El Mensaje de Datos como Evidencia Digital en Colombia

Espinel, Carlos. Bolaños, David
carlos.espinel@proelectrica.com, dafer_tlm@hotmail.com
Universidad Piloto de Colombia

Resumen—El objetivo de este documento es describir los requisitos técnicos y legales que deben cumplir los archivos catalogados como mensajes de datos, para ser aceptados como evidencia valida en un proceso administrativo, disciplinario o judicial en el contexto colombiano. Para esto se tuvieron en cuenta diversos conceptos de los ámbitos legal y pericial.

Índice de Términos—datos, digital, evidencia, mensajes, prueba.

I. Introducción

No es un secreto para los profesionales que se desempeñan en el campo de la seguridad de la información el creciente incremento de los delitos informáticos cometidos en el mundo actual. El hecho de que las personas ahora pasen la mayor parte de su tiempo en el universo digital, ha convertido a los medios informáticos tanto en objetivos como en herramientas apetecidas por los delincuentes para ejecución de conductas ilegales.

Del mismo modo, en muchos de los procesos judiciales y disciplinarios que se adelantan hoy en día, se ve un aumento de la presencia de información contenida en medios digitales como evidencia clave para el desarrollo de estos casos. Una evidencia digital, puede encontrarse en cualquier información que haya sido generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como correos electrónicos, mensajes de texto, videos, grabaciones digitales, unidades de almacenamiento, sitios web, entre otros. [1]

II. Evidencias Digitales

La informática forense dentro de sus objetivos cuenta con técnicas especializadas para ubicar, reproducir y analizar evidencias digitales que le permiten al perito o investigador obtener datos relacionados con rastros de procesos o hechos que pudieron haber sido llevados a cabo en la escena del delito informático. Pero para entender mejor éste tema e ir más a profundidad en el conocimiento, lo principal es saber exactamente que es o de qué se trata una evidencia digital, que se define como: “cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático” [2]. En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal" [3].

Por lo tanto, cuando hablamos de evidencia digital nos podemos referir a cualquier documento, carpeta, registro o dato contenido en un soporte informático que es susceptible de tratamiento digital.

Teniendo en cuenta que existen diversos tipos de evidencia digital ésta es clasificada en diferentes categorías tales como:

- Datos o información que han sido almacenados en un equipo o dispositivo tecnológico, dentro de los cuales se contemplan correos electrónicos, imágenes o archivos en otros formatos.

- Información o registros de datos que genera un equipo informático por medio de diferentes procesos, tales como logs de auditoria, sucesos del sistema, rastreo de transacciones o consultas a bases de datos, errores de aplicaciones o componentes del sistema operativo, etc.

- Datos o archivos que han sido parcialmente generados y almacenados en un dispositivo o equipo informático, en este caso hablamos también de archivos ofimáticos como hojas de cálculo o archivos de texto, consultas realizadas a bases de datos, pero que tienen su origen en el equipo informático usado inicialmente.

Como se puede ver, la evidencia digital es la base principal para los investigadores, porque la examinación y análisis detallado de la misma es parte fundamental del proceso de investigación en caso de un presunto delito informático. Sin embargo, así como tiene sus propiedades o características, también cuenta con vulnerabilidades que son a las que se enfrenta un investigador o perito informático, ya que por el constante cambio que se ve reflejado día tras día en el mundo de la tecnología, la evidencia digital puede ser trasladada de un lugar a otro fácilmente por su nivel de volatilidad. Dicha evidencia también puede tener origen de autoría anónima, existiendo un original sin las propiedades de seguridad de copia, que puede ser vulnerable a la duplicidad de la misma y por ende es altamente modificable, alterable y en el peor de los casos puede ser eliminada.

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada en una escena del delito. Por lo tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

III. VALIDEZ JURÍDICA

Aunque las transacciones globales de comercio electrónico tuvieron un aumento del 162% durante los primeros meses del 2013 con respecto al año anterior [4], la mayoría de las personas aún desconocen el valor probatorio que posee la información que intercambian electrónicamente durante esas transacciones, y que esta adquiere obligaciones y derechos de cumplimiento con efectos jurídicos.

A partir de la Ley 527 de 1999, el mensaje de datos se convierte entonces en un instrumento jurídico que soporta las transacciones electrónicas con efectos legales. Esta legislación de carácter comercial, da a los mensajes de datos un reconocimiento jurídico a través del principio de *equivalencia funcional*, el cual tiene como objetivo determinar que en el ordenamiento jurídico colombiano, los actos y contratos del mundo digital tienen los mismos efectos jurídicos vinculantes que los actos tradicionales realizados en papel.

La Ley 527 también describe los requisitos jurídicos que debe tener el mensaje de datos para satisfacer la aplicación de una norma, estos son:

- *Escrito:* la información contenida en el mensaje de datos se puede acceder posteriormente para consulta.

- *Firmado:* se ha utilizado un método que permita identificar quien inició un mensaje de datos y para indicar que el contenido cuenta con su aprobación. Además este método debe ser tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado. Las firmas electrónicas pueden ser *simples* (usuario, contraseña, rubrica, etc.), *biométricas* (retina, huella, etc.) o *digitales* (llave privada, entidad certificadora, etc.). La

elección del mecanismo de firma a utilizar debe basarse en un análisis de riesgos según el proceso que se quiera autenticar.

- *Original:* Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva como mensaje. En el marco de esta la Ley 527, la integridad a la que hace referencia, aplica cuando la información contenida en el mensaje de datos ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación, como por ejemplo: la inserción de las direcciones IP de los servidores por donde pasa un correo electrónico en el encabezado de un mensaje, antes de llegar a su destinatario, no invalida la integridad del mensaje en el contexto de esta ley.

Por otra parte, la Ley 527 también menciona los aspectos a tener en cuenta al momento de presentar una evidencia digital en un proceso, refiriéndose a la *Admisibilidad y fuerza probatoria de los mensajes de datos, dice:* "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original". [5]

En resumen, para que en Colombia un mensaje de datos tenga valor probatorio debe asegurarse: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje; la confiabilidad en la forma en que se haya conservado la integridad de la información, y la confiabilidad en la forma en la que se identifique a su iniciador y cualquier otro factor pertinente [6].

IV. PROCEDIMIENTO FORENSE PARA LA PRESENTACIÓN DE MENSAJES DE DATOS COMO EVIDENCIA DIGITAL

Además de haber validado las características admisibles de un mensaje de datos desde el punto de vista legal, el análisis de esta información también debe realizarse en el marco de otros requisitos desde la perspectiva forense, cuyo objetivo es la recogida segura de datos de diferentes medios y evidencias digitales, sin alterar los datos de origen con el fin de establecer la relación entre un delito y su autor [7].

Con el fin de garantizar su validez probatoria, los peritos forenses deben asegurarse que la metodología utilizada en el análisis y presentación de los mensajes de datos cumpla con los siguientes requerimientos:

- *Autenticidad:* hace referencia a que el contenido de la evidencia no ha sido modificado, que proviene de una fuente previamente identificada y que la información contenida en la misma es precisa.

- *Precisión:* la información contenida en la evidencia digital permite ser relacionada positivamente o afirmativamente con el incidente o delito informático. No deben existir o presentarse dudas en los procesos llevados a cabo en la recolección o incautación de la evidencia digital para evitar que se haga nula la presentación de la evidencia digital en un proceso.

- *Suficiencia:* la evidencia digital presentada debe ser completa, es decir que por sí misma pueda aclarar el escenario del delito informático y no parcialmente circunstancias o eventos del mismo.

En términos informáticos, estas pruebas documentales son archivos de diversos formatos que han sido encontrados en distintos tipos de almacenamiento, como por ejemplo discos duros, dispositivos móviles o medios extraíbles; que

aplicándoles las adecuadas normas de recolección y análisis previo pueden ser debidamente presentados por un perito o investigador en un proceso judicial o administrativo.

De acuerdo a lo expuesto anteriormente es posible determinar o detallar la presentación de pruebas documentales de archivos comúnmente manejados en el ámbito tecnológico que son comunes en éste tipo de procesos, dichos archivos pueden ser:

- *Correos electrónicos:* deben ser presentados por el perito o investigador en formato original (msg, eml, ó mbox), que contengan las características principales del correo, entre las que se encuentran: el encabezado del mensaje, la fecha ya sea de envío o recepción, la cuenta del emisor y el receptor o destino. Una vez teniendo estos datos base del archivo, es posible realizar trazas de rastreo del mensaje que pueden aclarar situaciones o acciones llevadas a cabo en los antecedentes del presunto delito informático.

- *Fotografías o imágenes*: la presentación en original de los archivos de tipo imagen puede proporcionar varios datos de gran importancia para ser presentados como evidencias, como: la fecha de creación, dimensiones e incluso tratándose de fotografías se pueden extraer datos de referencias de cámaras o dispositivos con los que fueron capturadas las mismas y la ubicación geográfica al momento de tomar las imágenes.

- *Sitios Web*: al igual que los correos electrónicos también deben ser presentados en su formato de archivo original, bien sea html, php o un archivo único web e incluso el código fuente del mismo. Pero adicional a esto, el perito o investigador debe percatarse de capturar o tener en cuenta un método para certificar la fecha y hora en que se realizó la extracción o toma de la evidencia.

- *Archivos de audio y video*: en el caso de grabaciones de voz, intercepciones telefónicas o capturas de video con o sin audio, es requerido el formato original en que se capturaron las evidencias acompañado por su estampa cronológica que permita al perito demostrar datos de fecha y hora precisos en que fue generado el contenido del archivo presentado en el juicio o proceso judicial.

Con ejemplos de presentación como los anteriores se puede determinar que un perito o investigador debe estar muy atento al momento de realizar la captura de las evidencias digitales, no debe dejar pasar ningún detalle o proceso y al momento de presentar una prueba documental de las evidencias digitales recolectadas asegurarse que las mismas cumplan con los requisitos mínimos para su aceptación frente a un tribunal.

V. CONCLUSIONES

- Se debe tener en cuenta la importancia de llevar una correcta y completa documentación en un proceso de análisis de evidencia digital. En estos apuntes, formales o informales, es donde el perito puede registrar desde el comienzo de su labor y paso a paso la metodología utilizada y los hallazgos que evidencia durante el análisis. Para posteriormente compararlos con los resultados generados por las herramientas (software o hardware) que haya utilizado como apoyo durante la investigación.

- Actualmente se consiguen en el mercado muchas herramientas que sirven de apoyo al perito forense en el desarrollo de su investigación, algunas son licenciadas, otras son gratuitas, pero no todas ofrecen las mismas opciones de análisis y se puede decir que ninguna es completa por si sola. Por esa razón, el investigador forense debe asegurarse de conocer muy bien la metodología y el procedimiento a seguir para llevar a cabo el análisis de la evidencia, ya que solamente teniendo una amplia claridad sobre el método

a seguir, podrá elegir una u otra herramienta de acuerdo a su conveniencia, y podrá defender ante un juzgado o ante la junta directiva de su empresa, de manera profesional, los hallazgos que encuentre durante su trabajo, sin importar que tipo de herramientas haya utilizado.

- Las pruebas documentales basadas en evidencias digitales deben ser examinadas muy bien por el perito o investigador para evitar que al momento de la presentación de las mismas en un proceso no cumplan con los requerimientos establecidos ante una corte.

- La persona encargada de realizar la recolección de las evidencias digitales y presentación de las mismas como pruebas documentales requiere tener un nivel profesional o técnico calificado con la suficiente experiencia en los temas a exponer ya que es de gran importancia para demostrar la validez de los hallazgos encontrados en las pruebas periciales. Y es importante que nunca olvide que se debe realizar la menor cantidad de modificaciones posibles sobre la evidencia, para no invalidarla a la hora de presentar el informe.

REFERENCIAS

[1] Ley Nº 527 de 1999. Diario Oficial No. 43.673, de 21 de agosto de 1999. Bogotá, 18 de agosto de 1999. Artículo 2º literal a. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999_pr001.html

[2] A. Ghosh. (2004, marzo). "Guidelines for the Management of IT Evidence" [En línea]. Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf

[3] J. Cano. "Introducción a la Informática Forense" [En línea], Revista 96, ACIS, pag. 66. Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[4] H. A. Rodríguez. (2013, julio 15). "Estadísticas Estudio de Comercio Electrónico Según Bigcommerce" [En línea]. Disponible en: http://blog.e-mipyme.com/2013/07/estadisticas-estudio-de-comercio-electronico-segun-bigcommerce.html

[5] Ley Nº 527 de 1999. Diario Oficial No. 43.673, de 21 de agosto de 1999. Bogotá, 18 de agosto de 1999. Artículo 10º. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999_pr001.html

[6] D. Torres, J. Cano, S. Rueda, "Evidencia Digital en el Contexto Colombiano" [En línea]. Disponible en: http://www.acis.org.co/index.php?id=856

[7] E. Pérez. "La informática forense o Forensic" [En línea]. Disponible en: http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=121

Autores

Carlos Yesid Espinel Ballén
Estudiante Especialización en Informática Forense

David Fernando Bolaños Marín
Estudiante Especialización en Informática Forense