento para el análisis de sucesos o registros (*logs*) del sistema  
Consideraciones previas  
Procedimiento para el análisis de información de las cuentas de usuarios  
Consideraciones previas  
Procedimiento para el análisis del directorio de inicio (*Home*)  
Consideraciones previas  
Procedimiento para descryptar la carpeta de inicio del usuario cifrada por el servicio FileVault  
Consideraciones previas  
Síntesis - Lista de control  
Procedimiento para la recuperación de datos del navegador web Safari de la imagen adquirida  
Consideraciones previas  
Caché del navegador  
Íconos de la URL de los sitios (*webpagelcons.db*)  
Archivos plist  
Sitios más visitados (*TopSites.plist*)  
Marcadores (*Bookmarks.plist*)  
Descargas de archivos (*Downloads.plist*)  
Historial (*History.plist*)  
Última sesión (*LastSession.plist*)  
Cookies.plist

Síntesis - Lista de control  
Procedimiento para la función del navegador Safari como visor de archivos en el sistema operativo de Microsoft Windows  
Consideraciones previas  
Ubicación de los archivos plist en el sistema operativo de Microsoft Windows  
Procedimiento para la recuperación y análisis de elementos de correo electrónico e iChat de la imagen adquirida  
Consideraciones previas  
Procedimiento para la recuperación de mensajes del cliente de correo de Microsoft Entourage de Office: Mac 2008 para Mac  
Procedimiento para la recuperación y análisis de la libreta de direcciones (Address Book) de la imagen adquirida  
Consideraciones previas  
Procedimiento para la recuperación y análisis de datos del iChat de la imagen adquirida  
Consideraciones previas  
Síntesis - Lista de control  
Apple Mail  
Libreta de direcciones  
iChat  
Procedimiento para la recuperación y análisis de fotografías de la imagen adquirida  
Consideraciones previas  
Características de la aplicación iPhoto  
Ubicación de los archivos de iPhoto  
Síntesis - Lista de control  
Procedimiento para la recuperación y análisis de películas y videos de la imagen adquirida  
Consideraciones previas  
Síntesis - Lista de control

Procedimiento para la recuperación y análisis de archivos del procesador de texto Word y de documentos portables (PDF)  
Consideraciones previas  
Síntesis - Lista de control  
Procedimiento para el análisis del historial de conexiones de dispositivos  
Consideraciones previas  
Procedimiento para el análisis de conexiones Bluetooth  
Consideraciones previas  
Procedimiento para el análisis de conexiones VNC  
Consideraciones previas  
Procedimiento para el análisis de la aplicación Volver a mi Mac (Back to My Mac)  
Consideraciones previas

## **Capítulo 10 - Android**

Consideraciones previas  
Componentes de hardware de los celulares Android  
Componentes de software de los celulares Android  
Estructura del sistema de archivos en Android  
Estructura del encabezado (entrada de directorio)  
Tipos de memoria en los dispositivos Android  
Sistemas de archivos  
Procedimiento para crear un emulador de un dispositivo Android  
Etapa de recolección y adquisición de datos  
Procedimiento para la duplicación de los dispositivos USB de almacenamiento (UMS - USB *Mass Storage*) en dispositivos Android  
Consideraciones previas  
Procedimiento para la recolección lógica de datos en dispositivos Android  
Consideraciones previas  
Procedimiento para la recolección lógica de datos con AFLogical

Productos comerciales para la recolección de datos en Android

Procedimiento para la recolección física de datos

Consideraciones previas

Procedimiento para el acceso como usuario *root* por medio de las herramientas de software

Procedimiento para el método AFPhysical de imagen física del disco de las particiones de la memoria Flash NAND de Android

Síntesis - Lista de control

Etapa de análisis de datos

Procedimiento para el análisis del núcleo del sistema operativo Linux

Procedimiento para descargar la memoria RAM en Android

Procedimiento para el análisis de la línea de tiempo en YAFFS2

Consideraciones previas

Procedimiento para el análisis del sistema de archivos YAFFS2 con las áreas de reserva OOB

Consideraciones previas

Procedimiento para el análisis de fragmentos (*carving*) del sistema de archivos

Procedimiento para el análisis del sistema de archivos con el comando strings

Procedimiento para el análisis del sistema de archivos con el visor en hexadecimal ncurses-hexedit

Procedimiento para el análisis del contenido de los directorios del sistema de archivos de Android

Procedimiento para la creación de la línea de tiempo en el sistema de archivos FAT de la tarjeta SD

Procedimiento para el análisis del sistema de archivos FAT de la tarjeta SD

Procedimiento para el análisis de las aplicaciones en Android

Aplicación de mensajes

- Aplicación de ayuda de mensajes
- Aplicación de Navegador de Internet
- Aplicación de contactos
- Aplicación de Explorador de Medios
- Aplicación Google Maps
- Aplicación Gmail
- Aplicación de correo
- Aplicación Dropbox
- Aplicación Adobe Reader
- Aplicación YouTube
- Aplicación Cooliris Media Gallery
- Aplicación Facebook

## **Capítulo 11 - Discos ópticos**

- Análisis forense de almacenamiento de discos ópticos
  - Consideraciones previas
  - Composición física
  - Tabla de especificaciones de discos ópticos
  - Técnicas de escritura en los discos ópticos
  - Sistemas de archivos
- Etapa de identificación, registro, protección, embalaje y traslado
  - Identificación y registro
  - Protección de los discos ópticos
  - Rotulado de los discos compactos
  - Embalaje y traslado
- Etapa de recolección y adquisición de datos
  - Procedimiento para la duplicación de discos ópticos CD y DVD
- Etapa de análisis de datos
  - Procedimiento para la preparación del análisis de los discos ópticos
  - Procedimiento para el análisis del sistema de archivo ISO9660
  - Consideraciones previas

- Procedimiento para el análisis del sistema de archivo Joliet
- Procedimiento para el análisis del sistema Rock Ridge
- Procedimiento para el análisis del sistema UDF
- Procedimiento para el análisis del sistema HFS y HFS+ (Apple Macintosh)
- Procedimiento para el análisis del sistema El Torito
- Procedimiento para el análisis de la imagen adquirida con Autopsy para Windows
- Procedimiento general para el análisis de discos ópticos y/o de sus respectivas imágenes
- Consideraciones previas

## **Capítulo 12 - Dispositivos de navegación vehicular por gps tom tom**

- Consideraciones previas
- Etapa de identificación, registro, protección, embalaje y traslado de dispositivos de GPS Tom Tom
- Etapa de recolección y adquisición de datos
  - Procedimientos de recolección de datos en dispositivos de GPS Tom Tom
- Etapa de análisis de datos
  - Procedimiento para el análisis de datos en dispositivos de GPS Tom Tom

## **Capítulo 13 - Miscelánea**

- Características del software de bloqueo de escritura
- Procedimiento del uso de software bloqueador de escritura
- Referencia acerca del software bloqueador de escritura
- Dispositivos BlackBerry
  - Consideraciones previas
  - Tipos de almacenamiento de archivos en dispositivos BlackBerry
  - Etapa de identificación, registro, protección, embalaje y traslado

Procedimiento: El dispositivo tiene el código de acceso  
Etapa de recolección y adquisición  
Procedimiento para la adquisición física de datos  
Procedimiento para la adquisición de datos a partir del  
archivo de resguardo  
Consideraciones previas  
Etapa de análisis de datos  
Procedimiento para el análisis de los datos del archivo  
de resguardo  
Procedimiento para el análisis de archivos de  
imágenes  
Consideraciones previas  
Procedimiento de identificación de los metadatos del  
archivo de la imagen  
Análisis del contenido de la imagen  
Detección de rostros e imágenes de adultos  
Herramientas para reconocimiento de caras  
Herramientas para el análisis de los metadatos del  
archivo de la imagen  
Procedimiento para el análisis de los archivos de audio  
y video  
Consideraciones previas  
Tipos de archivos de audio y video  
Procedimiento para el análisis del contenido del video  
forense  
Guía para el procedimiento de video de la Agencia  
Federal de Investigaciones (FBI)  
Herramientas para el análisis de video de vigilancia  
Formulario de registro de evidencia de video

## **Anexo 1 - Procedimiento para la cadena de custodia en la pericia de informática forense**

Procedimiento  
Duplicación y autenticación de la prueba  
Operaciones a realizar  
Recolección y registro de evidencia virtual

Equipo encendido  
Procedimiento para el acceso a los dispositivos de almacenamiento volátil  
Procedimiento con el equipo encendido  
Equipo apagado  
Procedimiento para la detección, recolección y registro de indicios probatorios  
Procedimiento para el resguardo de la prueba y preparación para su traslado  
Traslado de la evidencia de Informática forense  
Inventario de hardware en la inspección y reconocimiento judicial  
Formulario de registro de evidencia de la computadora  
Formulario de registro de evidencia de celulares  
Rótulos para las evidencias  
Formulario - Recibo de efectos\*  
Formulario para la cadena de custodia  
Formulario de responsables de la cadena de custodia 4  
Modelo de Acta de inspección o secuestro  
Modelo de Acta de escribano

## **Anexo 2 - Estructura demostrativa judicial**

El problema de la prueba  
El problema de la redacción

## **Anexo 3 - La notificación por correo electrónico (ley 14.142, pcia. de Bs. As.)**

El correo epistolar y el aviso de retorno  
El correo electrónico y el concepto de *No Repudio*  
La casilla profesional y la casilla personal  
La casilla profesional como dato filiatorio  
Los servicios disponibles y los servicios necesarios

## **Anexo 4 - Uniformar las formas y formar los uniformes**

El peso del bronce

Idoneidad: capacitación vs. aceleración  
Informe estructurado vs. estructura informal  
Las contradicciones evidentes

### **Anexo 5 - Contradicciones judiciales**

Reflexión doctrinaria  
El problema subjetivo  
La “vulnerabilidad” ante la copia ilegítima (e ilegal)  
La acción penal en manos del Estado

### **Anexo 6 - Modelos**

Modelo de oficio a ISP  
Modelo de ofrecimiento de prueba documental  
informática y pericial informático forense en subsidio

### **Anexo 7 - La yapa** **Bibliografía**

# PRÓLOGO

Es indiscutible en la Argentina de hoy que la generación de conocimiento científico y de la innovación tecnológica ha tenido un desarrollo sustancial y un creciente reconocimiento en el papel clave que juega para generar respuestas efectivas a los requerimientos de la sociedad; concomitantemente, se ha revalorizado, de manera taxativa, el rol de las políticas públicas para su promoción y se han jerarquizado las instituciones con incumbencias en ese campo.

Indudablemente, no hay problema de conocimiento laboral, médico o de cualquier campo que no se relacione con el desarrollo exitoso de la ciencia y la tecnología. Las herramientas tecnológicas nos permiten hoy explorar nuevos campos y, por su parte, la investigación tecnológica nos permite favorecer y propiciar el desarrollo de software para la aplicación de técnicas científicas y analíticas especializadas que posibilitan identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal, como es el caso de la Informática forense. Esta relación entre los desarrollos de la Universidad Tecnológica Nacional-Facultad Regional Avellaneda y la presente publicación no es más que compartir otro nuevo desarrollo sobre el cual la tecnología echa luz.

El sistema operativo para forenses desarrollado en nuestra Facultad y que hoy se presenta en este ejemplar es el producto de diversos factores que lo han impulsado: los programas de incentivos que favorecen y promueven el desarrollo de software libres, la línea de desarrollo en investigación-acción en la que trabaja nuestra universidad y

la definición intrínseca de una institución como la nuestra cuya búsqueda se centra en dar respuesta efectiva a la creciente demanda de conocimiento en las diferentes áreas.

El software libre desarrollado para Informática forense es el primero en habla hispana en esta línea y, sin duda, marca un camino de fortalecimiento de las tecnologías específicas en América Latina. Según diversos críticos, en un futuro cercano no será el inglés la única lengua de la tecnología, evidentemente, han de ser los desarrollos tecnológicos generados en nuestros países los que inicien este proceso de cambio.

Es en esta línea en la cual la tecnología de software libre, como toda tecnología, involucra conocimientos, destrezas, herramientas, recursos y valores cuyo sentido debe centrarse en el compromiso intelectual como inclusión social; en este nuevo orden no nos queda más que dar la bienvenida a un nuevo libro que desde la concepción de libertad nos permite generar conocimiento y ofrecer respuestas a una sociedad mejor y en expansión.

Ing. Jorge Omar Del Gener  
Decano Facultad Regional Avellaneda  
Universidad Tecnológica Nacional .

*A calvo ad calvum, bove maiori discit arare minor: fronte  
praecipitium tergo lupi, ergo a priori, barba stulti discit  
tonsor.*  
(Anónimo)

## **PREFACIO**

Superada la instancia de reunir, clasificar, organizar y presentar conceptos constitutivos de la Informática forense, actividad que hemos concretado en el *Manual de Informática Forense*, con los errores, equívocos y falacias que el mismo pueda contener, ya que es obra de seres humanos y los seres humanos somos falibles, intentamos esta vez complementar aquellos puntos que quedaron poco claros y que luego, a partir de la práctica diaria, las consultas, y en particular los intercambios de opinión, es decir, gracias a la afortunada participación de tantos colegas profesionales, nos inducen a intentar complementar dicha obra.

Diversos problemas se han ido presentando respecto del tratamiento de la Prueba Documental Informática: el rechazo o desestimación de la misma, en diversos fueros, como resultante de errores metodológicos en el proceso de recolección de la prueba indiciaria informático forense, su certificación digital (eventualmente por autoridad competente), la preservación del material recolectado, su traslado y puesta a disposición del tribunal interventor. Estos temas ya han sido tratados en la obra antes referida, no obstante esta carece de una explicación explícita y detallada del procedimiento a realizar para asegurar la cadena de custodia del material probatorio obtenido.

A medida que explicitábamos dicho procedimiento, fueron surgiendo nuevos interrogantes, que ampliaron considerablemente los temas a tratar. Estos interrogantes forman parte de la propuesta académica que ofrecemos a nuestros lectores en la parte teórica que da inicio a la presente obra.

Por supuesto, aún nos restaba trabajar sobre los elementos innovadores que se agregan e integran diariamente a la tecnología informática: computación móvil, celulares, receptáculos de información variados, todos ellos susceptibles de análisis pericial informático forense y, por lo tanto, objeto de recolección de prueba documental informática. En la segunda parte del libro, se ofrecen una serie de procedimientos particulares para los casos más frecuentes. Esperamos que este se constituya en una guía de trabajo útil, para el profesional de la Informática forense que lo requiera y en particular para la formación académica de quienes sientan vocación por integrarse a esta actividad tan propia de este siglo en que vivimos.

Hemos preservado la metodología general de tratamiento teórico y práctico ofrecida en la obra anterior; el lector encontrará sustento para las afirmaciones, considerando los marcos criminalístico, informático (general y específico) y legal. Reiteramos lo expresado anteriormente: estamos seguros de no haber podido realizar una obra adecuada a las pretensiones anteriores, pero también podemos asegurar que, aunque se trata de una propuesta complementaria, dispersa, con fallas, criticable y perfectible, tiene el valor de ser una propuesta al fin.

# ESTRUCTURA GENERAL

*La metodología de recolección de prueba indiciaria informático forense es, al tratamiento de la prueba documental informática ofrecida, lo que la norma jurídica escrita es a la decisión consagrada por el Tribunal que juzga (obligación de sentenciar).*

Este segundo tomo ha sido planificado y desarrollado con el objeto de aportar al perito informático forense una guía de referencias y consultas rápida, sencilla y fundamentada que complemente los conceptos vertidos en el *Manual de Informática Forense*.

El primer tomo se sustentaba en la aplicación del método científico, con soporte metodológico sistémico y criminalístico, haciendo uso de tecnología pericial reconocida por su utilidad práctica y en especial en un marco legal estricto e ineludible. En este nuevo volumen, se intentó integrar dichos marcos, para conformar una Metodología Pericial Informático Forense estricta y científicamente fundamentada, la que se concreta en el correspondiente informe pericial.

En esta ampliación doctrinaria, hemos intentado completar los conceptos que establecimos con anterioridad y en especial poner énfasis en los mecanismos alternativos necesarios para el tratamiento de los elementos de computación móvil que nos inundan a diario y se integran a nuestra vida familiar, profesional y social.

## **Orientación para la lectura del manual**

Pensamos que la mejor manera de acercarse a la obra es realizar una lectura detallada del cuerpo principal teórico (es decir de la primera parte). Esto debería ser suficiente para aquellos profesionales que se aproximan a la especialidad forense con fines de obtener conocimientos generales y/o interactuar con otros profesionales, empleando un lenguaje en común, algo de suma utilidad para los operadores del Derecho a la hora de interactuar con la prueba documental informática y sus características específicas. En lo que respecta a los interesados en llevar a la práctica la disciplina informático forense, deberían acceder a la segunda parte (práctica) con el fin de reconocer e implementar, *a posteriori*, los procedimientos propuestos para los distintos tratamientos de recolección de prueba documental informática, que no forman parte del clásico equipo de computación personal, con el que frecuentemente se trata en la actividad pericial habitual. Todos los documentos que constituyen la obra se encuentran disponibles en su versión digital, para uso de quienes los necesiten y los consideren pertinentes.

Es imprescindible tener en cuenta cuál es el rol del perito dentro del proceso judicial:

1. El perito debe conocer en profundidad el Derecho procesal (de todos y cada uno de los fueros en que participa), en especial si este Derecho procesal pertenece a un país cuya estructura federal lo hace diferente entre los distintos Estados o provincias que lo conforman y delimitan (caso de Argentina), ya que ignorar las normas podría implicar la anulación de la prueba en detrimento del sustento argumental que fuere (todo litigio judicial no es otra cosa que la discusión fundada de una pretensión, a efectos de convencer al juez sobre su validez y pertinencia).

2. El perito no debe opinar sobre el Derecho procesal; para el perito el Derecho procesal es un hecho al que debe acogerse y limitarse, ya que es el marco legal en el que debe desempeñarse. Sin embargo, puede hacerlo como ciudadano, pero en el ámbito que corresponda y por los medios democráticamente vigentes; si la ley no es buena, la solución no es transgredirla, sino modificarla o derogarla: *“Dura lex, sed lex”*. De ahí la necesidad de especificar claramente su rol dentro del tema en análisis (opinión ciudadana vs. opinión profesional, testimonio vs. testimonio experto).
3. Un perito en funciones no puede ni debe actuar como: juez, detective, cronista, “opinólogo”, difusor mediático, etc. Su función debe limitarse a actuar como testigo experto, limitando su tarea a los resultados fundados (científica, tecnológica y técnicamente) obtenidos a partir de la aplicación de las técnicas periciales de su especialidad sobre los indicios (testigos mudos) obrantes en un determinado lugar (lugar del hecho real o lugar del hecho virtual propio e impropio), que puede o no constituir una escena del crimen, ya que la tarea criminalística se ha expandido desde el Derecho penal a todos los fueros y a todos los ámbitos (empresarial, educativo, laboral, académico, familiar, etc.).

Coincidiendo con la doctrina establecida por los distintos tribunales de EE.UU., consideramos que resulta imposible generar una doctrina y una metodología, particularizadas y personalizadas, para cada tipo de soporte de información posible. El desarrollo científico, tecnológico y técnico, que nos inunda a diario, avanza en progresión geométrica; los mecanismos criminalísticos lo siguen en progresión aritmética, y el Derecho observa todo el proceso desde lejos, sin involucrarse demasiado, hasta que arrollado por la realidad, se ve obligado a adaptarse al cambio y adecuarse

a la realidad social en que se encuentra inmerso (firma digital, expediente digital, notificaciones digitales, entre otros temas), produciendo continuas adaptaciones legislativas, reglamentarias o simples acordadas que reducen un poco la distancia cada vez más extensa que separa a la tecnología de uso diario de las normas jurídicas que deberían regularla.

No es, por lo tanto, posible ni necesario crear un procedimiento para cada nueva tecnología que aparece en el mercado. De ahí que sostenemos con vehemencia que las bases sentadas en el *Manual de Informática Forense* deben ser sostenidas a ultranza, salvo que sean francamente incompatibles con la nueva tecnología analizada. La prueba documental informática y sus principios deben prevalecer. Los mecanismos de recolección, certificación, traslado, verificación y supervisión deben mantenerse en cuanto a sus principios básicos, agregando únicamente aquellos elementos propios de la nueva tecnología analizada que deban ajustarse para asegurar la preservación y confiabilidad de la documental informática recolectada.

En el campo de los procedimientos, ya no es posible aplicar uno solo a todos los casos posibles (*“one-size-fits-all”*), por el contrario, deben adecuarse los modelos a cada caso en particular, integrando las formas de recolectar y seleccionando el modo pertinente a cada situación planteada, pero respetando los principios criminalísticos, establecidos para el tratamiento de la prueba indiciaria informático forense y su especie la prueba documental informática. El investigador necesita libertad para seleccionar aquellas acciones puntuales que requiere para el caso en particular, pero siempre dentro del marco general del procedimiento válido. Este acto debe ser susceptible de revisión, debate y confrontación con la contraparte, para establecer su pertinencia y validez científica, criminalística e informático forense. El Tribunal debe analizar el problema planteado y decidir, acorde a su evaluación legal, si la