MANUAL DE INFORMÁTICA FORENSE III

(Prueba Indiciaria Informático Forense)

Gestión integral de la prueba documental informática para operadores del Derecho. Guía de ejercicios resueltos para peritos informáticos forenses (bajo licencia GNU)

INCLUYE ACTUALIZACIÓN ON-LINE

María Elena Darahuge
Luis E. Arellano González

Prólogo del Dr. Juan Pedro Hecht

ERREPAR

MARÍA ELENA DARAHUGE
LUIS E. ARELLANO GONZÁLEZ

MANUAL DE INFORMÁTICA FORENSE III

(PRUEBA INDICIARIA INFORMÁTICO FORENSE)

Gestión integral de la prueba documental informática para operadores del Derecho. Guía de ejercicios resueltos para peritos informáticos forenses (bajo licencia GNU)

Darahuge, María Elena
Manual de informática forense III / María Elena Darahuge ; Luis Enrique Arellano González. - 1a ed . - Ciudad Autónoma de Buenos Aires : Errepar, 2019.
Libro digital, PDF

Archivo Digital: online
ISBN 978-987-01-2431-3

1. Seguridad Informática. I. Arellano González, Luis Enrique. II. Título.
CDD 658.478

Manual de informática forense III

ERREPAR S.A.
Paraná 725 (1017) - Buenos Aires - República Argentina
Tel.: 4370-2002
Internet: www.errepar.com
E-mail: clientes@errepar.com

ISBN: 978-987-01-2431-3

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

Digitalización: Proyecto451

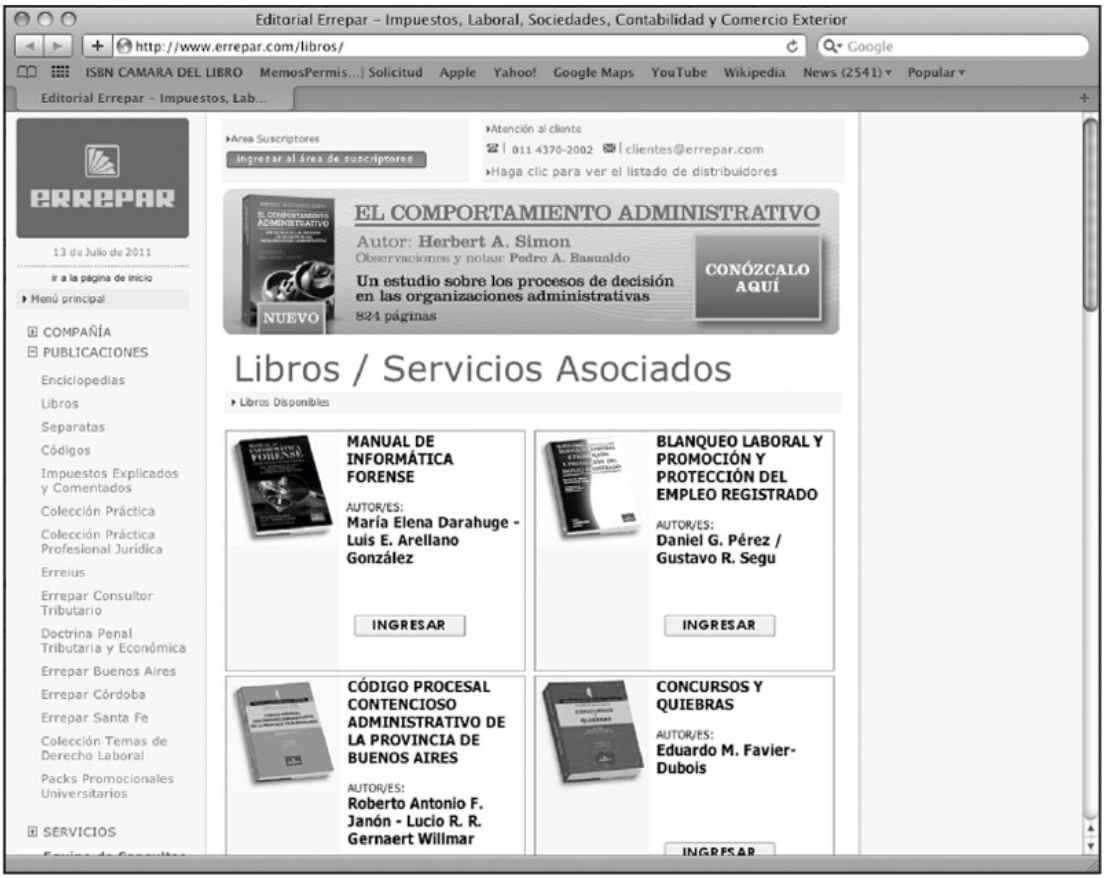
Índice de contenido

Anexo 11. Guía de recolección de información en Linux con el equipo encendido

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 acceso (22462691) y que complete una serie de datos personales.

Tenga presente que es muy importante ingresar 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 ícono 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.
Máster en Dirección Estratégica en Tecnologías de la Información, UEMC.
Especialista en Criptografía y Seguridad Teleinformática, Facultad del Ejército.
Postgrado en Ciencias Forenses.

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.
Especialista en Criptografía y Seguridad Teleinformática, Facultad del Ejército.
Postgrado en Ciencias Forenses.

PRÓLOGO

Pocas veces en la vida ocurren encuentros que nos dejan una impronta imborrable. Eso es lo que me ocurrió cuando en un Curso de Criptografía tuve el enorme placer de conocer a María Elena y a Luis Enrique. Un dúo que es una sólida unidad. Voy a aprovechar estas líneas para trazar una semblanza humana que por modestia ellos jamás escribirían.

Creo que fue una empatía mutua y que se fue acrecentando día a día con el diálogo y en ellos no hubo disciplina que no hayamos abordado. Así pasaron la biología, la mecánica celeste, la inteligencia artificial, los deportes, la criptología, la sociedad, los avances tecnológicos, el sentido del tiempo, la ética, la computación cuántica, el agnosticismo, la política, la cosmología, el arte y fundamentalmente lo que los filósofos alemanes llamaron *weltanschauung (1)*.

Así conocí a dos personas de cultura renacentista, inteligentes de absoluta integridad y coherencia, de fuertes convicciones y con esa elocuencia y precisión del lenguaje que sólo poseen los buenos docentes. No es que siempre hayamos coincidido, pero el hecho de habernos intercambiado ideas a mí en lo personal me ha enriquecido enormemente. La gran enseñanza fue entender que todos los días y en las formas más diversas, nos volvemos un poco menos ignorantes pero nunca sabios.

Escuchemos sus voces: hay que aprovechar nuestro tiempo que es un recurso escaso y con fecha de vencimiento. Sus citas lo plasman: "*Mors est non esse*" y "*Vive memor leti, fugit hora*". No hace falta que insista más

acerca de la idoneidad profesional, el acervo cultural, la superlativa capacidad intelectual que ambos poseen y la simpatía que despiertan en todos los que tengan la suerte de llegar a conocerlos. No tengo más que decir, me congratulo por haberlos conocido y que me consideren su amigo.

Por todo ello, sean bienvenidos. Invito a los lectores a disfrutar este libro.

Dr. Juan Pedro Hecht
Profesor Titular de Criptografía I/II y Coordinador Académico Maestría de Seguridad Informática (FCE - FCEyN - FI - UBA)
Especialización en Criptografía y Seguridad Teleinformática (EST - IUE)
Director Titular de EUDEBA

---

1. De difícil traducción, una postura de vida, cosmovisión, http://encyclopedia2.thefreedictionary.com/Weltanschaung

PREFACIO

La experiencia diaria como peritos de partes, consultores y/o asesores técnicos que enmarca nuestras tareas, desde el punto de vista del Derecho procesal considerado (según su respectiva jurisdicción y competencia), nos ha demostrado la existencia de una profunda laguna conceptual y procedimental en la gestión de la prueba documental informática, que constantemente aumenta en cantidad y calidad, lo cual constituye auténticos escollos en el análisis probatorio, por parte del Juez involucrado en la tarea.

Aunque la prueba documental informática solo difiere de su homóloga clásica en el soporte (papel vs. digital), deviene en un problema mayúsculo a la hora de realizar su gestión práctica y su implementación efectiva, eficiente y eficaz como prueba indiciaria relevante para el desarrollo del proceso judicial que la involucre.

En calidad de prueba indiciaria, debe demostrarse su utilidad como elemento necesario y suficiente para el desarrollo de la justificación argumental que pretende sostener una determinada pretensión controversial judicializada.

Por otra parte, debe soportar un procedimiento racional basado en particular en la lógica deóntica, propia del proceso judicial, que asegure que se trata de componentes conducentes y pertinentes a la temática controvertida. A esto debemos sumar que el marco general de encuadramiento de la prueba documental informática es estrictamente jurídico. Sin embargo, debe conformarse estrictamente dentro del método científico, utilizando una

metodología criminalística clara y precisa, a la que recién en esta etapa de su revisión metodológica se le puede integrar la tecnología y la técnica derivadas del diario desarrollo de la Informática.

Esta tarea no es simple porque requiere profesionales con formación transdisciplinaria, algo que no tiene nada de raro en otras disciplinas. Por ejemplo, en la Medicina legal donde un profesional luego de siete años de estudios para alcanzar el título de médico, y de dos años de residencia, y habiendo completado su especialización en Medicina general, Traumatología y Cirugía general, y con cinco años como mínimo de ejercicio de la profesión, puede acceder a un curso de dos años, en el que se lo capacitará en Derecho y Criminalística, y luego de presentar y aprobar un trabajo final, se le otorgará por fin el deseado y respetabilísimo título de médico legista.

Desde nuestra visión profesional, la Informática no tiene razón ni fundamento alguno para ser considerada una disciplina inferior en cualidad y complejidad a la Medicina. De hecho, en el *Manual de Informática Forense I* (editorial Errepar, Buenos Aires, 2011), afirmamos y desarrollamos el aserto: *“La Medicina legal es a la Medicina lo que la Informática forense a la Informática”*.

Por lo tanto, deberíamos encontrarnos con peritos en Informática forense que, como condición *sine qua non*, ostentaran títulos de grado universitario (en la forma de Licenciaturas o Ingeniería en Informática; no en otras profesiones similares, equivalentes o análogas), al que sumaran una formal y estricta capacitación en Derecho y, en especial, en Criminalística.

Esta afirmación no pasa de ser una simple y llana expresión de deseo. En el ambiente pericial informático forense, lo que se nota a diario es la improvisación. Las cosas se hacen según el leal saber y entender de aquel que se autodenomina experto o perito en Informática forense, sin otra validación académica ni profesional que el haberlo

expresado con vehemencia y convicción, ante un auditorio, en el mejor de los casos indiferente y, en el peor, absolutamente ignorante e impasible ante los profundos e irreversibles errores que tales supuestos expertos provocan en la gestión de la prueba documental informática.

Por supuesto, se olvida de manera tajante que el ser perito en Informática forense implica un servicio de apoyo a la decisión para un operador del Derecho y que de dicha decisión depende, sin lugar a dudas, el patrimonio o la libertad ambulatoria (ver Anexo 3: Glosario) de una persona.

Es frecuente en este particular espacio-tiempo que nos ha tocado ocupar, escuchar en boca de docentes y sus auxiliares, la manifestación, descripción y manipulación de prueba documental informática, casi siempre de manera inadecuada desde el punto de vista criminalístico, y frecuentemente ilegítima e ilegal.

La violación al derecho a la privacidad por parte de los supuestos “expertos o peritos informático forenses” parece haberse constituido en la norma dolosa y no en la excepción culposa o accidental, como parte de la práctica pericial, incluyendo la que se enseña en el aula, todo lo cual difunde, expande y disemina una actitud solapadamente delictiva, por parte del estudiante que desconoce el derecho involucrado, como si se tratara de normas con vigencia extraplanetaria y no de derecho vigente, real y obligatorio.

Si a esto sumamos la misma falta de capacitación formal inter y transdisciplinaria por parte de los operadores del Derecho (miembros y funcionarios del Poder Judicial o trabajadores que ejercen la profesión de manera independiente), en lo referente a la inserción de la Informática forense como especie del género Criminalística, llegando al extremo de que la materia Criminalística ni siquiera forma parte de la currícula obligatoria de la carrera de Abogacía de la Universidad de Buenos Aires (numéricamente la más importante de nuestro país), el resultado final puede resumirse en dos opciones principales:

una decisión judicial basada en conceptos, procedimientos y conclusiones erróneas que aumenta e incentiva la inseguridad jurídica que nos rodea (es decir, una decisión injusta, arbitraria y denigrante) o, en el mejor de los casos, cuando alguno de los actores del proceso se ha tomado el trabajo de ampliar su formación profesional criminalística, de manera voluntaria, a veces formal y a veces no, en una nulidad irreversible e insalvable que contradice absolutamente todo criterio de economía judicial vigente.

Se pierden cientos de horas hombre, páginas impresas y discusiones infructuosas e improductivas que inevitablemente terminan con la nulidad de la prueba indiciaria recolectada a los efectos probatorios, por inoperancia y soberbia de quienes tienen la responsabilidad de gestionarla científica, tecnológica, técnica y lógicamente.

El sentido de este texto reside en la necesidad evidente de evaluar los mecanismos utilizados para detectar, identificar, preservar, resguardar, trasladar, transferir y evaluar la prueba indiciaria informática recolectada en el lugar del hecho real o virtual (propio o impropio). Los resguardos deben cumplir con las reglas conceptuales, procedimentales y actitudinales, determinadas por las disciplinas mutuamente interactuantes: la Informática, la Criminalística y el Derecho vigente (en particular, el Derecho procesal).

En síntesis, pretendemos establecer un mecanismo coherente para la gestión integral de la prueba documental informática, como especie del género “prueba documental clásica”.

Este mecanismo requiere una descripción exhaustiva del procedimiento inter y transdisciplinario que asegure la confiabilidad de la prueba indiciaria informática recolectada, como elemento de apoyo a la decisión judicial legalmente obligatoria (sentencia).

La prueba indiciaria informático forense, desde lo legal, debe ser conducente y pertinente. Desde lo técnico-

demostrativo, necesaria y suficiente. Por supuesto, se nutre de su principal componente, la información, que también debe ser suficiente, pertinente y oportuna.

Lleva implícita la estructura que confiere sustento lógico a la cualidad pretendida: la confiabilidad de la prueba. Confiabilidad en el sentido de credibilidad y transparencia. Credibilidad como comprensibilidad y repetibilidad. Transparencia como trazabilidad y responsabilidad.

El marco teórico que proponemos se basa en la descripción exhaustiva conceptual y procedimental que asegure la confiabilidad de la prueba documental informática, como elemento de apoyo fiable a la sentencia.

En virtud de lo expresado, esta obra pretende conformarse en una descripción metódica, estricta y minuciosa del procedimiento propuesto, ya que la descripción de este puede efectuarse de manera completa y detallada.

Las variables involucradas confluyen al mismo desde el Derecho, la Criminalística y la Informática, cuya relación intrínseca respecto de la prueba indiciaria en general y de la prueba indiciaria informática son evidentes *per se.*

Por fin, y a pesar del poco tiempo de vigencia disciplinaria que exhibe la Informática forense, en razón de la antigüedad de las tres disciplinas involucradas en ella, es posible aplicarle criterios teóricos adecuados para el análisis de los datos ofrecidos.

En razón de nuestra formación profesional, dicha descripción se realizará de manera integradora entre las disciplinas: Derecho, Criminalística e Informática.

El presente trabajo no tiene antecedentes formales en la bibliografía de nuestro país. Ha sido desarrollado parcialmente por los autores en los *Manuales de Informática Forense I y II* (editorial Errepar, 2011-2012), pero nunca en forma integradora, con el objeto de efectuar un análisis detallado, meticuloso y progresivo sobre la problemática de

la gestión de la prueba documental informática, desde sus aspectos informático, criminalístico y legal.

Por tratarse de una prueba novedosa e intrínsecamente relacionada con la prueba pericial informático forense, resulta de sumo interés para su tratamiento judicial, actualmente en pleno desarrollo y evolución.

Algunos componentes del trabajo han sido evaluados con anterioridad, pero nunca en una obra que los integre con un objetivo único: lograr un protocolo tentativo de gestión de la prueba documental informática.

Este protocolo, una vez convalidado y refutado por otros expertos, pretende consolidarse como piedra fundamental en la gestión integral de la prueba documental informática; en tal sentido, es una obra inédita y precursora de posteriores desarrollos complementarios y suplementarios, conceptuales, procedimental y actitudinales.

Por tratarse de una obra descriptiva, se limitará a la integración de las visiones informática, criminalística y legal, en las cuales poseemos formación universitaria que respalda nuestra opinión profesional, y si bien somos conscientes de que tendrá falencias, pueden ser corregidas para alcanzar un instrumento eficiente, efectivo y eficaz, en apoyo de la gestión de la prueba documental informática y sus homólogas relacionadas (de informes y pericial informático forense).

Resumiendo: es imprescindible capacitar al perito o experto en Informática forense en el empleo práctico del método criminalístico. Este es el sentido del presente trabajo, ofrecer una forma de interactuar ante la prueba indiciaria informática, gestionar su producido: la prueba documental informática– y presentarlo en un informe pericial clásico, convincente y confiable, que reúna todas las condiciones que la Criminalística exige a los demás informes provenientes de otras disciplinas.

En tal sentido, es necesario hacer evidentes las analogías que existen entre la aplicación criminalística metódica a

otras disciplinas (por ejemplo, Balística, Documentología) respecto de las características propias de la prueba documental informática, generando tablas de comparación y evaluación ponderables numéricamente que permitan comunicar, compartir, interpretar y discutir los resultados obtenidos, desde valores mensurables y no desde la simple opinión cualitativa del experto considerado.

En este trabajo pretendemos dar el puntapié inicial en el sentido especificado y constituir la base de una futura normalización comparativa criminalística (2), que sea confiable en apoyo de la decisión judicial obligatoria (sentencia) que radica en manos del magistrado interventor.

---

2. En similitud con otras disciplinas criminalísticas, por ejemplo en Balística, determinar la identidad pericial de dos proyectiles (incriminado y testigo) implica coincidencia en los siguientes aspectos: mismo calibre, misma cantidad de estrías, misma orientación del estriado, mismo paso de estrías y (establecido mediante fotorrodado sistema Belaunde y Microscopía de comparación) doce puntos característicos igualmente situados, orientados y dirigidos. O, en Dactiloscopía: mismo dedo, misma mano, misma clasificación dactiloscópica (tipo fundamental), misma subclasificación dactiloscópica y doce puntos característicos, igualmente situados, orientados y dirigidos.

PRIMERA PARTE

REVISIÓN CONCEPTUAL Y PROCEDIMENTAL (criminalística, legal e informática)

CAPÍTULO 1

PRUEBA DOCUMENTAL INFORMÁTICA VS. PRUEBA INFORMÁTICA

“Probatio est demonstrationis veritas”

Considerando la estructura actual de un litigio judicial, es posible advertir la presencia de diversos componentes fundamentales para asegurar su pertinencia procesal y su desarrollo conforme a derecho. Simplificando la generalidad procesal, se puede decir que un litigio judicial sigue las siguientes etapas cronológicas:

1. Se produce un conflicto entre intereses contrapuestos. Estos intereses se pueden corresponder a dos personas (físicas y/o jurídicas) enfrentadas entre sí o al poder central respecto de uno de sus administrados (incluyendo el fuero penal y el administrativo).
2. Se intenta la resolución por medios no judiciales, en los ámbitos civil y comercial, por medio de métodos alternativos de resolución de conflictos y también mediante el remedio (a veces obligatorio) de la conciliación. Respecto del fuero administrativo, utilizando las herramientas propias y exorbitantes del poder punitivo directo que este representa (3). En cuanto al fuero penal, con el soporte de las organizaciones dedicadas a la prevención del delito, no solo de las Fuerzas de Seguridad y Policiales, sino también de las