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

ERREPAR

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

1. 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
E-mail: clientes@errepar.com

ISBN: 978-987-01-1682-0

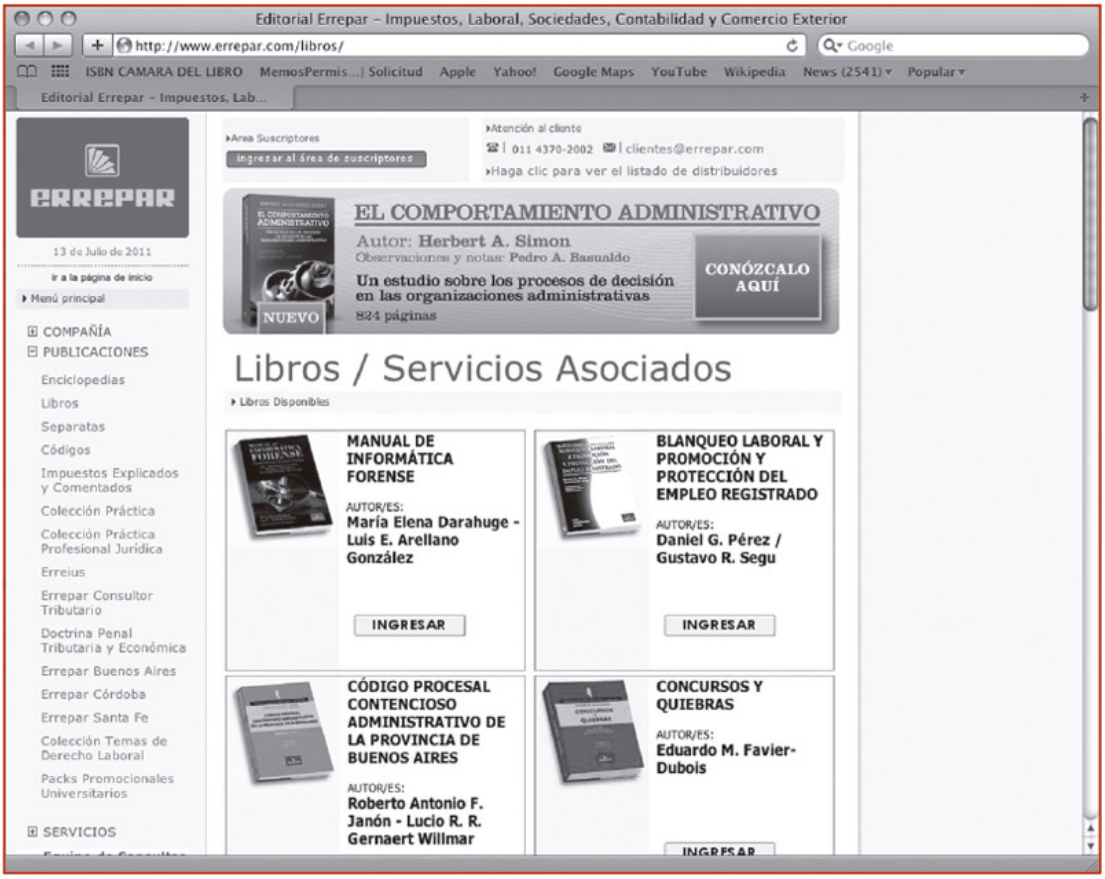
Nos interesan sus comentarios sobre la presente obra:
editorial@errepar.com

Digitalización: Proyecto451

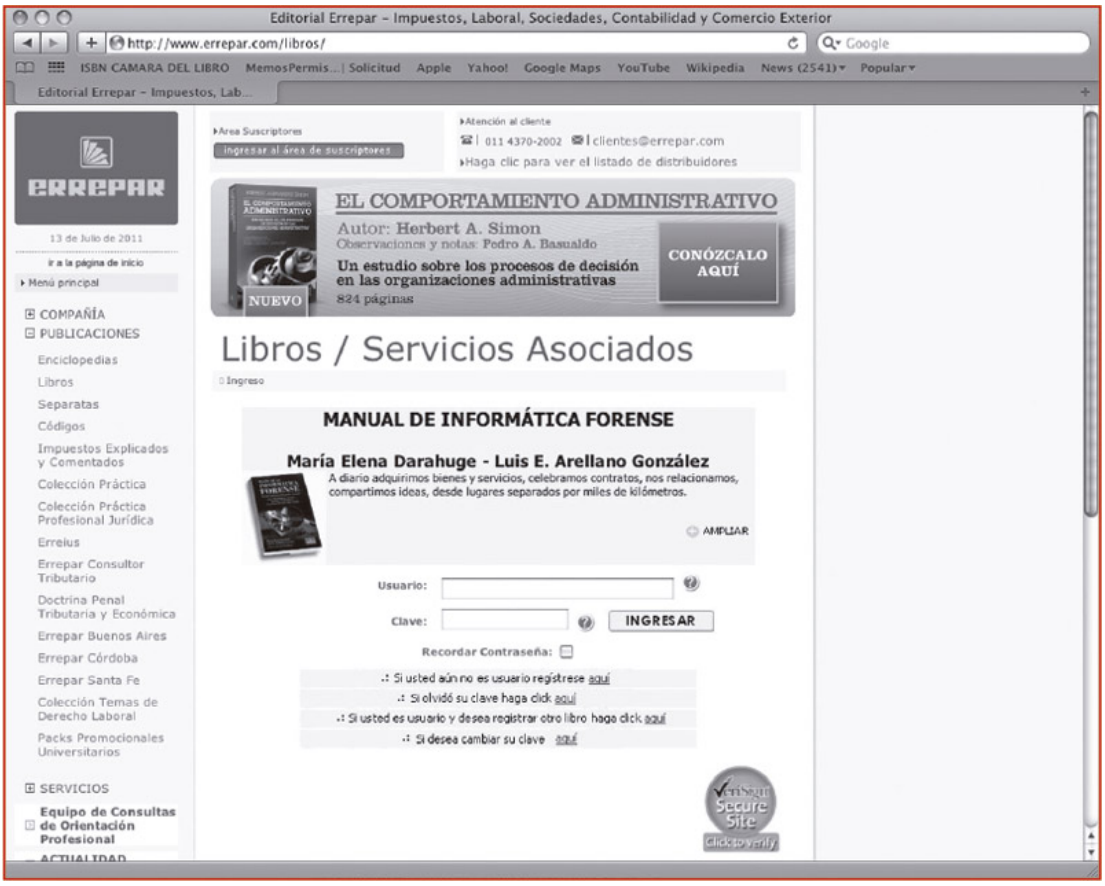
ACTUALIZACIÓN ON-LINE

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

Deberá ingresar a www.errepar.com/libros.



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



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

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