DOCTRINA

Conservación de la cadena de custodia de una evidencia informática

Javier RUBIO ALAMILLO

Ingeniero Superior en Informática, Vocal de la Junta de Gobierno del Colegio Profesional de Ingenieros en Informática de la Comunidad de Madrid

Resumen

No han sido pocas las ocasiones en las que los Tribunales han denegado la validez procesal a pruebas informáticas (1) en procedimientos judiciales debido a la destrucción de la cadena de custodia de las mismas. La cadena de custodia es un asunto de extrema importancia en lo que a pruebas informáticas se refiere, puesto que determinar una posible alteración de la prueba en una evidencia de este tipo es una cuestión matemática y absolutamente dicotómica, esto es, o la prueba no ha sido alterada o la prueba ha sido alterada (salvo, actualmente, para evidencias informáticas de teléfonos móviles, en las que se ahondará en este artículo). Si la prueba no ha sido alterada desde su recolección hasta su estudio forense (2), la cadena de custodia habría sido conservada, mientras que, por el contrario, si la prueba ha sido alterada, la cadena de custodia habría sido destruida.

La conservación de la cadena de custodia de una evidencia informática es un aspecto trascendental en los procedimientos judiciales actuales (sobre todo en los penales). Es cada vez más habitual que, dentro de las piezas de convicción incautadas a cualquier sospechoso de haber cometido un delito, se encuentren discos duros, memorias USB, discos ópticos y, especialmente, teléfonos móviles o tabletas. Estas evidencias son, posteriormente, volcadas y analizadas por profesionales de las Fuerzas y Cuerpos de

Seguridad del Estado, pero se ha de prestar especial cuidado y atención a no manipular las evidencias (ni encenderlas, ni conectarlas a ningún ordenador u otro tipo de máquina), bajo ningún concepto, hasta que el volcado de las mismas no haya sido autorizado por el juez y, siempre, bajo la tutela del letrado de la administración de justicia o del funcionario de la Policía Judicial al mando de dicha tarea.

Cualquier intromisión, acceso, conexión o cualquiera otra interacción con las evidencias en el intervalo de tiempo que media desde la incautación de las mismas hasta su volcado, las contaminará e invalidará irremediablemente. La interacción con las evidencias en dicho intervalo, dejará huella casi sin ningún género de dudas y, cualquier perito informático colegiado de parte, con experiencia y herramientas forenses de última generación a su alcance, podrá dictaminar que la cadena de custodia fue quebrada.

I. CONCEPTO DE CADENA DE CUSTODIA

No han sido pocas las ocasiones en las que los Tribunales han denegado la validez procesal a pruebas informáticas (1) en procedimientos judiciales debido a la destrucción de la cadena de custodia de las mismas. La cadena de custodia es un asunto de extrema importancia en lo que a pruebas informáticas se refiere, puesto que determinar una posible alteración de la prueba en una evidencia de este tipo es una cuestión matemática y absolutamente dicotómica, esto es, o la prueba no ha sido alterada o la prueba ha sido alterada (salvo, actualmente, para evidencias informáticas de teléfonos móviles, en las que se ahondará en este artículo).

Si la prueba no ha sido alterada desde su recolección hasta su estudio forense (2) , la cadena de custodia habría sido conservada, mientras que, por el contrario, si la prueba ha sido alterada, la cadena de custodia habría sido destruida.

La cadena de custodia para una prueba es el procedimiento que permite conservar, desde su recolección hasta su análisis, a la prueba tal cual es. Esta definición implica que cualquier alteración a la que sea sometida la prueba, de forma accidental o consciente, desvirtúa la prueba y la convierte en algo que ya no es la prueba.

La prueba está sometida, desde su recolección hasta su análisis, a numerosas vicisitudes. Primeramente ha de identificarse, posteriormente, ha de precintarse, etiquetarse, inventariarse y almacenarse, quedando siempre bajo custodia de un funcionario público como un letrado de la administración de justicia, que actúa como fedatario público, para finalmente analizarse ante dicho funcionario u otro que le sustituya, en todo caso, aquél que la Ley y la jurisprudencia autoricen.

En España, las leyes procesales carecen de artículos que dispongan sobre cómo actuar con las pruebas para conservar la cadena de custodia

Cualquier cambio en el *estatus* de la prueba, como el desprecintado de la misma para su análisis o, simplemente, un cambio en el funcionario que la custodia, debe ser recogido en un acta firmada por los funcionarios que analizan la prueba, o por el funcionario bajo el cual pasa a estar custodiada la prueba y, siempre, firmada también por el funcionario bajo el cual se encuentra custodiada la prueba en el momento del cambio en el *estatus* de la misma. Cualesquiera cambios en el *estatus* de la prueba que no aparezcan perfectamente documentados y firmados por el funcionario en custodia de la

prueba, van a levantar suspicacias sobre si la cadena de custodia ha sido quebrada, especialmente si la prueba es *de cargo*.

En España, las leyes procesales civil y criminal carecen de artículos que dispongan sobre cómo actuar con las pruebas para conservar la cadena de custodia, ni tampoco existen reglamentos que indiquen a los funcionarios cómo proceder. El sentido común, la buena fe de los funcionarios, la presunción de veracidad de éstos y la jurisprudencia, guían las actuaciones en pro de la conservación de la cadena de custodia de las pruebas. Sin embargo, tal y como advirtió el profesional que suscribe en un artículo publicado en el número 8662 de La Ley (3) , es inadmisible que las garantías procesales de un acusado descansen sobre funcionarios públicos en lugar de sobre el propio proceso.

Una de las definiciones más utilizadas en la literatura jurídica española para la cadena de custodia aparece en la STS 1190/2009, de 3 de diciembre, en la que se indica que la conservación de la cadena de custodia satisface la garantía de la «mismidad de la prueba». Según la citada sentencia, «la cadena de custodia es una figura tomada de la realidad a la que tiñe de valor jurídico con el fin de en su caso, identificar el objeto intervenido, pues al tener que pasar por distintos lugares para que se verifiquen los correspondientes exámenes, es necesario tener la seguridad de lo que se traslada y analiza es lo mismo en todo momento, desde que se recoge del lugar del delito hasta el momento final que se estudia, y en su caso, se destruye». La conservación de la cadena de custodia, en esencia, garantiza que una prueba es la que es.

Aplicando la definición de cadena de custodia a las evidencias informáticas, la STC 170/2003 indica que «la incorporación al proceso penal de los soportes informáticos» debe realizarse «con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y, consecuentemente, que los resultados de las pruebas periciales» se llevan a cabo «sobre los mismos soportes intervenidos o que éstos no hubieran podido ser manipulados en cuanto a su contenido».

II. CONSERVACIÓN DE LA CADENA DE CUSTODIA EN EVIDENCIAS INFORMÁTICAS *NO VOLÁTILES*

Cuando se habla de evidencias informáticas *no volátiles*, se hace referencia a aquéllas que pueden prevalecer, si se toman las debidas precauciones, inalteradas a lo largo del tiempo, ya que se hallan contenidas en soportes físicos como discos duros, memorias USB, discos ópticos, etc., físicamente accesibles para el investigador forense. Así pues, una evidencia informática *no volátil* podría ser cualquiera de estos dispositivos.

Supóngase el escenario de un crimen en el que los investigadores forenses encuentran el arma homicida junto al cadáver. Parece claro que éstos, en ningún caso, van a tomar directamente y sin precauciones, el arma, a fin de almacenar la prueba de cualquier manera entre los efectos encontrados. La forma de proceder, previsiblemente, será primero tomar fotografías de todo el lugar, posteriormente y con unas precauciones extremas, tomar con unos guantes de látex el arma a fin de evitar la contaminación de las huellas del investigador con las del homicida y, finalmente, introducir la prueba en una bolsa hermética que deberá ser debidamente precintada, etiquetada, inventariada y almacenada, levantando acta de todo el proceso, a fin de ser enviada al laboratorio forense cuando proceda para ser analizada.

Una evidencia informática debe recibir el mismo trato que cualquier otra evidencia, con la certeza

absoluta de que cualquier conexión que se produzca a un ordenador de la evidencia (disco duro, memoria USB, dispositivo móvil, etc.), sin tomar las debidas precauciones, la contaminará de forma irremediable (es decir, conectar a un ordenador la prueba sin precauciones, sería el equivalente a tomar el arma homicida del ejemplo anterior sin guantes). Si se trata de un dispositivo móvil, como un teléfono inteligente o una tableta, el quebrantamiento de la cadena de custodia se producirá con el encendido o puesta en funcionamiento del terminal, ya que el sistema operativo del aparato realizará modificaciones en el estado del mismo, imposibles de impedir, de forma inmediata a ser activado, mientras que su posterior conexión a la red telefónica y/o de datos podría ocasionar que se enviasen y/o recibiesen mensajes o, incluso, órdenes para destruir la información contenida en el terminal o en terminales u ordenadores remotos.

En caso de evidencias informáticas es esencial desconectarlas inmediatamente de la alimentación eléctrica

Cuando se intervienen evidencias informáticas en funcionamiento, es esencial, para el correcto mantenimiento de la cadena de custodia de las mismas, desconectarlas inmediatamente de la alimentación eléctrica (4) . Esta apreciación descarta que se pueda producir un apagado *ordenado* del dispositivo, utilizando periféricos como el ratón y/o el teclado, ya que esta acción alteraría la evidencia y, además, podría ocasionar la activación de un proceso informático preparado para lanzarse inmediatamente antes de ejecutarse el apagado *ordenado*, configurado para destruir archivos que podrían ser esenciales para la investigación. Igualmente, el tiempo empleado en esta operación podría ser vital para que al criminal responsable de la infraestructura, o a algún subalterno, le diese tiempo a ejecutar de forma remota lo que se conoce como «botón de pánico», que es un programa que, a distancia, activa un proceso configurado en el ordenador para eliminar toda la información sensible.

Desconectando el dispositivo de la fuente de alimentación, se tiene la certeza de que la información almacenada en los dispositivos físicos (discos duros, memorias USB, discos ópticos, etc.) hasta el mismo momento de la desconexión, permanecerá inalterada. Existen riesgos evidentes en esta operación, como por ejemplo la interrupción de un programa delictivo que se halle en ejecución en ese preciso instante, el cual constituiría una prueba y cuya huella de ejecución ya se habría perdido, puesto que la desconexión del dispositivo de la fuente de alimentación desmagnetiza la memoria principal o RAM (5) . Para evitar esta pérdida de pruebas y, siempre antes de desconectar la fuente de alimentación, un perito informático colegiado o policial, podría extraer los procesos en ejecución de la memoria RAM, detallando todo el procedimiento ante fedatario público (para evitar que se levanten suspicacias sobre una posible alteración maliciosa de la evidencia), utilizando herramientas forenses, siempre y cuando exista la completa seguridad de que nada va a alterar sustancialmente la evidencia (y, por tanto, habiendo desenchufado y deshabilitado previamente todos los elementos alámbricos e inalámbricos, respectivamente, conectados a la red local y a Internet, para evitar que el dispositivo reciba órdenes del exterior que pudieran destruir toda o parte de la información almacenada, o envíe órdenes a otros sistemas remotos).

En el caso de dispositivos móviles intervenidos en funcionamiento, el procedimiento prioritario de custodia a seguir no es extraer la batería, como podría deducirse de lo indicado anteriormente para evidencias informáticas no móviles, sino que deben mantenerse con batería hasta su análisis forense, con la única precaución de evitar que reciban información del exterior y que, por tanto, se

conecten a la red telefónica y/o de datos, por supuesto sin interactuar de forma directa con el dispositivo, ya que esta interacción contaminaría la evidencia. Para poder compatibilizar estas premisas, debe utilizarse, para cada una de las evidencias móviles intervenidas, un artilugio conocido como *jaula de Faraday*. Una *jaula de Faraday* es, esencialmente, un contenedor fabricado con material especial que impide que las ondas de radiofrecuencia penetren al interior del mismo, o que salgan al exterior, aislando el terminal.

Por otra parte, cabe reseñar que, si se sabe con certeza que las evidencias móviles no van a ser analizadas en un espacio breve de tiempo y, por tanto, que no pueden ser, bajo ningún concepto, mantenidas con batería, la mejor opción es, efectivamente, retirar la batería. En caso de que la compuerta de la batería no pueda abrirse o que la batería se encuentre inaccesible (ya existen modelos de este tipo), es necesario utilizar una *jaula de Faraday* para el dispositivo, al menos hasta que la batería del mismo se consuma y el teléfono o tableta se apague, al objeto de que sea imposible que el aparato pueda recibir información desde el exterior o enviarla. La *jaula de Faraday* también debe utilizarse cuando se produzca el encendido del dispositivo, ante funcionario público, en el momento de su análisis forense en el laboratorio con herramientas especializadas, una vez vaya a ser extraído volcada toda la información que contiene el terminal para su posterior análisis, dejando salir, de la *jaula de Faraday*, el cable de conexión al terminal de forma muy cuidadosa, para enchufarlo al sistema que extraerá, aplicando técnicas forenses, la información del terminal.

En caso de que las evidencias informáticas intervenidas no se encuentren en funcionamiento, o si se encontraban en funcionamiento y, tal y como se ha indicado, ya hayan sido desconectadas de la alimentación eléctrica, es necesario precintarlas y etiquetarlas, dando fe el letrado de la administración de justicia del acto. En el acta del letrado de la administración de justicia debe constar, con escrupuloso lujo de detalles, acompañando si es posible con fotografías, el estado de cada una de las evidencias, así como bajo qué condiciones se procede a la custodia de las mismas, hasta el momento de ser volcadas o clonadas (6) para su posterior análisis. Al objeto de evitar posibles suspicacias relativas al lugar en el que se almacenan las evidencias intervenidas, la mejor opción, siempre que sea posible llevarla a cabo, es volcar las evidencias en el acto mismo de la intervención de éstas, con material forense especializado, calculando para todas ellas sus correspondientes códigos *hash* (7) . Así, los códigos *hash* para cada una de las evidencias, quedarían anotados en el acta del letrado de la administración de justicia, pudiendo posteriormente precintar, etiquetar, inventariar y almacenar las evidencias sin temor a que puedan ser alteradas de forma accidental o maliciosa o, en caso de que lo fuesen, que dicha alteración sea fácilmente detectable cotejando el código *hash* obtenido a posteriori para cada evidencia, con el anotado en el acta.

El letrado de la administración de justicia está autorizado a no intervenir en las clonaciones o volcados de evidencias informáticas

Es preciso indicar en este punto que, el letrado de la administración de justicia, antiguamente secretario judicial, está autorizado por la jurisprudencia a no intervenir en las clonaciones o volcados de evidencias informáticas, debido a su falta de conocimientos técnicos en la materia. Así pues, la STS 1599/1999, de 15 de noviembre, dispone textualmente que «lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia

del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia». Esta afirmación no implica que el letrado de la administración de justicia no deba estar presente en el momento de la intervención, precintado, etiquetado, inventariado y almacenado de las piezas de convicción, tal y como pone de manifiesto la misma sentencia cuando indica, refiriéndose al letrado de la administración de justicia, que «cumplió estrictamente con las previsiones procesales y ocupó los tres ordenadores, los disquetes y el ordenador personal», sino que únicamente indica que no es necesario que esté presente en el volcado. Asimismo, la propia sentencia indica que el momento de solicitar una contrapericia es durante la fase de instrucción, ya que expresa, textualmente, que «la parte recurrente tuvo a su disposición, durante toda la fase de instrucción, y pudo solicitar como prueba para el juicio oral, una contrapericia que invalidase o matizase el contenido de la que realizaron los peritos judiciales. No lo hizo así, lo que pone de relieve que confiaba en su imparcialidad y objetividad». Esta sentencia fue ratificada, asimismo, por la posterior STS 256/2008, de 14 de mayo, así como por la STS 480/2009, de 22 de mayo.

Por el contrario, en caso de que no se puedan clonar in situ las evidencias, éstas deberán ser volcadas en el laboratorio, por funcionarios policiales, sin que se precise, como se acaba de indicar, la presencia del letrado de la administración de justicia para que dé fe del acto de volcado. En cualquier caso, se vuelquen las evidencias en el mismo acto de su intervención, estando el letrado de la a administración de justicia presente, o se vuelquen en el laboratorio, sin estar dicho fedatario público presente (o, estándolo, ya que en algunas ocasiones se le requiere, «para mayor garantía» del proceso, como se pone de manifiesto en la sentencia dictada el 6 de julio de 2016 por el Juzgado de lo Penal número 3 de Gijón),es un hecho incontestable que los funcionarios encargados de la clonación, deberán calcular los códigos *hash* para todas y cada una de las evidencias analizadas. Estos códigos *hash* deberán ser anotados en un acta levantado a tal efecto, en el que también se indiquen la cadena de eventos desde que la evidencia fue intervenida y puesta en custodia de un funcionario público, hasta ser volcada, así como el procedimiento de desprecinto de las evidencias (todo ello para evitar suspicacias en cuanto al proceso de custodia y almacenaje de las mismas, desde que fueron intervenidas hasta que fueron volcadas).

III. CONSERVACIÓN DE LA CADENA DE CUSTODIA EN EVIDENCIAS INFORMÁTICAS *VOLÁTILES*

Cuando se habla de evidencias informáticas *volátiles*, se hace referencia a aquéllas que podrían no prevalecer inalteradas a lo largo del tiempo, ya que se hallan contenidas en servidores y/o discos duros remotos, únicamente accesibles a través de una red de ordenadores, fundamentalmente Internet. Es decir, se trata de pruebas que el investigador forense puede visualizaren el momento de la investigación y, posiblemente en dicho momento, descargar de la red o copiar a un fichero, disco duro o memoria USB, pero a cuyo contenido *original* no tiene acceso directo y no existe la garantía de que, dichas evidencias, en un futuro inmediato, vayan a permanecer inalteradas o incluso existir, pudiendo llegar hasta desaparecer.

En esta tipología de evidencias informáticas se encuadrarían las páginas web, los mensajes enviados a través de las redes sociales más conocidas, las fotografías, audios, vídeos, documentos o, incluso, programas informáticos, cargados en páginas web temáticas y redes sociales, etc. Este tipo de contenido, corre el riesgo de ser modificado o incluso hecho desaparecer por las personas que tienen acceso físico al mismo, razón por la que es vital tomar las debidas precauciones en la

captura y preservación de dichas evidencias, utilizando lo que, en la jerga, se denominan *terceros de confianza*, que certifican el contenido de la página web, así como su URL (dirección de Internet) y, además, generan un documento con el contenido completo de dicha web, la fecha y la hora de la certificación y una firma electrónica que garantiza la integridad e inalterabilidad de dicho documento.

Asimismo, es procedente también la descarga de los contenidos que se hallen en las webs certificadas, como fotografías, archivos audiovisuales y documentos o programas informáticos, a fin de poder adjuntarlos como pruebas, calculando siempre su correspondiente código *hash*, que deberá ser anotado en el acta de captura de las evidencias firmada por el letrado de la administración de justicia o funcionario policial a cargo de la investigación. Es necesario indicar que, en las capturas certificadas de dichas páginas web, deberán observarse todos los ficheros informáticos aportados, o los enlaces a los mismos, a fin de evitar que las pruebas puedan ser impugnadas por un quebrantamiento de la cadena de custodia, en el sentido de que no se pueda asegurar que dichas pruebas verdaderamente estaban accesibles desde Internet y que realmente pudieron descargarse otras pruebas distintas, o incluso inventarse.

El letrado de la administración de justicia podrá dar fe de contenidos digitales que constituyan pruebas

El letrado de la administración de justicia, evidentemente, podrá dar fe de contenidos digitales que constituyan pruebas, dentro del ejercicio de sus funciones como fedatario público, en caso de que los funcionarios no sepan utilizar o no conozcan ninguna herramienta de *tercero de confianza*. Igualmente, las Fuerzas y Cuerpos de Seguridad del Estado, en el ejercicio de sus funciones y bajo mandato judicial, podrán levantar actas de contenidos digitales, siempre teniendo en cuenta que se deberán obtener los contenidos completos accesibles desde Internet y que deberán descargarse todos y cada uno de los ficheros informáticos que constituyan parte de la prueba, calculándose el código *hash* para cada uno de ellos y, detallando, en todo momento, el proceso de captura de las evidencias para evitar posibles impugnaciones de contenido que no pueda visualizarse en las capturas digitales pero que, los investigadores, en sus informes, indiquen que aparecía accesible desde Internet.

Por ejemplo, si se está realizando un informe cuyo objetivo es la demostración de que un vídeo con contenido audiovisual ilícito está publicado en determinada página web, con el objetivo de evitar que el autor, una vez haya sido denunciado, pueda retirar el contenido y alegar que el vídeo nunca estuvo ahí, sería necesario que los investigadores, en su informe, tomasen una captura de pantalla en la que se visualice, junto al vídeo, la dirección URL desde la que está accesible el mismo, así como otra captura con el título del vídeo, una serie de capturas con el contenido real del vídeo, obtenidas de forma aleatoria y, por último, una captura en la que se pueda apreciar la duración del vídeo. Igualmente, sería necesaria la descarga del vídeo para la aportación del mismo a la causa en un DVD y el cálculo del código *hash* del mencionado vídeo, que sería anotado en el acta de la investigación y en el informe realizado a tal efecto.

Con una fotografía, el procedimiento sería muy similar al indicado para un vídeo y, con un fichero exclusivamente de audio, además de las capturas de pantalla en las que se observe la URL del fichero, su nombre y el acceso al mismo, la descarga de éste para ser aportado en un DVD al proceso y el cálculo de su código *hash*, sería interesante la grabación de un vídeo que se pueda aportar a la causa en el que se observe todo el proceso de captura de la evidencia.

IV. EL CÓDIGO *HASH*

El cálculo del código *hash* es fundamental para la conservación de la cadena de custodia de una evidencia informática. Un código *hash* es el resultado de la aplicación de un algoritmo estándar, es decir, de un procedimiento matemático, a un conjunto de datos, que pueden estar contenidos en un fichero (como un documento o una fotografía), en una memoria USB, en un disco compacto, en un DVD, en un disco duro, etc. El código *hash* es un resumen único para el conjunto de información sobre el que se aplica el algoritmo, obteniéndose otro resumen completamente distinto, para el mismo algoritmo, con el mínimo cambio que se produzca en la información original.

La aplicación del algoritmo de *hash* es completamente unidireccional, de tal forma que es matemáticamente imposible obtener la información original si únicamente se dispone del código *hash*y del algoritmo utilizado y, además, se garantiza que es absolutamente improbable que dos conjuntos de datos distintos den como resultado el mismo código *hash* (lo que, en la literatura informática, se denomina *colisión*). Es improbable, pero no imposible, habiéndose detectado, por parte de los científicos, colisiones en algunos de estos algoritmos, como el MD5 (8) , que son absolutamente despreciables para ser tenidas en cuenta en los procedimientos judiciales, ya que para encontrar estas colisiones, se necesita la utilización de superordenadores únicamente en posesión de los mejores laboratorios informáticos del mundo. Los algoritmos de *hash* más utilizados de forma global son el ya citado MD5 (en desuso) y la familia SHA (9) . Además, las clonadoras forenses (10) profesionales más conocidas, calculan códigos *hash* para dos algoritmos, con lo que las posibilidades de colisión se reducen a prácticamente cero (el producto de las posibilidades de colisión de cada uno de los algoritmos), ya que los procedimientos de cada algoritmo son distintos y sería prácticamente imposible que un par de conjuntos de datos generase colisiones para dos algoritmos distintos, siendo ya de por sí, extremadamente difícil, que las genere para un algoritmo.

Sin cálculo del código hash para la evidencia puede decirse que la prueba no existe

Sin cálculo del código *hash* para la evidencia, se puede realizar una afirmación tan sumamente grave y tajante como que la prueba no existe, ya que es absolutamente imposible garantizar la integridad de la misma, es decir, no se podría asegurar que se esté analizando la prueba intervenida y no otra, o la prueba después de haber sido alterada consciente o inconscientemente (una prueba informática puede ser alterada, por expertos, sin dejar rastro). El código *hash*, por tanto, garantiza la «mismidad» de la prueba reseñada en la STS 1190/2009 y permite la realización de una contrapericia de parte, tal y como recoge la STS 1599/1999, partiendo del volcado de la prueba y de su código *hash* calculado. Por otra parte, es necesario reseñar que, el código *hash*, sólo garantiza la «mismidad» de la prueba desde el momento en que se calcula, por lo que es necesario prestar sumo cuidado al lugar donde se almacena la prueba antes de ser volcada, debiendo documentar dicho lugar en el acta de intervención de las evidencias y, prestando atención, a que éste se encuentre accesible únicamente a personal debidamente autorizado (lo mejor sería almacenar las pruebas bajo llave, en algún tipo de caja fuerte, indicando este extremo en el acta de fe pública, así como qué funcionario se encuentra en custodia de la llave). Asimismo, el precinto utilizado para cerrar el sobre o caja en que se guarde la evidencia antes de ser volcada y, el mismo sobre o caja, deben asegurar que una rotura de los mismos, anterior al volcado, es detectada por los funcionarios encargados de ejecutar el procedimiento de clonación, eventualidad que deberían reflejar en el acta de volcado de la evidencia.

La mejor de las opciones, para evitar cualquier tipo de suspicacia, será siempre el volcado de las evidencias y el cálculo del código *hash* para cada una de ellas en el momento de la intervención de las mismas. Así, se evitará la posibilidad de poner en duda el precintado de las evidencias y el lugar de almacenaje de éstas, en caso de que no se tomasen fotografías de dicho precintado en la intervención y de su desprecintado en el laboratorio, o que no se documentase el lugar de almacenamiento de las evidencias. Asimismo, se evitarán también posibles impugnaciones de la prueba en caso de encontrarse información fechada con posterioridad a la intervención de la evidencia (lo cual es perfectamente posibles se conecta, sin protección, una evidencia de tipo disco duro o memoria USB a un ordenador y, de hecho, ocurre constantemente en evidencias móviles, puesto que los terminales permanecen habitualmente encendidos y conectados a la red tras haber sido incautados, ya que no se suelen utilizar las mencionadas *jaulas de Faraday* o, en ocasiones, son activados —de forma bienintencionada— por los funcionarios policiales, al objeto de encontrar pruebas de los delitos, lo cual no debe realizarse bajo ningún concepto, puesto que se quiebra de forma absoluta la cadena de custodia, debiendo esperar para realizar el análisis hasta que las evidencias se encuentren en el laboratorio y, siempre, bajo las premisas ya descritas de precintado, etiquetado, inventariado y almacenado).

El cálculo del código *hash* para una evidencia intervenida de tipo disco duro o memoria USB es muy sencillo, puesto que la clonadora forense lo calcula de forma automática cuando se realiza la clonación o volcado. El letrado de la administración de justicia, actuando como fedatario público, en caso de estar presente en el proceso o, en su defecto, el funcionario policial a cargo del volcado, deberá anotarlo en el acta levantada a tal efecto. Cualquier variación en este código *hash*, calculada a posteriori sobre la prueba, por un perito informático colegiado de parte, debería ser condición necesaria y suficiente para invalidarla.

En cuanto al cálculo del código *hash* para evidencias móviles, es necesario tener en cuenta que el volcado de un dispositivo móvil ya de por sí altera la evidencia original, puesto que es necesario encender el dispositivo para realizar el volcado forense con alguna de las múltiples (y costosas) herramientas que ofrece el mercado. La tecnología forense móvil no está tan avanzada —no pudiéndose, en la mayoría de los casos, volcar toda la información del terminal— y, para volcar una evidencia móvil, es necesario encender el terminal (y, a veces, alterar éste mediante la instalación de algún tipo de programa informático, que posteriormente debe ser retirado para dejar la evidencia en un estado similar a como estaba). Esto significa que cada vez que se repita el proceso de volcado, se obtendrá una imagen o copia forense distinta para el terminal, con ciertos cambios, muy pequeños, pero cambios al fin y al cabo, puesto que el hecho de que el terminal esté activado, con el sistema operativo funcionando mientras se está realizando la extracción forense o volcado, provoca que ficheros y registros estén siendo modificados continuamente, lo cual implica que la extracción forense o volcado será diferente cada vez y, por tanto, también el código *hash* del volcado será distinto.

La mayoría de las soluciones forenses comerciales para dispositivos móviles, proporcionan el código *hash* para cada extracción, que debe ser anotado en el acta de volcado forense de la evidencia móvil, aunque cuando la extracción conste de varios archivos, lo más cómodo es comprimir, en un único fichero, todos los archivos de la extracción y calcular el código *hash* para el mismo, que será anotado en el acta, debiendo ser dicho fichero, posteriormente, grabado en un DVD y aportado a la causa. Este DVD, conteniendo el fichero de la extracción, junto a su pertinente código *hash* anotado en el acta, deberá ser el utilizado para realizar la pericial del contenido del terminal por parte de los investigadores policiales, usando las herramientas forenses correspondientes y, además, permitirá la realización de la eventual contra pericia de parte que consagra la STS

1599/1999.

Si no se realiza extracción forense del terminal móvil, calculando el código *hash* de ésta y, por el contrario, se decide investigar el terminal accediendo directamente a la evidencia, no se podría asegurar de ningún modo la «mismidad» de la prueba. Alterar la base de datos de cualquier aplicación instalada en un terminal móvil, sin dejar rastro, es sumamente sencillo, pudiendo afectar esta alteración, sin ningún género de dudas, a las posibles comunicaciones mantenidas desde el terminal, como ya puso de manifiesto este mismo profesional en un artículo técnico (11) publicado en su página web el día 30 de septiembre de 2015, en el que se demostraba la posibilidad de manipular, sin dejar rastro, la base de datos de la conocida aplicación de mensajería instantánea WhatsApp, con una notable repercusión en los medios más importantes del país, tales como el diario El Mundo (12) , la cadena COPE (13) o el Telediario de Televisión Española (14) , así como en medios internacionales. Este problema, a fecha de la escritura del presente artículo, aún no ha sido solventado por WhatsApp.

El Tribunal Supremo también se ha pronunciado a este respecto en la STS 300/2015, indicando que la facilidad con la que se puede manipular cualquier conversación mantenida a través de Internet, inclusive hasta el punto de la posibilidad de crear perfiles falsos que simulan una comunicación con otro perfil, pero que en realidad se están comunicando consigo mismo, obliga a que cualquier prueba de este tipo, se presente avalada por un peritaje informático que dictamine la autenticidad de la misma.

V. DESTRUCCIÓN DE LA CADENA DE CUSTODIA

La destrucción de la cadena de custodia, en una evidencia informática, puede producirse de múltiples formas. La más común consiste en conectar a un ordenador, sin ningún tipo de precaución, el dispositivo que debe analizarse. Cualquier conexión de un dispositivo como una memoria USB, una tarjeta SD o un disco duro, a un ordenador, sin la debida protección de lectura que proporciona un bloqueador de escritura, provocará la pérdida irreversible de la prueba, ya que el sistema operativo escribirá en los registros de acceso del dispositivo, alterando la prueba, de tal forma que el código *hash* calculado ulteriormente, será forzosamente distinto al calculado cuando la prueba fue volcada. De la misma forma, el mero hecho de encender un teléfono móvil en un momento anterior al determinado judicialmente para su volcado, también invalidará la cadena de custodia sobre el mismo, puesto que, cuando se conecta un terminal móvil, el sistema operativo del terminal comienza a funcionar y a modificar la memoria interna del terminal y, posiblemente, éste envíe o reciba información del exterior al conectarse a la red.

En cualquier caso, para que se anule la prueba debido a la pérdida de la cadena de custodia sobre la misma, será necesario que esta pérdida pueda ser probada de manera absolutamente fehaciente, no siendo suficiente la sospecha de que la cadena de custodia se ha interrumpido. Así lo dejan claro la STS 685/2010 y la STS 356/2016, en las que se dictamina que únicamente la mera sospecha sobre la pérdida de la cadena de custodia de una prueba, no es suficiente para invalidar la misma, por lo que la certeza de dicha interrupción deberá ser absoluta.

Para el caso de pruebas informáticas, en las que se calcula un código *hash* que queda anotado en el acta levantada por el

Si el hash es distinto, se tendrá la certeza absoluta de que la cadena de custodia se ha roto

letrado de la administración de justicia o por los oficiales del Cuerpo Nacional de Policía o de la Guardia Civil (o de los cuerpos policiales autonómicos) encargados del volcado o clonado de las evidencias, es muy sencillo conocer si se ha perdido o no la cadena de custodia y, además, con una certeza matemática y, por tanto, total. Basta con calcular de nuevo, ante fedatario público o funcionario policial, el código *hash* de la evidencia. Si el *hash* es distinto, se tendrá la certeza absoluta de que la cadena de custodia se ha roto y de que la prueba ya no es la *misma* que la inicial, por lo que se habría perdido ese concepto de «mismidad de la prueba» ya indicado anteriormente y que recoge la STS 1190/2009.

El ejemplo mediático más reciente de invalidación de una prueba informática por la pérdida en su cadena de custodia, a partir de la determinación de un código *hash* distinto al inicialmente calculado para la prueba, se da en la sentencia dictada para el conocido como «caso Anonymous», el 6 de julio de 2016, por el Juzgado de lo Penal número 3 de Gijón. En ella, se advierte que «el volcado de la información de los objetos incautados no fue realizado de manera adecuada dado que no coinciden los resúmenes del secretario judicial que dan garantía de que la información contenida en el dispositivo original y la volcada en un dispositivo secundario coinciden y no han sido modificadas y si se trataba de dar fiabilidad a la prueba informática, en todos los dispositivos en que no coinciden los resúmenes indicados por el Secretario y la BIT se habría perdido la fiabilidad».

VI. CONCLUSIONES

Este perito, a lo largo de su carrera profesional, ha participado en numerosos procedimientos en los que la cadena de custodia fue conservada, así como también, en procesos en los que no fue conservada y las pruebas fueron desechadas. Es vital que, para la conservación de la cadena de custodia de una prueba informática, se calcule el código *hash* de cada una de las evidencias intervenidas, en el mismo momento en el que le son incautadas al acusado o, si esto no es posible, que las pruebas sean precintadas, etiquetadas, inventariadas y almacenadas para su posterior volcado y el cálculo de su código *hash* ante funcionario policial o letrado de la administración de justicia. Además, el cálculo del código *hash* deberá producirse sin haber conectado previamente la evidencia a un ordenador y, si se trata de un terminal móvil, evitando en todo momento que éste se conecte a la red, aislándolo para ello con una *jaula de Faraday*.

Sólo realizando el cálculo del código *hash*, se podrá garantizar la conservación de la cadena de custodia en evidencias informáticas, sean éstas memorias USB, discos duros, discos ópticos, etc., o evidencias móviles, en cuyo caso, si bien existe una imposibilidad real de mantener la cadena de custodia debido a que es necesario activar el terminal para extraerla información que contiene, sí existe una posibilidad práctica de mantener dicha cadena de custodia con la utilización de la mencionada *jaula de Faraday*, que evita que el terminal se comunique con el exterior y permite la utilización, sin alterar la evidencia, de herramientas que extraen una imagen completa del terminal mientras éste se encuentra aislado.

---

(1) TARUFFO, Michele, La prueba, Ed. Marcial Pons 2008, pág. 85.

Ver Texto

---

(2) Forense, del latín forensis, «relativo al foro», «público y notorio». En la Antigua Roma, los notables de la ciudad se reunían en el foro, que era el lugar donde se discutían los asuntos públicos, que afectaban a la ciudad o al mismo Estado.

Ver Texto

(3) RUBIO ALAMILLO, Javier, La Informática en la Ley de Enjuiciamiento Criminal, Diario la Ley, número 8662, pág. 14.

Ver Texto

(4) BOIXO PÉREZ-HOLANDA, José Ignacio, Ingeniero en Informática, Responsable de Peritaje Informático en la Brigada de Investigación del Banco de España – Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos, Infoperitos.

Ver Texto

(5) Random Access Memory, memoria de acceso aleatorio, constituye la memoria principal del ordenador, donde se cargan las instrucciones que ejecuta el procesador. Se denomina«de acceso aleatorio» porque se puede leer o escribir en una posición de memoria con un tiempo de espera igual para cualquier posición, no siendo necesario seguir un orden para acceder (acceso secuencial) a la información de la manera más rápida posible. Se diferencia de la memoria secundaria o disco duro en que en esta última se almacenan los ficheros de forma persistente, mientras que en la RAM no, además de que el tiempo de acceso a la RAM es al menos un orden de magnitud más rápido que al disco duro (unas diez veces).

Ver Texto

(6) La clonación es un procedimiento forense en virtud del cual se copia la información, bit a bit, es decir, unidad mínima de información a unidad mínima de información, desde un dispositivo fuente a uno destino. Este proceso de copia incluye toda la información almacenada en el dispositivo original, incluyendo la posible información borrada de regiones del disco que aún no hayan sido sobrescritas por el sistema operativo. El dispositivo destino contendrá exactamente la misma información que el original.

Ver Texto

(7) El código hash es el resultado de la aplicación de un algoritmo matemático a un conjunto de datos, siendo, en principio, único para cualquier conjunto de datos, de tal forma que es matemáticamente imposible obtener dicho conjunto de datos original con la aplicación inversa del algoritmo.

Ver Texto

(8) El MD5 (Message-DigestAlgorithm 5, Algoritmo de Resumen del Mensaje 5), es un algoritmo de hash, desarrollado en 1991 por Ronald Rivest, profesor del prestigioso Instituto Tecnológico de Massachusetts de los Estados Unidos, con un tamaño de palabra de 128 bits o, lo que es lo mismo, 32 caracteres en código hexadecimal, hallándose actualmente en desuso debido a que se han encontrado colisiones en el mismo.

Ver Texto

(9) La familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro), es un conjunto de algoritmos de hash, desarrollados a partir de 1993 por el Instituto Nacional de Normas y Tecnología, del Departamento de Comercio del Gobierno de los Estados Unidos. Tienen una longitud de palabra que varía entre…

Ver Texto

(10) Una clonadora forense es un dispositivo capaz de clonar discos duros y memorias USB

Ver Texto

(11) RUBIO ALAMILLO, Javier, http://peritoinformaticocolegiado.es/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/

Ver Texto

(12) http://www.elmundo.es/tecnologia/2015/10/01/560d531a22601d40448b459b.html

Ver Texto

(13) http://www.cope.es/player/ponedores-whatsapp-rastro-Javier-Rubio-121015&id=2015101205040001&activo=10

Ver Texto

(14) http://www.rtve.es/alacarta/videos/telediario/telediario-21-horas-13-10-15/3322221/

Ver Texto