Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital.

Tomás Marqués-Arpa
Estudios de Informática, Multimedia
y Telecomunicación.
Universitat Oberta de Catalunya.
Email: tomasmarques@uoc.edu

Jordi Serra-Ruiz
Estudios de Informática, Multimedia
y Telecomunicación.
Universitat Oberta de Catalunya.
Email: jserrai@uoc.edu

***Resumen*—Uno de los problemas principales en el análisis forense de la información es la CdC (Cadena de Custodia), es decir, el procedimiento de trazabilidad de todas las pruebas que se obtienen durante las distintas etapas del proceso de instrucción judicial. Generalmente, las evidencias son obtenidas por los Cuerpos y Fuerzas de Seguridad del Estado y, posteriormente, son examinadas y analizadas por analistas forenses en seguridad de la información. Es imprescindible que la transferencia de información entre las partes implicadas en el proceso se lleve a cabo con las máximas garantías, tanto judiciales como procesales.**

El propósito de este artículo es la propuesta de una CdC digital y segura, vista como un conjunto de eslabones. Gracias a ello, la prueba no perderá valor jurídico puesto que aunque se haya roto un eslabón, habrá quedado asegurada por la solidez de los eslabones anteriores.

***Palabras clave*—Cadena (*chain*), cifrado (*cipher*), custodia (*custody*), estampado (*stamping*), evidencia (*evidence*), forense (*forensic*), geolocalización (*geolocation*), huella (*footprint*), paquete (*package*).**

I. Introducción

En la actualidad, con el auge de las TICs (Tecnologías de la Información y las Comunicaciones), es necesario proporcionar herramientas, métodos y procedimientos que aseguren la misma seguridad para las evidencias digitales.

El estudio se ha desarrollado en virtud de las "líneas de investigación de la Comisión Europea para 2013" [1].

La metodología utilizada ha sido la de "Diseño y Creación" (sensibilización, sugerencia, desarrollo, evaluación y conclusión) [2], [3]. Así, podemos indicar que los principales beneficios o resultados de este estudio en las evidencias digitales, serán los siguientes: la generación de una propuesta en el proceso de creación y transmisión, la contribución para la mejora en la gestión y el planteamiento de un método seguro para el envío.

Las principales cuestiones planteadas son si es posible desarrollar un nuevo método para la CdC dgital, si se puede implementar y en caso afirmativo, si se puede extender a los enlaces, datos y aplicaciones. Otras cuestiones son si el método propuesto es más seguro que el utilizado en la actualidad y con menor carga computacional, así como si existen métodos anteriores similares al tema tratado.

Así pues, se fijan los objetivos de la investigación que son:

- Una revisión, análisis y evaluación de la literatura propuesta [4]–[8].
- La implementación de un MGED (Marco de Gestión de la Evidencia Digital) y el estudio de su funcionalidad.

Análisis forense. En cuanto a la etimología de la palabra forense, se puede decir que viene del latín *forensis* ("antes del foro"), aunque en la actualidad se refiere a algo relacionado con los "Tribunales de Justicia" [9].

Como se define por Clint et al [10] y Carrier [11], la ciencia forense digital es una rama de la ciencia forense que abarca la recuperación e investigación de los materiales que se encuentran en los dispositivos digitales o generados por ellos y a menudo, en relación con delitos informáticos. En la ciencia forense, los principios científicos, métodos y técnicas se aplican a la justicia buscando el bien de la sociedad y de la seguridad pública [9]. Así pues, el forense informático es responsable de asegurar, identificar, preservar, analizar y presentar pruebas digitales de modo que se acepten en los procesos judiciales [9].

Evidencia. Se denomina así a cualquier elemento que proporcione la información, mediante el cual se pueda deducir alguna conclusión o que constituya un hallazgo relacionado con el hecho que está bajo investigación [9].

Cadena de Custodia. Consiste en un informe detallado que documenta la manipulación y el acceso a las pruebas objeto de la investigación. La información contenida en el documento debe ser conservada adecuadamente y mostrará los datos específicos, en particular todos los accesos con fecha y hora determinada [12].

Citando a Colquitt: *"El objetivo pues, de establecer una Cadena de Custodia es para convencer al Tribunal de Justicia de que es razonablemente probable que la exposición sea auténtica y que nadie ha alterado o manipulado la prueba física"* [13].

ISBN: 978-84-9717-323-0

El Instituto Nacional de Justicia de los EE.UU., define la CdC como *"un proceso que se utiliza para mantener y documentar la historia cronológica de las pruebas"*. Esto significa el control de las personas que recogen la evidencia y de cada persona o entidad que posteriormente tiene la custodia de la misma, de las fechas en las que los artículos fueron recogidos o transferidos, de la agencia y el número del caso o el nombre del sospechoso, así como una breve descripción de cada elemento [14].

En lo que respecta al tratamiento de la evidencia digital en la CdC, podemos citar la norma: "BS 10008:2008. *Especificación sobre las pruebas y admisibilidad legal de la información electrónica*, BSI British Standard" [15]. En ella se incluyen los diferentes aspectos relacionados con el tratamiento de las principales pruebas digitales.

Para probar la CdC, es necesario conocer todos los detalles sobre cómo se manejó la evidencia en cada paso del camino. La vieja fórmula utilizada por la policía, los periodistas y los investigadores de "quién, qué, cuándo, dónde, por qué y cómo" (del inglés "las cinco Ws y una H"), se puede aplicar para ayudar en la investigación forense de la información [7], [16].

Para garantizar la admisibilidad de las pruebas, es necesario prestar especial atención a los métodos y procedimientos utilizados para la obtención de las mismas, respetando no sólo los procedimientos técnicos sino también la legislación judicial y la legislación aplicable al caso. Las medidas tomadas no deben modificar las pruebas y todas las personas involucradas deben ser competentes en procedimientos forenses. Todas las actividades realizadas deben documentarse y conservarse las pruebas, de modo que estén disponibles para la repetición de exámenes con el mismo resultado. En ciertos momentos, los procedimientos podrán llevarse a cabo en presencia de un notario o secretario judicial. Las personas que están a cargo de las pruebas digitales son las responsables de las medidas adoptadas con respecto a ellas mientras estén bajo su custodia [15].

II. Estado del Arte

Marco de Gestión de la Evidencia Digital (MGED). Ćosić y Bača han propuesto el *Digital Evidence Management Framework* [7], mediante el cual es posible desarrollar un marco de gestión sencillo para el proceso de la investigación digital basado en las causas y en los efectos producidos por los eventos. Las fases se pueden organizar en función de los requisitos básicos de la investigación, es decir, habrá que encontrar la evidencia que muestre las causas y efectos de un evento y por tanto, será necesario desarrollar hipótesis sobre los hechos ocurridos en la escena del delito. Cada fase tiene un objetivo claro y los requisitos y procedimientos se pueden desarrollar en consecuencia. Como afirman Carrier y Spafford, se deberán perfilar claramente las definiciones y los conceptos que se utilicen en este marco [17].

En la Figura 1 se muestra la propuesta del concepto del MGED, que garantiza la seguridad de una cadena de custodia sobre la base de los "cinco Ws y una H" que proponen Ćosić y Bača [7]. Aconsejan utilizar una función SHA-2 (*Secure Hash Algorithm*) de la huella digital de la evidencia, una característica biométrica de autenticación e identificación para la firma digital (quién), control de fecha y hora mediante la adición de un estampado generado por una entidad de confianza (cuándo), la utilización de servicios (posicionamiento global por *GPS* y *GLONASS* y/o *Google Maps*) o algún dispositivo de *RFID* para la geolocalización (dónde) y el cifrado asimétrico para asegurar la evidencia digital (cómo).

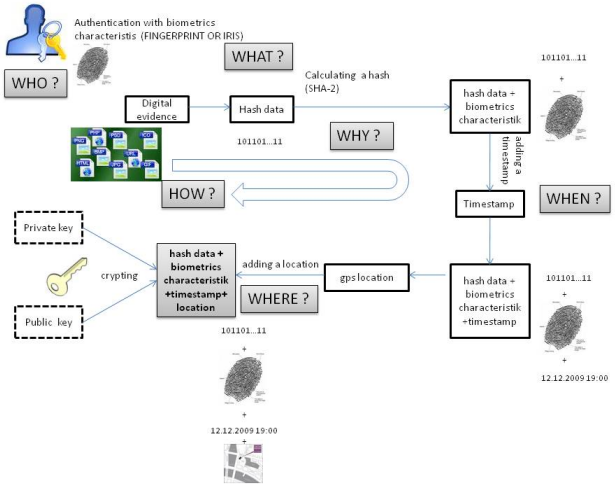

Fig. 1. MGED propuesto por Ćosić and Bača [7].

Huella de la evidencia. Ćosić y Bača proponen que no se utilice la evidencia digital original, en su lugar recomiendan que se maneje una huella digital de las pruebas [7]. Para calcular la huella digital se utilizará una función hash SHA-2, en lugar de las funciones SHA-0 ó SHA-1. Esto se hace para evitar un ataque criptográfico (colisión y/o ataque preimagen).

No hay límite del tamaño del archivo de evidencia digital para el que se desea calcular un hash. Se puede utilizar un archivo (*jpg, tiff, txt,* etc.), un grupo de archivos o algún tipo de archivo específico (*zip, rar, tar,* etc.) o incluso una unidad física (disco duro, memoria externa,etc). Al utilizar una función hash SHA-2, se dará un valor de tamaño fijo (224, 256, 384 ó 512 bits dependiendo de sí se usa SHA-224, SHA-256, SHA-384 ó SHA-512). Las huellas más utilizadas son SHA-256 y SHA-512.

Características biométricas. Ćosić y Bača plantean, con el fin de realizar la autenticación e identificar y conocer a las personas que manejan la evidencia, la utilización de las características biométricas del individuo [7]. Como pueden ser la huella de algún dedo de la mano, las características del iris del ojo, las características morfológicas de la cara, etc. El requisito previo para poder utilizar las características biométricas, es la necesidad de disponer de una base de datos de todas las personas que manejan las evidencias, entre las que se deben incluir los agentes de policía relacionados de alguna manera con el caso, los investigadores que han obtenido

las pruebas de campo, los investigadores forenses, los peritos judiciales y el personal judicial.

Estampado de tiempo. Ćosić y Bača recomiendan para conocer el momento en el tiempo en el que se descubre la evidencia y han sucedido los acontecimientos y acciones, una estampación digital del tiempo utilizando una fuente de confianza conocida [7].

Otros autores como Willassen [18], indican que también es posible el uso de métodos correlativos de sello de tiempo almacenado en el sistema de adquisición y que ya fueron creados por otros sistemas (por ejemplo, mediante la fecha y hora de páginas web generadas dinámicamente).

Gayed et al [4] citan la "web semántica" como solución flexible para simbolizar la diferente información, ya que proporciona los lenguajes de marcas semánticas (*markup*) para la representación de los datos con el apoyo de diferentes vocabularios. Estas características pueden ser explotadas para mostrar el documento tangible de la CdC que asegura su fiabilidad e integridad. Por otra parte, pueden incluirse también los mecanismos de consulta de los datos representados para responder a diferentes cuestiones forenses y de procedencia, formuladas por los jurados sobre el caso tratado.

Ćosić y Bača proponen que el método para esta fase sea un "tiempo de estampado de confianza" [8]. El estándar "RFC 3161" define que la marca de tiempo de confianza es un sello de tiempo emitido por una Autoridad de Certificación (*Trusted Third Party, TTP*), que actúa como una Autoridad de Sellado de Tiempo (*Time Stamping Authority, TSA*) [19]. Cuando se obtiene la evidencia digital, el marco de gestión envía una solicitud a la *TSA* para obtener un certificado de sello de tiempo de confianza. En este proceso hay que tener un acceso al sistema de gestión de la *TSA*, o podemos desarrollar un sistema interno con la infraestructura de la *TSA*. Es imprescindible mencionar que en este tipo de "sistema de tiempo" deben existir unos "auditores externos" que actúan como testigos [7].

Geolocalización. Ćosić y Bača indican que se debe determinar el lugar exacto donde se maneja la evidencia digital y dónde se ha manipulado [7]. Actualmente en los EE.UU. algunos organismos utilizan la tecnología de *RFID* (*Radio Frequency IDentification*), para hacer un seguimiento de la evidencia durante su ciclo de vida. A pesar de que con *RFID* se puede hacer un seguimiento de una evidencia digital, no se pueden conseguir las coordenadas (localización). Por este motivo, otros autores como Strawn [20], recomiendan el uso de un Sistema de Posicionamiento (*GPS* o *GLONASS*) para efectuar la recogida e investigación de las evidencias.

Respecto a la utilización de etiquetas *RFID*, podemos asegurar que es muy práctica en la clasificación y almacenamiento de la evidencia física, como por ejemplo en los depósitos judiciales, porque si se pierde el documento de control es posible encontrar la evidencia. Pero lo ideal es que la evidencia digital incorpore los datos de geolocalización en los metadatos, tal y como se propone en el presente trabajo.

Cifrado asimétrico. Para una seguridad mayor, Ćosić y Bača se refieren a un cifrado asimétrico [7]. La evidencia digital y el valor obtenido se cifrarán con la clave privada recibida de la Autoridad de Certificación y se almacena para su uso posterior. Todo el proceso se representa en la Figura 1.

III. Nuestra propuesta

Propuesta de creación y transmisión de la evidencia digital. Se muestra en la Figura 2 y se basa en el método de los "Cinco Ws y una H" [7], [16].

Ćosić y Bača [7] proponen el uso de la identificación biométrica de la persona que se encarga de la captación de las pruebas, como la mejor forma de referencia. Aunque en las aplicaciones de *Smartphones* su uso está limitado, en la actualidad, se está comenzando a crear aplicaciones para *Android* que detectan el iris del ojo o incluso la huella dactilar en la identificación personal y su posterior uso como medio de pago. Así, en un futuro próximo no será necesario el *PIN* (*Personal Identification Number*) para desbloquear los sistemas como hasta ahora y se aplicará en su lugar la identificación biométrica.

En la identificación sí es posible aplicar el número *IMEI* (*International Mobile Equipment Identity*) del teléfono, así como el número de teléfono asociado a la tarjeta *SIM* (*Subscriber Identity Module*). Debido a la legislación antiterrorista aplicada en la mayoría de los países, los números de teléfono asociados a las tarjetas *SIM* identificarán al propietario.

Para determinar el lugar donde se genera la evidencia digital es necesario el uso de la geolocalización. Para ello, la forma más precisa es mediante el uso de satélites. Hasta hace poco sólo era posible utilizar la constelación de satélites norteamericanos *GPS*, pero a partir de los últimos años también se puede utilizar en combinación los rusos *GLONASS* y, en un futuro próximo, también se podrá utilizar la constelación europea *Galileo* o *GNSS* (*Global Navigation Satellite System*). Si en la actualidad la identificación de la posición se realiza con un error máximo entre 2 y 3 metros, próximamente gracias a la exactitud será de centímetros. Así mismo, el uso de datos cifrados *GNSS PRS* (*Public Regulated Service*) en la geolocalización por parte de los investigadores policiales podrá evitar la posibilidad de ataques *jamming* y *spoofing* mediante interferencias.

La utilización de redes *WiFi* será limitada a *WiFi WPA2 PSK* con clave robusta no contenida en diccionario, que junto a la utilización de redes de telefonía 3G/4G podrán proporcionar geolocalización *"indoor"* mediante el servicio de Google, incluso como verificación de que la localización *"outdoor"* por satélite no está siendo atacada, dentro de los márgenes lógicos de inexactitud del servicio de Google.

Además, existe otra posibilidad de asegurar la geolocalización de las pruebas. Si el dispositivo móvil está conectado a una red de telefonía *GSM*, el proveedor de servicios tiene un registro de las conexiones entre el dispositivo y las antenas en la zona, por tanto el dispositivo está geolocalizado. El problema del uso de estos datos está en que es necesaria

una orden judicial para que el proveedor de servicio de datos telefónicos pueda facilitar la información en una investigación (solicitud de prueba anticipada) [21].

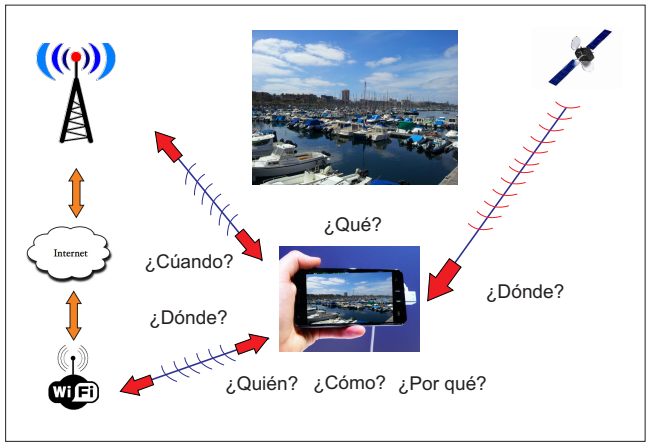

Fig. 2. Propuesta de creación y transmisión de la evidencia digital.

Para generar la evidencia, tal como se muestra en la Figura 2, en primer lugar la cámara debe estar activada en el dispositivo. De este modo se obtiene una fotografía por una persona identificada y cualificada (tanto a nivel técnico como jurídico, normalmente un miembro de las Fuerzas de Seguridad del Estado), para así poder obtener unas pruebas válidas que podrán ser utilizadas en las actuaciones judiciales posteriores. En caso de que el dispositivo se encuentre bajo el área de cobertura de los satélites o con acceso seguro a Internet, la prueba obtenida podrá ser geolocalizada. Una vez obtenida la evidencia con sus respectivos metadatos (datos asociados), se obtiene una huella digital que es enviada de manera segura (con cifrado *SSL/TLS* por el puerto 443) a una *TSA*, la cual devuelve otro archivo (por el mismo enlace seguro) con el "tiempo de confianza de estampado" como está definido en el estándar "RFC 3161", junto con la evidencia que indica la certificación, mediante la fecha y hora de envío.

Propuesta de creación del paquete de evidencia. El paquete estará formado por un archivo *zip* en cuyo interior contendrá los ficheros de evidencias (fotografías, audios y videos), los ficheros devueltos por la *TSA* (en formato *p7s*) y el fichero "documento de pruebas y control de cambios".

Con el fin de garantizar la CdC, es esencial mantener copias de seguridad tanto del paquete de evidencia recibido como del enviado, en dispositivos físicos externos. Así, en caso necesario y a requerimiento de los investigadores forenses, será posible determinar el punto de ruptura de la cadena de custodia y el momento a partir del cual la evidencia deja de ser válida, pero se evita su anulación.

El diseño de la CdC debería ser genérico y no debe limitarse al tamaño de las evidencias, cuyo valor puede ser desde unos pocos *MBytes* (fotografías, audios, etc.) hasta valores de *TBytes* (discos duros). Aunque para ficheros pequeños es posible su transmisión por correo eléctrónico, la forma más segura de envío es a través de un servidor *SFTP* (*Secure File Transfer Protocole*) o un *FTPS* (*FTP-SSL*) que proporcionen acceso remoto y, sobre todo, seguro. Aunque en los dos protocolos se recurre al algoritmo asimétrico (*RSA*, *DSA*), algoritmo simétrico (*AES*), y un algoritmo de intercambio de claves, para la autenticación del *FTPS* utiliza certificados X.509, mientras que *SFTP* utiliza las claves *SSH*. Por otro lado, aunque *SFTP* es más avanzado que *FTPS*, algunos dispositivos pueden no ser compatibles con *SFTP* (como los móviles, consolas etc) y sin embargo con *FTPS* sí lo son.

La posibilidad de que la evidencia sea interceptada (*phishing*, ataques al servidor, etc) hace que sea muy conveniente su cifrado, por lo que se propone *AES* 128 o, preferiblemente, 256 bits [22], [23].

Mediante una herramienta alojada en la Web segura (para prevenir ataques *wiretapping* y *man-in-the-middle*) de la compañía *DigiStamp* que actúa como *TSA* (*https://www.digistamp.com*), se obtienen las huellas digitales (SHA-2, 256 ó 512bits). La *TSA* crea un archivo con el mismo nombre que la evidencia y extensión *p7s*, que es un "PKCS#7 Signature" (*Public-Key Cryptography Standard*), de acuerdo con la sección 3.2 del "RFC 2311" [24]. La huella digital se almacena en la base de datos de la *TSA* y devuelve al emisor el archivo de extensión *p7s*. La *TSA* vía herramienta alojada en su página web, ofrece la posibilidad de comprobar en el futuro la fecha y la hora de certificación del archivo (a modo de herramienta de auditoría).

Como cada vez que se envía a la *TSA* una solicitud de sello de tiempo se genera un archivo de extensión *p7s*, es posible el análisis forense de la CdC mediante el estudio de la correlación temporal de archivos.

Análisis de funcionalidad del paquete de evidencia. Se trata de demostrar que mediante un teléfono móvil inteligente o *Smartphone* (o Tableta, *Smartcamera*, etc), es posible obtener evidencias digitales, así como definir e iniciar una CdC.

Mediante el análisis de los metadatos asociados con la evidencia (datos contenidos en el archivo de imagen intercambiable, *Exif*), es posible analizar con más detalle las características de la prueba:

- Título de la prueba. Es conveniente no modificar el nombre que de forma automática genera el *Smartphone*, ya que incluye la fecha y hora de la adquisición de la prueba.
- Tipo de archivo de la prueba. Permite identificar si se trata de un archivo de audio, vídeo o imagen fotográfica.
- Fecha y hora de la captura de la evidencia.
- Carpeta donde la evidencia se guarda en el *Smartphone*.
- Nombre del lugar en donde se obtuvo la evidencia. Se basa en el sistema de geoposicionamiento *Google*, por tanto, es esencial que la opción esté habilitada en el sistema operativo y *3G/4G* o cobertura *WiFi WPA2 PSK* con clave robusta no contenida en diccionario.
- La geolocalización de la prueba (latitud y longitud), basada en el dispositivo *GPS* y/o servicio de *Google*.

- Tamaño de la evidencia, válido para indicar el camino a seguir en el tratamiento y la mejor manera de enviar la información.

- Resolución del archivo de imagen. Muestra la calidad de la información de las pruebas.

- La localización del archivo en la estructura de ficheros de la memoria del *Smartphone*: datos necesarios con el fin de tratar el archivo denominado "paquete de evidencia".

GPS	
Referencia de latitud GPS	Latitud norte
Latitud GPS	28.124170' 0"
Referencia de longitud GPS	Longitud oeste
Longitud GPS	15.424470' 0"
Referencia de altitud GPS	Nivel del mar
Altitud GPS	34.5 m
Marca de fecha y hora GPS	15:13:43
Método de procesamiento GPS	(41,53,43,49,49,00,0...
Marca de fecha GPS	2013:05:05
Misceláneo	
Versión Exif	2.2
Nota del fabricante	(05,00,01,00,07,00,0...
Versión de FlashPix	1.0
ID Versión GPS	(2,2,0,0)

Fig. 3. Detalle del fichero *Exif* del GPS.

La mayor parte de los datos incluidos en los metadatos se pueden utilizar al generar la información en el documento de pruebas y de control de cambios. La Figura 3 muestra los detalles del fichero *Exif* generado en la utilización del *GPS*.

Lo mismo sucede con la posición exacta para localizar el punto de adquisición de las pruebas. La mejor manera de confirmar dicho lugar es mediante el uso de *GPS*, pero tiene el inconveniente de sólo ser posible si el satélite es visible, ya que si no la información será aproximada.

Una vez que se ha obtenido la prueba y se han extraído los datos de identificación, es posible cifrar la evidencia. Para ello se puede recurrir al uso de aplicaciones de cifrado *AES* de al menos 128 bits.

Con la evidencia cifrada, será necesario enviar de manera segura el fichero a una *TSA* que proporcione un servicio de notaría electrónica. Si se utilizan los servicios de *DigiStamp*, se obtiene a nivel local una huella del tipo SHA-256 o SHA-512 bits. En cualquier momento se podrá verificar que el sello de tiempo ha sido generado por la *TSA*, así como el momento de generación.

Hay que señalar tres desventajas detectadas:

- La certificación es sólo para el momento en que se envía el archivo a la *TSA*, pero no indica la hora de la generación de evidencia.

- El trabajo de campo en el sitio web *DigiStamp* es imposible, ya que no está diseñado para funcionar en dispositivos móviles y no funciona con cualquier navegador (*Android, Opera, Firefox, Chrome*, etc.). Por lo tanto, es necesario transferir la información a un ordenador personal y utilizar un navegador de Internet.

- El servicio tiene un costo por fichero. Por dicho motivo, se podría crear algún sistema que funcionara directamente para nuestro propósito.

Documento de pruebas y control de cambios. Existen varias opciones para el formato del mismo (texto plano, *xml, doc*, etc.) La propuesta de este trabajo, por su sencillez y universalidad, es de texto plano. El documento deberá contener, como mínimo:

- Nombre detallado de la persona que adquiere la evidencia, la posición, la razón, el lugar, la hora y la fecha, las autorizaciones, el nombre de las evidencias y los nombres de los ficheros de sellado de tiempo (archivos *p7s*).

- Nombre detallado, la posición, la razón, la ubicación, la hora y fecha de cada persona a la que se envía el documento en la CdC.

- La certificación en clave asimétrica del documento completo, con indicaciones de principio y fin.

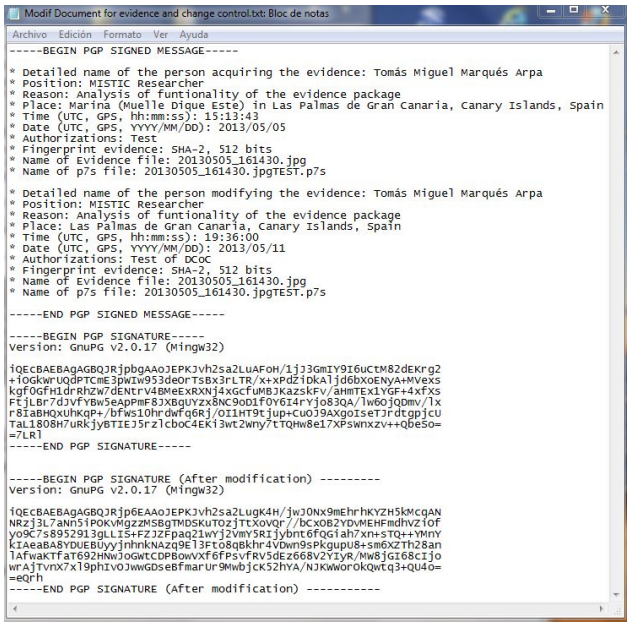

Fig. 4. Documento de pruebas y de control de cambios.

La Figura 4 es un ejemplo del documento, que ha sido firmado con una clave *RSA* asimétrica de 2048 bits, utilizando el programa *GnuPG* versión v2.0.1 para Windows 7. La aplicación del programa será necesaria cada vez que el documento avance en la CdC y se hagan modificaciones a firmar.

Propuesta de una aplicación en *Android*. Consiste en la creación de una aplicación para teléfonos móviles inteligentes. Debe ser capaz de capturar la evidencia, crear el paquete de evidencia y realizar envíos de correo electrónico o a un servidor seguro *SFTP* o *FTPS*.

La aplicación ha de tener en cuenta los componentes del equipo que necesiten ser activados. Una vez que la evidencia ha sido capturada, la aplicación será capaz de cifrar, realizar una conexión segura a una *TSA* y obtener los archivos *p7s*. Con la ayuda de los metadatos, será capaz de generar el documento de pruebas y de control de cambios, que estará firmado utilizando una clave asimétrica *RSA* de 2048 bits.

Al final ha de ser capaz de generar un archivo comprimido de la evidencia, formado por la propia evidencia, el archivo

p7s y el documento de pruebas y de control de cambios. Este fichero es el paquete de evidencia. Finálmente, el resultado deberá estar listo para ser enviado por email o preferentemente a un servidor seguro *SFTP*.

IV. Conclusiones y trabajos futuros

Este trabajo ha sido desarrollado con la intención de crear un método válido de CdC. En un principio la idea era sólo crear la cadena, pero con posterioridad se comprobó que ésta debía tener un punto de partida: la generación de la evidencia. Y fue allí donde se ha hallado lo que posiblemente sea el punto más débil de ella.

Por lo tanto, ¿se debe seguir un guion en la adquisición de pruebas para asegurar que se procede de manera correcta? La respuesta es que no. La tecnología actual puede permitir la automatización de ciertas tareas y rutinas, que es la propuesta principal de este trabajo mediante la creación de una herramienta que automatice el proceso en la parte más débil de la cadena: la correcta adquisición de la evidencia. Posteriormente, la prueba debe ser protegida de las mayores amenazas que se han detectado: *spoofing*, *jamming*, *phishing*, *man-in-the-middle*, *wiretapping*, colisión y preimagen. Para evitar esto y sobre todo, para que no se pueda modificar fácilmente la evidencia sin dejar rastros, se ha propuesto un método de trabajo.

Las dos cuestiones planteadas en las preguntas y objetivos de investigación: ¿es posible desarrollar un nuevo método para la Cadena de Custodia? y, ¿el nuevo método puede ser implementado? La respuesta es afirmativa en ambos casos, como se ha demostrado.

Principalmente los trabajos de mejora se pueden centrar en los siguientes aspectos:

- Creación de una aplicación *Android* en la forma propuesta.
- Diseño de un dispositivo hecho en una plataforma del tipo *"Raspberry Pi"* o *"BeagleBone Black"* (pequeños ordenadores de muy bajo coste que admiten conexión de periféricos) y que pueden ofrecer otras posibilidades en la creación de las CdC mediante la utilización de imágenes en lugar de huellas, y que por tanto eviten la recusación de una evidencia por la degeneración del soporte físico que la contiene.
- Uso de la identificación biométrica de los usuarios de acuerdo con el progreso técnico.
- Utilización de geolocalización lo más precisa y segura posible con la incorporación de datos de posicionamiento cifrados GNSS-PRS
- Uso de datos de la tarjeta *SIM* para proporcionar la identificación del usuario.
- Realización de ciberataques a la propuesta con el fin de demostrar su debilidad o su fortaleza.

Agradecimientos

This work was partly funded by the Spanish Government through projects: TIN2011-27076-C03-02 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES".

Referencias

[1] European Commission C-4536. "Líneas de investigación de la Comisión Europea para 2013". Cooperación, tema 10, seguridad. Área material: 10.1.4. Delincuencia común y forense - Topic SEC-2013.1.4-2.- *Desarrollo de un Marco Común Europeo para la aplicación de las nuevas tecnologías en la recopilación y el uso de la evidencia*, julio 2012.

[2] V. Vaishnavi, W. Kuechler. "Design research in information systems", 2004 (revisión octubre 2013). Disponible en http://desrist.org/design-research-in-information-systems/.

[3] B. J. Oates. "Researching information Systems and Computing". SAGE Publications Ltd. London, 2006, (revisión 2013).

[4] T. F. Gayed, H. Lounis, M. Bari. "Cyber Forensics: Representing and (Im)Proving the Chain of Custody Using the Semantic web". *COGNITIVE 2012: The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 2012.

[5] G. Giova. "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems". *International Journal of Computer Science and Network Security*, vol. 11, no. 1, 2011.

[6] S. L. Garfinkel. "Providing cryptographic security and evidential chain of custody with the advanced forensic format, library and tools". Naval Postgraduate School & Harvard University, USA, 2011.

[7] J. Ćosić, M. Bača. "A Framework to (Im)Prove "Chain of Custody" in Digital Investigation Process". *Proceedings of the 21st Central European Conference on Information and Intelligent Systems*, 2010.

[8] J. Ćosić, M. Bača. "(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp". Universidad de Zagreb, 2010.

[9] M. Colobrán. "Análisis Forense de la Información". *Conceptos básicos*. MISTIC. Universitat Oberta de Catalunya, 2012.

[10] M.R. Clint, M. Reith, G. Gunsch. "An Examination of Digital Forensic Models", 2002.

[11] B.D. Carrier. "Defining Digital Forensic Examination and Analysis Tools". *International Journal of Digital Evidence*, 2002.

[12] P. G. Bradford, D. A. Ray. "An Online Algorithm for Generating Fractal Hash Chains Applied to Digital Chains of Custody". *Intelligence and Security Informatics 2007 Conference (ISI 2007)*.

[13] J. A. Colquitt. "Alabama Law of Evidence". The Mitchie Company–Law Publishers, Charlottesville, VA, 1990.

[14] National Institute of Justice, USA. "Crimes Scene Guides", 2011 (acceso febrero 2014). Disponible en http://www.ojp.usdoj.gov/nij/topics/law-enforcement/investigations/crime-scene/guides/glossary.htm.

[15] A. Guash. "Análisis Forense de la Información". *El informe pericial. Análisis forense y sistema legal*. MISTIC. Universitat Oberta de Catalunya, 2012.

[16] J. Tallim. "Deconstructing Web Pages". *Media Smarts*, 2012 (accesso febrero 2014). Disponible en http://mediasmarts.ca/.../deconstructing-web-pages-lesson.

[17] B. D. Carrier, E.H. Spafford. "An Event-Based Digital Forensic Investigation Framework". *DFRWS*, 2004.

[18] C. Willassen. "Hypothesis based investigation of Digital Time Stamp". *FIP, Advanced in Digital Forensic IV*, pp.75–86, 2008.

[19] S. Vanstone, P. van Oorschot, A. Menezes. "Handbook of Applied Criptografy". CRC Press, 1997.

[20] C. Strawn "Expanding the Potential for GPS". *Evidence Acquisition, Small Scale digital evidence Forensic Journal*, vol.3, no.1, 2009.

[21] J. L. García Rambla. "Un forense llevado a juicio". *Prueba anticipada en un proceso civil*, cap.7. Flu-Proyect y Sidertia Solutions, *Creative Commons*, 2013.

[22] NIST 197. "Advanced Encryption Standard (AES)". *Federal Information Processing Standards. Special Publication 197*. National Institute of Standards and Technology (NIST), Maryland, USA, 2001.

[23] Blue Book. "Recommendation for Space Data System Standards". *CCSDS Cryptographic Algorithms Recommended Standard CCSDS 352.0-B-1*. CCSDS Secretariat. Space Communications and Navigation Office. NASA Headquarters, Washington, USA, 2012.

[24] S. Dusse, USSE, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka "RFC 2311". *S/MIME Version 2 Message Specification*. ISOC, Virginia, USA, 1998.