La Importancia de la Correcta RECOLECCIÓN de la EVIDENCIA DIGITAL en los Procesos Legales

Morales Pinzón Andrés G.
agmorales99@gmail.com
Universidad Piloto de Colombia

Resumen— El presente artículo explica la importancia de la recolección de evidencias digitales y la forma en que éstas pueden llegar a ser fundamentales como pruebas en cualquier de delito que haya tenido como medio un recurso tecnológico informático. La correcta recolección, siguiendo el debido proceso establecido por la ley es determinante y establece la validez de la evidencia digital que puede desvirtuar o reafirmar cualquier tipo de proceso legal.

Índice de Términos— Cadena de custodia, delito informático, evidencia Digital, material probatorio, recolección de pruebas.

Abstract— This article explains why it's important to collect digital evidence. Also, how it can become critical as evidence in any case where a crime has been committed by using technological digital resources. Proper collection, following the due process of the law is crucial and establishes the validity of the digital evidence that may undermine or reinforce any legal process.

Keywords— Chain of custody, collecting evidence, computer crime, digital evidence, legally seizing computer Evidence, material evidence

I. Introducción

El delito se puede definir como toda aquella conducta de acción u omisión contraria al ordenamiento jurídico del país donde se produce [1], este comportamiento siempre ha existido y es inherente al ser humano por lo cual se han establecido diferentes reglas y sanciones para evitarlos y castigarlos. Estas conductas deben ser típicas; es decir, que sea una conducta claramente descrita por la ley y de la cual se imponga una pena.

Debido al imparable avance tecnológico y al desarrollo y creación de nuevas tecnologías de información, estos comportamientos tomaron una nueva forma o un nuevo modo de operación que tiene como medio el uso de tecnologías informáticas; en consecuencia es necesaria la creación de nuevas legislaciones para tipificar esta clase delitos y garantizar su buen uso. La ley que establece una referencia para este tipo de conductas en Colombia es la 527 de 1999, más conocida como la Ley de comercio electrónico, de ésta se desprenden los conceptos y principios básicos que hacen referencia a la utilización de medios digitales, y es aplicable a todo tipo de información en forma de mensaje de datos; estos últimos son definidos como la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio electrónico de datos, Internet, correo electrónico, telegrama o el telefax [2].

El uso de un medio informático en la mayoría de los casos deja un rastro de actividad en los dispositivos de almacenamiento o en la red, estos son de vital importancia para la resolución de un proceso legal en caso de haberse cometido un ilícito, pero la inadecuada manipulación de la evidencia digital al momento de su recolección puede traer como consecuencia la alteración, destrucción parcial, destrucción total o invalidez legal de esta; convirtiéndose en un talón de Aquiles para las autoridades encargadas de recolectar, analizar y presentar esta clase de pruebas, que en muchos casos se tiene que desechar debido a las malas prácticas.

En este artículo se explicará la importancia del debido proceso para la recolección de evidencias digitales y hará referencia a casos conocidos por la opinión pública sobre este tipo de incidentes.

II. ¿Qué es la Informática Forense?

La informática forense o cómputo forense

(*computer forensics*), se puede definir cómo una disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con un caso. Las tareas propias asociadas con la evidencia en la escena del crimen son la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección para así detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado [3].

La evidencia digital puede clasificarse en:

Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes… etc.).

Registros generados por equipos de tecnología informática como registros de auditoría, registros de transacciones, registros de eventos… etc.

Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática como hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos… etc. [3].

Al enfrentarnos a una situación de recolección de evidencia digital en un lugar donde acaba de ocurrir un evento informático, encontraremos muchas interrogantes sobre qué y cuál tipo de información debemos empezar a recolectar.

El procedimiento que se aplique debe garantizar que la información no desaparezca o se destruya, por ejemplo si ésta se encuentra contenida en un medio de almacenamiento temporal (memoria RAM)[1], o también a que se alterare, modifique o elimine. Este tipo de labor debe ser hecha por una persona experta con conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, además de conocimientos en técnicas y procesos interdisciplinarios competentes al tratamiento de la información digital, contando con herramientas y medios informáticos altamente especializados que le permitan garantizar la confiabilidad de los datos recogidos.

III. Las buenas prácticas en la Recolección de Evidencia Digital

Los aspectos fundamentales en la recolección de evidencia digital se basan en los mismos principios empleados por las ciencias forenses al momento de la llegada a la escena de un crimen, pero detalladas en aspectos técnicos propios. La recolección de evidencia que tenga que ser presentada como parte de un proceso judicial debe realizarse bajo el control y poder de las autoridades judiciales.

Se puede decir que el término "*evidencia digital*" abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. En el proceso de recolección se debe aplicar una aproximación metodológica que permita el manejo adecuado de la evidencia digital, minimice la posibilidad de cometer errores y que en alguna medida garantice la admisibilidad de la misma en situaciones jurídicas. [4].

Como medidas técnicas se debe tener en cuenta que los dispositivos y herramientas sean idóneos para dicha labor, además de otros aspectos como:

A. La integridad de los medios

Se debe asegurar que los medios informáticos en los cuales se vaya a recolectar la información no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares que puedan alterar la información, lo que se conoce en el ambiente del cómputo forense como esterilidad de los medios informáticos.

B. Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia, para esto se sugiere utilizar algoritmos y técnicas de control basadas en firmas digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. [3]. La Ley 794 de 2003

[1] Memoria RAM - Memoria de acceso aleatorio (en inglés: Random-Access Memory) memoria de trabajo temporal para el sistema operativo, los programas y la mayoría del software.

establece la Firma Digital[2] como un mecanismo de aseguramiento técnico y jurídico de las comunicaciones electrónicas.

C. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

Se debe documentar cada procedimiento paso a paso, herramientas y software utilizado, descripción de versión y licencias, para que en un caso de confrontación de idoneidad se puedan reproducir los resultados por una tercera persona.

D. Mantenimiento de la cadena de custodia de las evidencias digitales

En principio se debe asegurar el área donde ocurrió el incidente con el fin de tener custodia, dentro de ésta se comprometen los elementos allegados al caso y en poder de la persona encargada de la recolección, adelantando una diligencia formal y especial para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. También se debe referenciar: quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo [4, 5], así mismo se debe registrar en medio fotográfico o video la escena del posible ilícito y levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena detallando los elementos informáticos allí involucrados.[5].

Adicionalmente, es preciso que los software o aplicaciones soporte de la totalidad del proceso de recolección hayan sido previamente probados y analizados por la comunidad científica, para que conociendo su tasa de efectividad, sean validados en un procedimiento ante una diligencia legal; generalmente en el proceso de recolección, análisis y sustentación de evidencias digitales es muy aceptado el software forense llamado ENCASE [6], que goza con el alto reconocimiento de comunidades científicas y autoridades judiciales.

Por si mismos estos procedimientos y buenas prácticas no determinan la inocencia o culpabilidad en un delito, sólo aseguran que esta evidencia cumpla con los principios de autenticidad, confiablidad, suficiencia, completitud y que se hayan obtenido bajo el respeto por las leyes o normas legales vigentes en el sistema jurídico, y que en caso de representar un vínculo entre el delito y un posible autor, sean irrefutables.

IV. Declaración de Ilegalidad de la Evidencia Digital Recolectada durante la Operación Fénix

Uno de los antecedentes más conocidos por la opinión pública colombiana debido a su gran difusión a través de los medios de comunicación masivos, fue el de la llamada "Operación Fénix", hecho que tuvo lugar el 1 de Marzo de 2008 donde el Comando de Operaciones especiales "*COPES*" de la Policía Nacional de Colombia realizó un operativo contra de la guerrilla de las "*FARC*"[3] en territorio ecuatoriano, y donde se dio de baja al guerrillero Luis Édgar Devia Silva (Alias Raúl Reyes)[4]. En el sitio del ataque, se recuperaron computadores, discos duros, y memorias USB que contenían información que de algún modo podría determinar posibles vínculos con miembros del gobierno nacional, como lo era el caso del ex representante a la Cámara Wilson Alfonso Borja Díaz, quien fuera acusado públicamente en ese momento por altos funcionarios del gobierno, basándose en algunos documentos de la evidencia digital recuperada donde él era mencionado; esto desató un circo mediático del cual se podría deducir que éstas evidencias revelarían y demostrarían muchos de los secretos más importantes de las "*FARC*", al publicarse a través de medios de comunicación masivos comentarios y acusaciones por parte de altos funcionarios del Ejército

[2] Firma Digital - Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.

[3] FARC - Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo Grupo guerrillero que opera dentro del territorio Colombiano

[4] RAÚL REYES - Luis Edgar Devia Silva, alias Raúl Reyes, (30/09/1948 - 1/03/2008) fue un guerrillero colombiano, miembro del Secretariado, portavoz y asesor del Bloque del Sur de las "FARC".

Nacional, Policía Nacional, y hasta del entonces presidente Álvaro Uribe Vélez. Estos hechos generaron una expectativa sobre la forma en que este tipo de evidencia podría implicar a muchos funcionarios de oposición al gobierno; pero solo se pudo evidenciar un completo desconocimiento sobre las leyes y normas vigentes con respecto al correcto manejo de la evidencia digital por parte de la fuerza pública y del gobierno de la época.

En este caso particular se identifica el elemento objeto de investigación en este artículo, la evidencia digital que es recuperada en el sitio del operativo militar y que se presumió era propiedad del guerrillero alias Raúl Reyes. En este caso las evidencias digitales eran el eje central del juicio que enfrentó este funcionario ya que en estas se basaban todas las acusaciones, por lo tanto fueron sometidas a una rigurosa investigación que arrojó resultados contundentes con respecto a su recolección y manipulación, como resultado se declararon ilegales y desprovistas de toda validez jurídica para este y futuros casos, resolviendo así la absolución del acusado.

Entre los puntos resueltos por parte de la Corte Suprema en este caso se destacan los que hacen puntualidad en la ilegalidad de las pruebas obtenidas:

"*Ninguna Autoridad colombiana tiene competencia o está facultada para practicar en el extranjero inspecciones y recoger elementos materiales de conocimiento, por fuera de los mecanismos de la cooperación internacional y la asistencia judicial, lo que significa no haber obtenido previamente autorización, aval o visto bueno, por lo menos a través del visado sobre el específico propósito, de las autoridades del Estado concernido; que si algún servidor público lo hace más allá de sus específicos propósitos, la prueba recogida es ilegal, y ante la carencia absoluta de dicho contenido, de modo irremediable le aplica la cláusula de exclusión. No es admitida en el mundo jurídico para sustentar ningún propósito procesal.*" [7].

EL comandante del "*Grupo Blancos de Alto Valor*" de operaciones especiales, admitió que los documentos de los computadores de alias Raúl Reyes fueron recogidos por miembros de las fuerzas armadas colombianas, durante una inspección que hizo en el territorio ecuatoriano, desatendiendo frontalmente el debido proceso que gobierna la producción de pruebas en el exterior, además que quienes así procedieron ni siquiera tenían facultades de policía judicial, es imperativo declarar que el contenido demostrativo de estos elementos es ilegal y por consecuencia en términos del artículo 29 de la carta Política, se le aplicará la cláusula de exclusión como en efecto se procede. [7].

También se resolvió que la información encontrada donde era mencionado el acusado no establecía ningún vínculo que determinara los cargos de acusación y que por lo tanto no había existido una conducta delictiva.

En este caso se puede concluir que las autoridades colombianas en su afán de mostrar resultados diferentes a los de una acción militar exitosa, procedió de manera ilegal en la obtención de la evidencia digital. Además se generó una expectativa popular sobre el valor y el impacto que tenía un nuevo concepto en la cultura del pueblo colombiano como lo era el de "*evidencia digital*", y que por la conclusión del caso no tuvo los efectos esperados, demostrando así un paso en falso en el tratamiento y manejo discreto de la información.

V. Caso Nicolás Castro

Uno de los casos más mencionados por los medios de comunicación fue el de Nicolás Castro, estudiante de bellas artes de la Universidad Jorge Tadeo Lozano el cual fue denunciado formalmente ante la Fiscalía General de la Nación por Jerónimo Uribe hijo del presidente en ese entonces Álvaro Uribe Vélez, de la creación de una página en facebook.com, donde explícitamente lo amenazaba de muerte. [8].

El caso en particular, debido a que el demandante gozaba de un gran poder por ser el hijo del presidente de entonces, estuvo lleno de vicios y violaciones de todo tipo por parte del ente acusador[9], pero lo que determinó definitivamente la inocencia de Nicolás Castro fueron las evidencias digitales presentadas ante el juez, la más mencionada y conocida fue la presentación de un texto con una conversación sostenida por chat entre

Nicolás Castro y su novia, en formato de Microsoft Word y el cuál había sido copiado y pegado desde la aplicación de Microsoft Messenger; conversación en la cual se hacía mención de dicha página y que, presentada fuera de contexto, hacía parecer que el acusado admitía haber creado o tenido que ver con la creación de la misma [9]; esta prueba fue declarada ilegal ya que violaba el debido proceso de recolección, análisis y presentación de evidencia digital y no demostraba los principios básicos requeridos de autenticidad, integridad, y no repudio de cualquier elemento material probatorio; en consecuencia no se logró demostrar un vínculo entre la conducta y el acusado por lo cual fue absuelto.[10].

Aunque este caso fue arbitrariamente dilatado para demostrar la famosa mano dura que promulgaba el gobierno de Álvaro Uribe y para tratar de sentar un precedente disciplinario concerniente a los delitos informáticos, de nuevo solo se demostró el desconocimiento e inoperancia de los entes encargados de recolectar, mantener y presentar la evidencia digital, así como también el abuso de poder al que son sometidos los ciudadanos en el país.

VI. Conclusiones

En Colombia la Ley 527 de 1999 otorga validez jurídica y probatoria a los mensajes de datos, que entre otros, pueden ser usados para la persecución y procesamiento judicial de los criminales que hayan cometido un delito informático, y así mismo se pueda compensar daños causados por estos a través de la creación y aplicación de medidas para prevenir casos similares, pero para que estos objetivos sean logrados se deben tener en cuenta, entre muchos otros aspectos, el de la recolección de evidencia digital.

Después de haber descrito en este artículo la importancia de la recolección de evidencias digitales en un caso donde se pueda establecer una relación entre un delito y su autor, se puede concluir que en el proceso de recolección se debe aplicar una aproximación metodológica que minimice la posibilidad errores, garantice un manejo adecuado, así como los principios fundamentales de autenticidad, confiablidad, suficiencia, completitud, y teniendo en cuenta aspectos técnicos como:

La integridad de los medios informáticos usados para su recolección.

La verificación de las copias en medios informáticos a través de firmas digitales.

La detallada documentación de los procedimientos, situaciones, personas, elementos, herramientas y aplicaciones que hacen parte de la operación y su correcta custodia.

Todo esto siguiendo las normas legales vigentes del sistema jurídico para así garantizar la admisibilidad del material probatorio en situaciones legales.

REFERENCIAS

[1] Delito. En Wikipedia. Consultado: Abril 2013 Disponible en: http://es.wikipedia.org/wiki/Delito

[2] Colombia. Ley 527 de 1999: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos", Diario Oficial No. 43.673, 21 de Agosto de 1999.

[3] J.J. Cano, "Introducción a la informática forense" [online], Asociación Colombiana de Ingenieros de Sistemas-acis.org.co, consultado: Abril de 2013 Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[4] D.A. Torres, J.J. Cano, S. Rueda: "Evidencia digital en el contexto colombiano" [online], Asociación Colombiana de Ingenieros de Sistemas-acis.org.co, consultado: Abril de 2013 Disponible en: http://www.acis.org.co/index.php?id=856

[5] J.J. Cano, "Administración de la Evidencia" [online], Asociación Colombiana de Ingenieros de Sistemas-acis.org.co, consultado: Abril de 2013 Disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/JeimyCano_VIJNSI.pdf

[6] Guidance Software. Información sobre la Solución FIM[online], de EnCase® www.guidancesoftware.com, www.encase.com, www.missioncapable.com.

[7] Corte Suprema de Justicias Proceso No 29877, "Por el cual Profiere Auto Inhibitorio a favor de Wilson Borja", Mayo de 2011.

[8] J. Lombana & Abogados, "Radicado de denuncia de Jerónimo Uribe por amenaza y terrorismo", Julio de 2009 Recuperada de: http://farm3.static.flickr.com/2784/4489237955_e77280e244_b.jpg

[9] J. León, "Los Abusos que Sufrió Nicolás Castro antes de ser Absuelto" [online], lasillavacia.com, Septiembre de 2011, Disponible en: http://www.lasillavacia.com/historia/los-abusos-que-sufrio-nicolas-castro-antes-de-ser-absuelto-27604

[10] C. Cortés, “Crónica del 'falso positivo' de Facebook en nueve episodios” [online], *lasillavacia.com*, Abril de 2010 Disponible en: http://www.lasillavacia.com/historia/9091

Andrés G. Morales
Ingeniero de Sistemas, Egresado de la Universidad de Cundinamarca (Colombia), Programador de sistemas desde Agosto de 2008, actualmente cursando estudios de Seguridad Informática en la Universidad Piloto de Colombia.