La validez jurídica de los indicios digitales

The legal validity of digital evidence

Publicación: 20 de julio de 2024
Recibimiento: 30 de mayo de 2024
Aceptación: 29 de junio de 2024

https://doi.org/10.18537.iuris.19.02.08

Miguel Ángel Álvarez Martínez[1]
http://orcid.org/0009-0001-7428-0469
inacifo1@yahoo.com.mx

[1] Instituto Nacional de Ciencias Forenses, S.C.

Resumen

El presente trabajo induce al lector al conocimiento del cuidado y preservación de lo que se ha dado en llamar "indicio digital", en la inteligencia de que un documento electrónico o cualquier elemento que pueda ser considerado un medio de prueba, que haya sigo generado a través de cualquier tecnología de la información, deberá tener un tratamiento especializado que obliga a tener tanto un conocimiento avanzado de la informática como a su vez una formación sólida en criminalística y derecho, a fin de que su preservación sea no solo basada en la técnica informática sino a su vez, cumpla con los cánones que exige la propia ciencia forense en tanto que su validez, como en el caso de cualquier otro indicio físico, depende del cuidado con el que se rastrea, fija, levanta y embala correctamente, se identifica y se transporta a efecto de poder ser revisado en cualquier otro momento, conservando sus características originales y asegurándonos de que al momento de elaborar el peritaje correspondiente, bajo ninguna circunstancia se altere ni su contenido ni la información adicional que conoceremos como metadatos y que se hace indispensable para explicar un indicio digital, a fin de una prueba pericial, de donde depende completamente que el juez valide la prueba y adopte en realidad el peso probatorio para el que se ofrece.

Palabras clave: Indicio digital, prueba, metadatos, forense

Abstract

This work induces the reader to learn about the care and preservation of what has been called "digital evidence", in the understanding that an electronic document or any element that can be considered a means of proof, which has been generated through any information technology, must have a specialized treatment

ISSN: 2602-8425

that requires having both an advanced knowledge of computer science and at the same time a solid training in criminology and law, so that its preservation is not only based on computer technique but at the same time, complies with the canons required by forensic science itself, since its validity, as in the case of any other physical evidence, depends on the care with which it is tracked, fixed, lifted and packed correctly, identified and transported in order to be able to be reviewed at any other time, preserving its original characteristics and ensuring that at the time of preparing the corresponding expert report, under no circumstances is its content or the additional information that we will know as metadata and that is essential to explain a digital clue altered, for the purpose of expert evidence, on which the judge's validation of the digital evidence completely depends. test and actually carry the evidentiary weight for which it is offered.

Keywords: Digital evidence, proves, metadata, forensic

Introducción

El mundo de las tecnologías de la información ha penetrado de manera profunda en todos los aspectos de la humanidad, facilitando la vida diaria. Sin embargo, como es inherente a la naturaleza humana, algunas personas han pervertido estas tecnologías para su beneficio personal, perjudicando la seguridad o el patrimonio de otros y actuando de manera antisocial. En otros ámbitos del derecho, donde todo se ha digitalizado, existen documentos que ahora, en su versión electrónica, deben ser conocidos y validados. Estos documentos, originados en sistemas informáticos, requieren la intervención de un experto forense para realizar una especie de criminalística moderna. Este experto debe recuperar de manera confiable los recursos que el abogado considera como pruebas, asegurándose de que se presenten intactos, originales y en sus versiones tanto físicas como digitales.

De tal manera que se hace relevante comprender el origen mismo de los indicios llamados "digitales" y su naturaleza, a fin de que el abogado que arribe a utilizar este tipo de pruebas, tenga siempre presente no solo su ofrecimiento en físico impreso, sino aún más importante, la recuperación del indicio digital desde el equipo de cómputo que originalmente lo haya generado, sin perder de vista que en esta categoría, prácticamente entran todos los equipos que cuenten con un procesador matemático, memoria RAM y medios de almacenamiento, como son los teléfonos celulares, las *tablets*, *laptops* y todo aquel instrumento o aparato que cuente con las características técnicas antes descritas y que genere algún tipo de archivo que haya que ubicar y recuperar de una manera doctrinalmente forense.

En México, pocos ordenamientos legales exigen explícitamente la preservación de indicios digitales mediante la intervención de un perito experto que

garantice la originalidad del documento. Sin embargo, en el sistema acusatorio implementado en el país, es obligatoria la cadena de custodia. Esta no solo abarca el control administrativo de quienes manejan los indicios relacionados con el litigio, sino también los procesos y procedimientos necesarios para asegurar, preservar y conservar dichos indicios, independientemente de su origen. Por supuesto, esto incluye los indicios digitales.

Estos procedimientos deberán estar a cargo de un perito cuya idoneidad se sustente no solo en sus conocimientos de informática, criminalística y derecho, sino también en la suficiente práctica que lo convierta en un auténtico experto capaz de realizar este trabajo con la pericia requerida. Por tanto, la validez de estos indicios depende de la disciplina con la que se hayan fijado, recuperado, embalado y conservado según los cánones de la informática forense y la criminalística, así como de los métodos y la doctrina empleados en el peritaje y el dictamen que servirá como prueba pericial.

En el presente documento se explicará, desde una perspectiva pericial y con un enfoque jurídico, las formas correctas en que abogados y peritos deben trabajar en equipo para garantizar que los archivos digitales cuenten con la validez jurídica necesaria y que el dictamen pericial tenga un valor probatorio indiscutible.

La validez jurídica de los indicios digitales

Un indicio digital recibe este nombre porque es el resultado de un procesamiento a través de un sistema informático que convierte cualquier medio en una copia traducida a un lenguaje binario de unos y ceros dentro de la computadora. Es decir, los sistemas informáticos, en su funcionamiento más profundo, interpretan todo a través de pulsos electromagnéticos que podemos entender como positivos (1) y negativos (0). Este arreglo binario conforma todo lo que se genera en su interior.

Con esta explicación, podemos deducir que, al depender de pulsos electromagnéticos, la preservación de los indicios digitales es más compleja que la de cualquier otro indicio de carácter físico. Esto se debe a que los indicios digitales pueden cambiar su naturaleza a través de un programa informático o por la variación de voltajes, lo que podría afectar sensiblemente su contenido o disponibilidad, llegando incluso a inhabilitarlos. Hay que recordar que un "indicio" es cualquier objeto que puede ser sensible o proclive a cambios o modificaciones y que resulta significativo para la construcción de una teoría del caso. Por esta razón, es indispensable y obligatorio que cualquier indicio se conserve con su originalidad, tal y como fue generado.

En los indicios digitales, no solo son importantes las características aparentes que se perciben a simple vista, como una imagen o un audio, sino también los

ISSN: 2602-8425

datos de identidad del archivo y del equipo o sistema que lo generó, así como la fecha, hora y lugar de creación. Esta información, conocida como "metadatos", complementa ese "mundo del pequeño detalle" en el que trabajan los forenses y justifica la existencia de un área pericial en informática.

Dado que un indicio, por definición, es susceptible a sufrir alteraciones, los indicios digitales, al ser intangibles y generados por fuerzas electromagnéticas, son doblemente frágiles. En un mundo donde todo se "virtualiza", una alteración dolosa podría pasar desapercibida para ojos inexpertos, y en algunos casos, representar un reto demostrar la alteración fraudulenta, especialmente si estas modificaciones se realizan a nivel binario. Esto puede dificultar la identificación del archivo original.

Así como en las ciencias forenses existen diversos tipos de indicios según su origen, en la informática también hay diversos tipos de archivos digitales según el programa, aparato o instrumento que los genere. Encontramos indicios generados por suites de ofimática, *software* diseñado para funciones específicas, *software* especializado en áreas profesionales, aplicaciones de redes sociales, y medios de telecomunicaciones. Además, hay archivos genéricos, como imágenes, videos (videogramas) y audios (audiogramas), en diversos formatos de compresión y con distintas calidades o definiciones.

Todos los indicios digitales descritos, en su forma más primigenia, son en realidad un arreglo de ceros y unos, organizados en un esquema de lenguaje binario. Dentro del medio de almacenamiento del sistema computacional, no se distinguirían características visibles como tipos de letra, píxeles o formatos, sino únicamente *bytes* (arreglos binarios) en diversas combinaciones según el tipo de archivo. En última instancia, se trata de pulsos electromagnéticos que, para ser analizados más allá de lo superficialmente evidente, requieren un conocimiento avanzado en informática y en técnicas forenses. Este conocimiento es crucial para obtener la máxima cantidad de información posible de cada indicio.

Como hemos visto, el tipo de archivo electrónico y el equipo que lo genera determinan su origen. Por ello, para conservar la versión más original de cada archivo, es fundamental rastrear los indicios directamente del equipo que los generó y preservar el archivo exactamente como se ofreció en el juicio o en la carpeta de investigación.

Por ejemplo, si el indicio digital es una conversación realizada a través de la aplicación *WhatsApp*, aunque se visualice como texto plano acompañado de imágenes, videos o audios, la aplicación tiene una función para recuperar y preservar esas conversaciones. Esto puede hacerse archivando la conversación o enviándola por correo electrónico. Sin embargo, al transferirla, el texto en pantalla se convierte en un archivo de texto sin formato, conocido como "nota", que puede ser fácilmente editado.

Por lo tanto, una de las cualidades esenciales del perito en informática, como en cualquier área pericial, es la probidad en su actuación. Esto garantiza que el respaldo se realice exactamente como se genera, preservando y realizando una transcripción estenográfica (textual) precisa. Una simple captura de pantalla de la conversación no es suficiente para constituir una prueba. Es necesario seguir todo el procedimiento forense de recuperación, descripción y preservación para asegurar que el archivo de la conversación sea auténtico. Además, es importante tener en cuenta que la empresa *WhatsApp* asegura que las conversaciones se encriptan (codifican) y, por tanto, son seguras, lo que añade una capa adicional de complejidad a la recuperación de pruebas.

Algo similar ocurre con las conversaciones realizadas a través de sitios o aplicaciones de redes sociales, como *Messenger* de la empresa *Facebook*. Estas aplicaciones permiten la mensajería por textos y la inclusión de archivos multimedia, y requieren recursos de Internet para facilitar la comunicación. Además, estos servicios generan metadatos que pueden proporcionar información valiosa, como la ubicación geográfica o la georreferenciación a través de la dirección IP (Internet Protocol).

La dirección IP es un número único asignado a cada dispositivo conectado a la red, y es parte de un protocolo de comunicación que gestiona la retransmisión de señales a través de la infraestructura de Internet. Hoy en día, prácticamente todos los dispositivos portátiles generan datos que se transmiten a través de Internet, ya sea para alimentar redes sociales o para utilizar servicios de comunicación como el correo electrónico. Por lo tanto, cada archivo generado lleva consigo información técnica que ayuda a identificar el archivo para su envío y destino, así como a los usuarios involucrados. Gracias a las antenas y satélites que permiten estas comunicaciones, es posible localizar los domicilios de los participantes con cada vez mayor precisión.

De otro modo, sería prácticamente imposible que esos archivos pudieran ser enviados desde los dispositivos que los generan hacia otros destinos. Incluso las llamadas telefónicas, que antes viajaban por señales analógicas, ahora se transmiten de manera digital a través de la tecnología de "Voz sobre IP" (Voz IP). Esto convierte a Internet en un complejo sistema de carreteras digitales donde cada paquete de datos está claramente identificado, permitiendo determinar tanto el remitente como el destinatario.

Sin embargo, cuando los archivos se transfieren de un dispositivo a otro durante la socialización de información, se pierde la IP original, junto con datos esenciales como la fecha, hora y usuario original. En algunos casos, dependiendo del dispositivo y su configuración, también se puede perder información específica del aparato que generó el archivo.

La telefonía, que depende de una red de antenas, retransmisores y satélites para llegar a cualquier rincón del mundo, deja rastros en la infraestructura que permiten el seguimiento y la georreferenciación. Los sistemas GPS (Sistema de

ISSN: 2602-8425

Posicionamiento Global), cada vez más precisos, reducen el margen de error en la identificación de ubicaciones. Esta infraestructura de telecomunicaciones ofrece una oportunidad técnica para ubicar con mayor exactitud los archivos digitales generados por dispositivos móviles o fijos, asegurando que, al enviar un documento, llegue a su destino correctamente y que el sistema pueda identificar al remitente para fines de seguridad informática.

Esta es otra razón poderosa para exigir que los documentos sean peritados en sus aplicaciones originales y que se trabajen con los archivos digitales originales. De no hacerlo, estaríamos tratando con documentos que, aunque parecidos, no son originales y podrían narrar una historia diferente a la real, tal como lo sugieren los metadatos.

Por ejemplo, en el caso de los videogramas utilizados para vigilancia, ya sea por sistemas de los Centros de Comando, Control y Computo (C4) de las áreas de seguridad pública en México, o por sistemas de videovigilancia mediante circuitos cerrados (DVR) o *webcams*, la información sobre el lugar, el día y la hora es crucial para la conformación de una teoría del caso. La definición del video y la claridad del audio que pueda acompañar también son determinantes. En este contexto, es esencial seguir procedimientos forenses adecuados para recuperar y validar estos videos.

La necesidad de asegurar la autenticidad de los archivos digitales se vuelve aún más crítica debido a la sofisticación de las tecnologías actuales y la presencia de inteligencia artificial, que puede alterar archivos de manera casi imperceptible al ojo humano. Solo con tecnologías avanzadas se puede detectar la falsificación del archivo original. Por lo tanto, el perito debe garantizar que el video, imagen o audio recuperado y preservado sea la versión original.

En cuanto a la "vulnerabilidad" de los archivos digitales, su formato influye en su susceptibilidad a alteraciones. Por ejemplo, un archivo de audio es más difícil de alterar que un archivo de texto simple (.txt), que puede ser modificado fácilmente con aplicaciones básicas como el Bloc de notas. Esta diferencia en la vulnerabilidad destaca la importancia de aplicar procedimientos forenses rigurosos para asegurar la integridad de los archivos digitales.

Con base en la experiencia, los reportes de asistencia generados por sistemas biométricos son herramientas clave para los abogados laboristas al demostrar la relación laboral con una empresa o institución, el tiempo trabajado y la asistencia física a un lugar de trabajo. Dado que estos documentos son altamente vulnerables a alteraciones, es crucial preservar el archivo directamente desde el equipo biométrico de manera pronta y eficaz. Esto ayuda a evitar que el archivo sea modificado fraudulentamente en otros equipos.

En cuanto a la seguridad de la información, las aplicaciones móviles de los bancos han convertido en un problema significativo para los cuentahabientes. A menudo, estas aplicaciones presentan vulnerabilidades que permiten

a los ladrones cibernéticos acceder a información sensible y realizar fraudes económicos. A pesar de las técnicas de "ingeniería social" utilizadas por los delincuentes para obtener información de los usuarios, los bancos aún no han implementado procedimientos efectivos para detectar movimientos inusuales o comportamientos sospechosos en las cuentas.

En México, por ejemplo, no existe una obligación establecida para monitorear las direcciones IP desde donde se originan las transacciones. Esto significa que, si una compra se realiza en Tijuana y, en cuestión de minutos, se hace otra transacción desde Chiapas, no se activa una alerta automática para suspender la cuenta y verificar con el usuario. A pesar de que es físicamente imposible realizar tales transacciones simultáneas desde extremos opuestos del país, los ladrones digitales pueden explotar esta falta de control, a menudo con la ayuda de personal interno del banco. Esto subraya la necesidad urgente de que las instituciones financieras desarrollen procedimientos más robustos para proteger a los cuentahabientes y prevenir fraudes.

La revisión de las bitácoras de movimiento de cuentas bancarias resulta insuficiente si no se acompaña con información adicional relacionada con los procesos internos y externos de los movimientos desde el sistema. Para una validación completa, los peritos deben tener acceso a los niveles de seguridad, usuarios y conexiones asociadas con dichos movimientos. Sin embargo, esta información a menudo no está disponible en la contestación de la demanda debido al temor de filtrar datos que comprometan el secreto bancario.

En la práctica, durante las diligencias periciales en las oficinas bancarias, los peritos a menudo encuentran que la bitácora impresa proporcionada para la prueba no siempre refleja la información original de los servidores. En muchos casos, el personal no especializado prepara y presenta una versión aislada y manipulada de los datos, lo que no cumple con los estándares forenses. Esta actividad no es pericial y debería ser evitada, ya que solo los peritos debidamente capacitados están facultados para manejar y recuperar los indicios de manera directa, garantizando así la autenticidad de la prueba.

La búsqueda y conformación de las bitácoras de movimiento en las cuentas de los cuentahabientes afectados debería ser una práctica aceptada y comprendida por los bancos como un procedimiento esencial para validar la existencia y el *modus operandi* de los robos. Los bancos deberían ajustar sus políticas para permitir una mayor transparencia y supervisión, enfocándose en la detección de actividades inusuales para activar mecanismos de verificación antes de que las cuentas sufran daños indebidos.

Otro indicio comúnmente utilizado en juicios para periciales son las llamadas telefónicas o las "sábanas de llamadas". Como se mencionó anteriormente, estos registros de "voz IP" son susceptibles de rastreo y análisis detallado. Sin embargo, incluso en el caso de la telefonía celular convencional, la infraestructura de antenas y satélites permite identificar la ubicación de un teléfono

ISSN: 2602-8425

móvil en tiempo real, incluso si el dispositivo solo está encendido y con datos activados, sin necesidad de realizar una llamada.

Los correos electrónicos, por otro lado, requieren una atención especial. La tecnología de correo electrónico depende de una serie de sistemas en la Internet para el envío y recepción de mensajes y sus adjuntos. Aunque es común que los abogados impriman correos electrónicos como si fueran documentos físicos, a menudo omiten las cadenas de servidor que aparecen en la parte inferior del mensaje impreso. Estas cadenas y cabeceras son cruciales para verificar la autenticidad del correo electrónico y requieren de un análisis pericial para ser correctamente evidenciadas.

Para validar una impresión en papel de un correo electrónico, es esencial obtener el correo directamente desde la cuenta del usuario. Esto implica cotejar el mensaje original en el servidor de correo electrónico del remitente o del receptor, describir detalladamente el dominio del servicio de correo (como *Yahoo*, *Google*, o un dominio privado), identificar a los usuarios que intercambiaron los mensajes y proporcionar la información técnica que demuestra el trayecto del correo electrónico desde su origen hasta su destino. Este procedimiento asegura la integridad del correo electrónico como prueba pericial y confirma su autenticidad en el contexto judicial.

Es fundamental que la información de los correos electrónicos se obtenga y verifique directamente desde el sistema en línea. Durante una diligencia pericial para acceder a una cuenta de correo, es esencial que el propietario de la cuenta esté presente, ingrese con su contraseña y participe en la búsqueda del mensaje para evitar cualquier vulneración de su privacidad. Es una norma de cortesía profesional que el perito conduzca la búsqueda, mientras que el usuario maneja su propio correo electrónico.

En caso de encontrar el documento relevante para la *litis* o la prueba, el perito debe intervenir para preservar el mensaje y sus archivos adjuntos. Esto se realiza utilizando un medio de almacenamiento digital, el cual se incluirá como anexo al dictamen y se embalará adecuadamente, garantizando así la integridad de la evidencia.

Por último, en relación con las páginas de internet, es importante mencionar que sus nombres se registran bajo el concepto de "dominio". El dominio es un distintivo legal reservado al propietario que lo ha adquirido, sirviendo como identificación única para su marca o nombre en la red.

A partir de lo anterior, es evidente que dos personas físicas o morales podrían, en teoría, registrar el mismo nombre de dominio. Sin embargo, esto puede llevar a problemas de propiedad intelectual y fraude, ya que el uso no autorizado de un dominio registrado infringe los derechos de propiedad y puede llevar a engaños, suplantación de identidad y otros delitos.

El concepto de dominio en internet se convierte en una extensión de la identidad jurídica, ya que las páginas web y redes sociales, aunque gestionadas por seres humanos con derechos civiles, representan a entidades que tienen una identidad propia en el entorno digital. Esto implica que la protección de estos dominios y la prevención de su uso indebido son cruciales para mantener la integridad y la confianza en la red.

Este entendimiento es vital para evitar caer en engaños perpetrados a través de sitios web fraudulentos. Las tácticas como el *phishing*, donde se crean páginas falsas para obtener información confidencial, son comunes. Los usuarios pueden ser inducidos a proporcionar información sensible, como datos personales y técnicos del *Wifi*, o incluso su dirección IP, lo que puede comprometer gravemente su seguridad.

Por lo tanto, es esencial estar alerta ante páginas que aparentan ser legítimas pero que tienen la intención de engañar. La protección de nuestra identidad y datos en línea requiere una comprensión adecuada de cómo funcionan los dominios y la seguridad en internet, así como la adopción de medidas proactivas para evitar vulneraciones.

Conclusiones

En el mundo digital, donde la información es vulnerable a manipulaciones y fraudes, es crucial seguir rigurosamente los procedimientos de informática forense para asegurar la validez de los indicios electrónicos. Los expertos forenses, con su experiencia y conocimientos especializados, son esenciales para rastrear, recuperar y preservar estos medios de prueba con integridad.

Para garantizar la correcta intervención del perito, es recomendable que los abogados involucren a un experto desde el inicio del proceso de preparación de pruebas. Esto asegura que el perito no solo conozca previamente el caso, sino que también colabore estrechamente con los abogados en la preparación del cuestionario y en la coordinación para el desahogo de la prueba. De esta manera, se maximiza la validez y efectividad de las pruebas digitales presentadas en juicio.

Porque la Justicia no es virtual, debemos preservar y proteger los indicios digitales con el mayor rigor.

Referencias bibliográficas

Andrés, G. (2005). *Delitos informáticos en la legislación mexicana*. CdMx: Editorial Instituto Nacional de Ciencias Penales.

Avalos, R. (2015). *Técnicas de investigación forense*. CdMx: Editorial Trillas.

ISSN: 2602-8425

Burgos, A. (2010). *Seguridad PC desde cero, proteja su PC contra todas las amenazas de la Web*. Buenos Aires: Editorial Fox Andina.

Cano, J. (2013). *Inseguridad de la información, una visión estratégica*. Bogotá: Editorial Alfaomega.

Díaz, A. (2008). *Proceso penal acusatorio y teoría del delito*. CdMx: Editorial Straf.*

Espinosa, E. (2016). Código Nacional de Procedimientos Penales, Comentado y correlacionado. Jalisco: Ediciones Gallardo.

Flores, I. (2012). *Criminalidad informática. Aspectos sustantivos y procesales*. CdMx: Editorial Tirant lo Blanch Monografías.

González, J. (1984). *El porvenir de la razón en la era digital*. Madrid: Editorial Síntesis.

González, J. (2015). *Lecciones de la prueba pericial en el sistema acusatorio adversarial*. CdMx: Editorial Flores.

Gratton, P. (1998). *Protección informática en datos y programas, en gestión y operación, en equipos y redes, en Internet*. CdMx: Editorial Trillas.

Lázaro, F. (2013). *Introducción a la Informática Forense*. Madrid: Editorial Ra-Ma.

Lázaro, F. (2014). *Investigación forense de dispositivos móviles Android*. Madrid: Editorial Ra-Ma.

Lira, M. (2010). *Cibercriminalidad, Fundamentos de investigación en México*. CdMx: Editorial Instituto Nacional de Ciencias Penales.

Morales, J. (2015). *Teoría General del Delito Informático*. México: Editorial Impresiones Huella.

Montiel, J. (2008). *Criminalística*. 1, 2ª Edición. CdMx: Editorial Limusa.

Moreno, L. (1979). *Manual de introducción a la criminalística*. CdMx: Editorial Porrúa.

Moreno, L. (2021). *Los últimos avances de la criminalística en la administración de justicia*. CdMx: Editorial Instituto Nacional de Ciencias Penales.

Nava, A. (2013). *El Derecho en la Era Digital*. CdMx: Editorial Porrúa.

O´dea, M. (2003). *Claves Hackers en Windows*. Madrid: Editorial Mc Graw Hill.

Peña, J. (2021). *La prueba pericial criminalística: Particularidades en Ecuador*. Cuenca: Editorial Ucuenca Press.

Rodao, J. (2002). *Piratas Cibernéticos, Ciberwars, Seguridad Informática e Internet*. CdMx: Editorial Alfaomega.

Téllez, J. (1996). *Derecho Informático*. CdMx: Editorial Mc Graw Hill.

Vite, H. (2016). *Informática Forense Protocolo de Actuación*. CdMx: Editorial Flores.

Zonderman, J. (1993). *Laboratorio de Criminalística*. CdMx: Editorial Limusa.

Zoon, I. (2006). *Cibercriminalidad*. CdMx: Editorial Instituto Nacional de Ciencias Forenses.

Declaración de conflicto de interés

El autor declara que no existe conflicto de interés.