Revista ACTIVA, ISSN 2027-8101. Núm 3, enero-junio 2012, pp. 67-81
Tecnológico de Antioquia, Medellín (Colombia)

La cadena de custodia informático-forense

Computer forensics chain of custody

Luis Enrique Arellano
Ing. Informático-Abogado-Licenciado en Criminalística
Universidad Tecnológica Nacional-Argentina

Carlos Mario Castañeda
Ingeniero de Sistemas MsC
Tecnológico de Antioquia

Recibido: 1 de marzo 2012
Aprobado: 1 de abril 2012

Resumen

La cadena de custodia tiene como finalidad brindarle soporte veraz a la prueba digital ante el juez, en medio de lo que se conoce como el debido proceso. Por tal motivo deben establecerse los procedimientos indicados para garantizar la idoneidad de los métodos aplicados para la sustracción de la evidencia informática. Así se garantiza una base efectiva para el juzgamiento y la validez ante cualquier fuero judicial internacional. Para esto, es necesario que se eviten suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción (común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Procedimiento controlado y supervisable, la cadena de custodia informático-forense se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su

Valoración por los encargados de administrar justicia. Este artículo lista los procedimientos en cada caso de recopilación de evidencia informática.

Palabras claves: Cadena de custodia, informática forense, validez de la prueba.

Abstract

The aim of the chain of custody is to provide digital evidence with a truthful stand before the judge, by following the established course of law. Thus an effective ground for judgment and validity before any other international court are guaranteed. To do that, it is important to avoid any forgery, modification, tampering or destruction of evidence (be it delete or denial of service). A controlled and monitorable procedure, the computer forensic chain of custody is applied to material and virtual evidence related to a criminal event or otherwise, from its finding all the way up to its appraisal. This paper lists all the procedures to be followed to gather computer evidence for forensic applications.

Keywords: Chain of custody, computer forensics, validity of evidence.

La preservación de la cadena de custodia sobre la prueba indiciaria criminalística es obligación de la totalidad de los miembros del poder judicial, los operadores del derecho y sus auxiliares directos. Entre estos últimos debemos incluir el personal de las fuerzas de seguridad, la policía judicial y el conjunto de peritos oficiales, de oficio y consultores técnicos o peritos de parte.

Así, la implementación de mecanismos efectivos de recopilación de evidencias debe incluir procedimientos que aseguren la confiabilidad de la información recolectada. Dicha confiabilidad incluye la trazabilidad, *(Establecer un mecanismo que permita realizar un seguimiento estricto de los elementos probatorios, desde su detección hasta el momento de su disposición definitiva)* la confidencialidad, la autenticidad, la integridad y el no repudio de los datos. En términos sencillos, implica establecer mecanismos de garantía de que los elementos probatorios ofrecidos como prueba documental informática son confiables, es decir, que no han sufrido alteración o adulteración alguna desde su recolección.

1. La cadena de custodia informático-forense

El juez debe poder confiar en dichos elementos digitales, por considerarlos auténticos "testigos mudos", desde el punto de vista criminalístico clásico y evaluarlos en tal sentido, guiado por la sana crítica, la prueba tasada o las libres convicciones, según sea el caso y la estructura judicial en que se desarrolle el proceso. Desde la detección, la identificación, la fijación, la recolección, la protección, el resguardo, el empaque y el traslado de la evidencia del lugar del hecho real o virtual, hasta la presentación como elemento probatorio, la cadena de custodia debe garantizar que la evidencia recolectada en la escena es la misma que se está presentando ante el evaluador o decisor.

Consideramos la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración, por parte de los encargados de administrar justicia y que busca asegurar la inocuidad y la esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.

Con este fin es necesario establecer un riguroso y detallado registro, que identifique la evidencia y sus poseedores, indicando el lugar, la hora, la fecha, el nombre y la dependencia involucrada en el secuestro, la interacción posterior y su depósito en la sede que corresponda (judicial o no).

Si carece de alguno de estos componentes, la prueba documental informática recolectada no habrá alcanzado el valor probatorio pretendido. Es importante considerar el valor de los indicios recabados en el proceso de investigación, análisis y argumentación del cual dependen. En este marco de referencia adquirirán relevancia y pertinencia; de ahí la necesidad de evitar en lo posible la impugnación de los mismos en razón de errores metodológicos propios de cada disciplina en particular, pues no es igual la cadena de custodia de muestras biológicas que la de armas o documentos impresos o virtuales. Por ejemplo, un acta de secuestro es un elemento genérico, pero el asegurar la integridad de la prueba mediante un digesto (Hash) sobre un archivo secuestrado es un elemento propio de la cadena de custodia informático-forense.

La prueba documental informática tiene características particulares que requieren tratamiento particular en la recolección, la preservación y el traslado. Estos son:

1. Consiste en indicios digitalizados, codificados y resguardados en un contenedor digital específico, es decir, toda información es almacenada (aun durante su desplazamiento por una red, está almacenada en una onda electromagnética).

2. Hay diferencias entre el objeto que contiene la información (discos magnéticos, ópticos, cuánticos, ADN, proteínas, etc.) y su contenido —la información almacenada—. Para este caso consideramos:

a. Información: Todo conocimiento referido a un objeto o hecho, susceptible de codificación y almacenamiento.

b. Objeto: Conjunto físicamente determinable o lógicamente definible.

3. La información puede presentarse en uno de los siguientes estados:

a. En almacenamiento: se encuentra en un reservorio a la espera de ser accedida (almacenamiento primario, secundario o terciario). Es un estado estático y conforma la mayoría de las recolecciones posibles; sin embargo, difiere de la mayoría de los indicios recolectables a la que puede accederse por medios locales o remotos.

b. En desplazamiento, es decir, viajando en un elemento físico determinado (cable, microonda, láser, etc.). Es susceptible de recolección mediante interceptación de dicho elemento y está condicionada por las mismas cuestiones legales que la escucha telefónica o la violación de correspondencia.

c. En procesamiento: es el caso más complicado y constituye la primera decisión que debe tomar el recolector. Ante un equipo en funcionamiento, donde la información está siendo procesada, es decir, modificada, actualizada y nuevamente resguardada, debe decidir si apaga o no el equipo. Esta decisión es crítica y puede implicar la pérdida de información y la destrucción de la prueba documental informática pretendida. *Es una decisión incierta. Si se decide mantener el equipo encendido, se corre el riesgo de haber sido detectado durante su aproximación al mismo, y que en realidad la actividad del mismo esté consistiendo en borrar de manera segura cualquier información almacenada (usando técnicas específicas de eliminación de la información que la hacen irrecuperable a los métodos informático-forenses), con lo que cuanto más tiempo permanezca el equipo funcionando mayor será el daño producido. Si, por el contrario, se decide apagar el equipo, es posible que el mismo tenga un mecanismo de seguridad ante estos eventos que dispare las mismas acciones de borrado detalladas, sobre los equipos remotos, eliminando enlaces y reservorios dentro de la misma red o en redes externas (es muy común que, con fines delictivos o no, la información sea almacenada en un reservorio remoto, lo que aumenta la seguridad y confiabilidad de la misma, ya que está exenta de los riesgos edilicios, físicos y lógicos, del local donde se utiliza). La mejor manera de solucionar este problema es la labor de inteligencia previa (ataques pasivos, consistentes en intercepción, escucha o análisis de tráfico, por medios remotos). Esta tarea resuelve el problema, pero demanda recursos técnicos y, sobre todo, humanos sumamente escasos. Por otra parte, debe ser autorizada judicialmente y la práctica nos indica que la mayoría de los Juzgados, por muy diversas causas, son sumamente reacios a autorizar estar intervenciones (lo mismo ocurre con las clásicas y siempre restringidas medidas previas o preliminares, aunque constituyan prueba anticipada y reúnan las condiciones requeridas para la misma: peligro en la demora, credibilidad del derecho invocado* —fumus bonis iuris— *y contracautela de privacidad).* La solución por medio del acceso remoto, indetectable por el accedido, es un tema que aún no se encuentra en discusión en nuestro país. *(Con los medios adecuados es perfectamente posible acceder a un equipo remoto y recolectar la información pretendida, preservando las condiciones legalmente establecidas en la Constitución Nacional y sus normas derivadas. Sin embargo, en un ambiente donde la diferencia entre el delito informático impropio (delitos clásicos cometidos utilizando medios informáticos) tipificado en la Ley 26.388 y el delito informático propio (que afecta al bien jurídico protegido: "información", algo que ni siquiera está contemplado en nuestro Código Penal) es un que solo manejan algunos*

ISSN 2027-8101, No. 3, enero-junio 2012

operadores del derecho especializados en derecho de alta tecnología, parece utópico esperar comprensión real de las particularidades que identifican al lugar del hecho virtual (propio e impropio) respecto del lugar del hecho real, en el campo jurídico en el mediano plazo).

El significado de la prueba depende de su inserción como elemento pertinente y conducente a la argumentación presentada como sustento de la pretensión jurídica manifestada. Esto sugiere que constituye un documento más, diferente de la prueba documental clásica (bibliográfica, foliográfica y pictográfica) únicamente en el soporte (digital vs. papel). Sin embargo, es necesario tener en cuenta que un bit no es similar, sino idéntico a otro bit. De ahí que una copia bit a bit de un archivo digital es indiferenciable de su original, esto significa que no puede establecerse cuál es el original y cuál su copia, salvo que hayamos presenciado el proceso de copiado y tengamos conocimiento sobre cuál era el contenedor del original y cuál el de la copia (método indirecto e independiente de los archivos considerados). Esto no resulta un inconveniente, sino más bien una ventaja desde el punto de vista de la cadena de custodia, ya que permite preservar las copias, manteniendo el valor probatorio del original y evitando riesgos para el mismo. Se puede entregar al perito una copia de los archivos debitados y preservar los mismos en su reservorio original en el local del tribunal y con las seguridades que este pueda ofrecerle (caja fuerte, por ejemplo). *(Si un documento en papel es reservado en secretaría, en la caja fuerte y luego se le debe realizar una pericia caligráfica, debe ser entregado al perito, porque sólo puede trabajar sobre originales. Esto implica la salida de la prueba, abandonando la protección del Tribunal, hasta que regrese al mismo, si durante ese desplazamiento es destruido en forma dolosa o culposa, la prueba se pierde. En cambio si la documental informática es resguardada en el tribunal (por ejemplo en un CD o DVD) y al perito se le entrega una copia de la misma, podrá realizar su tarea sin inconveniente y si su copia es destruida, en nada afecta al original resguardado en el Juzgado).*

Por el contrario, en la recolección física de prueba indiciaria tradicional, se secuestra el indicio y se lo traslada. En la recolección de documentación informática esta acción puede realizarse o no, ya que es suficiente con copiar bit a bit la prueba y luego trasladar dicha copia. Es una extensión del caso anterior, donde no es necesario entregar el original al perito, sino que alcanza con una copia. La recolección de prueba, mediante copia debidamente certificada, puede sustituir perfectamente al original; es aplicable a los casos en que la información esté almacenada en reservorios vitales para la operación de una determina entidad u organización estatal o privada.

Supongamos la necesidad de secuestrar información almacenada en uno de los servidores operativos del Banco Central, es evidente que el secuestro de dicho servidor, podría sacar de operación a la entidad con las consecuencias que dicho hecho implicaría, mientras que su copia, certificación mediante hash y ante la autoridad judicial, administrativa o notarial correspondiente, en nada afectaría a la continuidad del servicio y serviría perfectamente como elemento probatorio.

Los mecanismos de certificación digital (*hash*, firma electrónica, firma digital) son mucho más confiables y difíciles de falsificar que los mismos elementos referidos a la firma y certificación ológrafas. Sin embargo, el desconocimiento de los operadores del derecho ante el nuevo mundo virtual hace que tengan sensaciones de inseguridad sin sustento en la realidad matemática que brinda soporte a los mecanismos referidos. Por tal motivo, se adopta una actitud sumamente crítica y negativa frente a la seguridad que los mismos brindan, en parte como consecuencia de la necesidad implícita de confiar en algoritmos que no se conocen. Entender, comprender y analizar un algoritmo de cifrado por clave pública, es una tarea de expertos y que no está al alcance de una formación matemática básica como la que posee la mayoría de los operadores del derecho. Por otra parte, el individuo inserto en la sociedad

tiende más a confiar en la medicina (por eso no cuestiona los métodos del médico legista o del psiquiatra forense) que la matemática, con la que se relaciona mucho menos. *(Las posibilidades reales de ser engañados al comprar un libro por internet son mucho menores que sus similares ante un vendedor ambulante. Sin embargo, sentimos cierta aprensión al ingresar el código de seguridad de nuestra tarjeta de crédito para confirmar la compra, algo que ocurre mucho menos con los jóvenes y los adolescentes; es un problema generacional que se superará con el paso del tiempo).* Es un proceso lento de aceptación, que como todo en derecho seguramente llegará a posteriori del desarrollo social y tecnológico.

Como se indicó anteriormente, la cadena de custodia informático-forense tiene por objeto asegurar que la prueba ofrecida cumple con los requisitos exigibles procesalmente para la misma, y por ello debe garantizar:

1. Trazabilidad:
    a. Humana (determinación de responsabilidades en la manipulación de la prueba, desde su detección y recolección hasta su disposición final).
    b. Física (incluyendo la totalidad de los equipos locales o remotos involucrados en la tarea, sean estos de almacenamiento, procesamiento o comunicaciones).
    c. Lógica (descripción y modelización de las estructuras de distribución de la información accedida y resguardada).
2. Confiabilidad (integridad, autenticidad, confidencialidad, no repudio).

Cadena de custodia vs. privacidad

La cadena de custodia se constituye de hecho en un elemento que permite asegurar la confiabilidad de la información recolectada, que si bien implica la trazabilidad de la misma, no protege por sí sola al derecho a la privacidad. Este componente asegura que la prueba recolectada se pueda seguir metodológica y procesalmente desde su origen hasta su disposición final, pero nada dice respecto de la legalidad de la misma, mucho menos de su legitimidad.

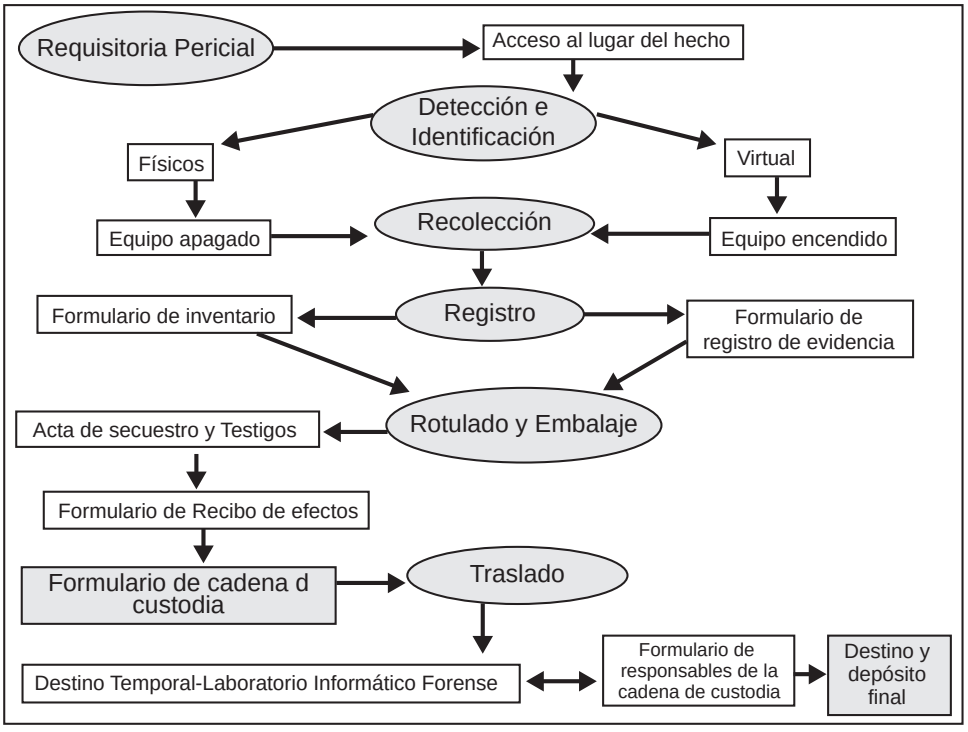
En efecto, la protección de la privacidad de la información no se conforma de manera exclusiva con la cadena de custodia. La privacidad requiere por supuesto confiabilidad, pero también respeto estricto de las normas procesales que resguardan el legítimo proceso asegurado constitucionalmente. Podríamos estar en presencia de una cadena de custodia bien realizada, con una trazabilidad adecuada, con preservación estricta criminalística, informática y procesal, pero que se haya realizado a partir de una acción ilegal o ilegítima. La condición de ilegalidad podría darse por falta de orden de allanamiento y secuestro previas a la recolección de prueba documental informática en una causa penal, y la ilegitimidad en el caso de la recolección de información propia, que excede los límites de lo permitido, accediendo no solo a la información estrictamente necesaria para asegurar la argumentación ofrecida, a efectos de justificar la pretensión litigada, resguardando otros elementos que nada tienen que ver con dicha cadena argumental-causal.

Protocolo para la cadena de custodia en la pericia informático-forense

La informática forense debe cumplir los requisitos generales establecidos en la inspección judicial en criminalística. En esta especialidad, los elementos dubitados pueden ser de tipo físico o virtual. En el caso de los elementos virtuales, la detección, la identificación y la recolección deberán efectuarse en tiempo real, es decir, en vivo, con el equipo encendido. La información es un elemento intangible que se encuentra almacenado en dispositivos que pueden ser volátiles o no. Con el fin de determinar la validez de la información contenida en los mencionados dispositivos será necesario efectuar la correspondiente certificación matemática por medio de un digesto o *hash*. Esta

comprobación es la que permitirá determinar la integridad de la prueba recolectada y su correspondencia con el elemento original.

El objetivo principal es preservar la evidencia. Por lo tanto, al acceder al lugar del hecho deberá: 1) identificar, 2) situar, 3) relacionar la información mediante un accionar metódico, sistemático y seguro, cuya consigna será: 1) rotular, 2) referenciar y 3) proteger.



Protocolo para la cadena de custodia en la pericia informático forense

En síntesis, la validez de la prueba informática depende del mantenimiento de la seguridad, de procurar el resguardo legal y del seguimiento de una metodología estricta. De este modo, en el lugar del hecho se deberá seguir una secuencia de pasos expresadas en el siguiente procedimiento que se considerará como etapa preliminar a la elaboración del formulario de la cadena de custodia, el cual debe ser considerado como información confidencial, clasificada y resguardada en un lugar seguro:

1. Detección, identificación y registro

En lo posible, debe identificarse la totalidad de los elementos informáticos dubitados —computadoras, red de computadoras, *netbook*, *notebook*, celular, iPad, GPS, etc.— y para ello realizar un inventario de hardware en la inspección y el reconocimiento judicial que quedarán consignados en el formulario registro de evidencia. Para ello, quien realice el procedimiento tendrá cuidado de:

a. Colocarse guantes.

b. Fotografiar el lugar del hecho o filmar todos los elementos que se encuentran en el área de inspección, desde la periferia hacia el área dubitada.

c. Fotografiar los elementos informáticos, determinando en cuál de ellos efectuar macro fotografía:

i. Pantallas del monitor del equipo dubitado.

ii. Vistas frontal, lateral y posterior, según corresponda.

iii. Números de series de los elementos informáticos, etiquetas de garantías.

iv. Periféricos, (teclados, mouse, monitor, impresoras, agendas PDA, videocámaras, video grabadora, PenDrive, dispositivos de almacenamiento en red, unidades de Zip o Jazz, celulares, iPod, etc.).

v. Material impreso en la bandeja de la impresora o circundante.

vi. Cableado.

vii. Dispositivos de conectividad, alámbricos e inalámbricos.

viii. Diagramas de la red y topologías.

d. Inventariar todos los elementos utilizando una planilla de registro del hardware, identificando: tipo, marca, número de serie, registro de garantía, estado (normal, dañado), observaciones particulares. *(Cfr. Inventario del hardware de la inspección judicial y el reconocimiento judicial – formulario de registro de evidencia de la computadora)*. Efectuar un croquis del lugar del hecho, especificando el acceso al lugar, la ubicación del o los equipos informáticos y de cualquier otro elemento, mobiliario, *racks*, cableado, existentes en el área a inspeccionar, para luego representarlo con cualquier herramienta de diseño.

2. Recolección de los elementos informáticos dubitados físicos o virtuales

El perito informático forense deberá recolectar la evidencia procediendo de manera acorde al origen del requerimiento de la pericia informático-forense, a saber:

1. Por orden judicial, cuyo texto indica:

   a. Secuestrar la evidencia para su posterior análisis en el laboratorio, el perito informático-forense procederá a:

      i. Certificar matemáticamente la evidencia.

      ii. Identificar y registrar la evidencia.

      iii. Elaborar un acta ante testigos.

      iv. Iniciar la cadena de custodia.

      v. Transportar la evidencia al laboratorio.

   b. Efectuar la copia de la evidencia para su posterior análisis en el laboratorio, el perito informático forense procederá a:

      i. Certificar matemáticamente la evidencia.

      ii. Duplicar la evidencia.

      iii. Identificar y registrar la evidencia y la copia.

      iv. Elaborar un acta ante testigos.

      v. Transportar la copia o duplicación de la evidencia al laboratorio.

2. Por solicitud particular de una persona específica, de una consultora, empresa, institución, organismo o por otros profesionales, el perito informático forense procederá a:

   a. Concurrir al lugar del hecho con un escribano público.

   b. Certificar matemáticamente la evidencia ante el escribano público.

   c. Duplicar la evidencia ante escribano público.

d. Solicitar al escribano que deje constancia en el acta de los motivos del secuestro, de los datos de la o las personas que solicitaron la pericia, las razones argumentadas y los fines pretendidos.

e. Solicitar una copia del acta realizada por el escribano.

f. Transportar la copia de la evidencia para su posterior análisis en el laboratorio

a. *Duplicación y autenticación de la prueba*

En ciertas situaciones el perito informático forense no podrá trasladar el equipamiento que contiene la información dubitada, por lo tanto deberá en el lugar del hecho efectuar la duplicación de la información contenida en su repositorio original. Esta tarea se deberá realizar de manera tal que la duplicación o copia generada preserve la validez de su contenido original.

A continuación se enuncian los pasos para efectuar la autenticación y duplicación de la prueba, el perito informático forense llevará en su maletín los dispositivos de almacenamiento limpios y desinfectados y el dispositivo de arranque (disco rígido externo, CD ROM, DVD, disquete) o inicio en vivo protegido contra escritura, que contiene el software de base seleccionado para la tarea y el software de autenticación y duplicación.

Las imágenes de los discos se deben realizar bit a bit para capturar la totalidad del disco rígido los espacios libres, no asignados y los archivos de intercambio, archivos eliminados y ocultos. Acorde a lo expresado por el NIST (National Institute of Standard and Technology), la herramienta utilizada para la generación de la imagen debe reunir ciertas especificaciones, como:

1. La herramienta deberá efectuar una imagen bit a bit de un disco original o de una partición en un dispositivo fijo o removible.

2. La herramienta debe asegurar que no alterará el disco original.

3. La herramienta podrá acceder tanto a discos SCSI como IDE.

4. La herramienta deberá verificar la integridad de la imagen de disco generada.

5. La herramienta deberá registrar errores tanto de entrada como de salida e informar si el dispositivo de origen es más grande que el de destino.

6. Se debe utilizar un bloqueador de escritura, preferiblemente por hardware, para asegurar la inalterabilidad del elemento de almacenamiento accedido.

La documentación de la herramienta deberá ser consistente para cada uno de los procedimientos. Esta imagen del disco se utilizará en la computadora del laboratorio para efectuar el análisis correspondiente.

1. Apagar el equipo desconectando el cable de alimentación eléctrica.

2. Retirar disquete, PenDrive, Zip.

3. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.

4. Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.

5. Desconectar la alimentación eléctrica del dispositivo de disco rígido

6. Ingresar al CMOS (complementary metal oxide Semiconductor) o configuración del BIOS (sistema de entrada y salida de la computadora):

   i. Encender la computadora.

   ii. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

   iii. Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia. y documentar todo tipo de dato

que el perito informático forense considere relevante.

iv. Modificar la unidad de inicio o arranque del sistema operativo, es decir, seleccionar la unidad de disquete, CD-ROM / DVD o zip.

v. Guardar los cambios al salir.

8. Verificar la existencia de discos CD-ROM o DVD:

   a. Abrir la lectora o grabadora de CD-ROM o de DVD y quitar el disco pertinente.

9. Colocar la unidad de arranque, disquete, CD-ROM/DVD o zip en el dispositivo de hardware pertinente.

10. Verificar el inicio desde la unidad seleccionada.

11. Apagar el equipo.

12. Asegurar el dispositivo de almacenamiento secundario original —generalmente está configurado en el CMOS como master (maestro o primario) con protección de solo lectura—, mediante la configuración de los *jumpers* que indique el fabricante del disco o mediante el hardware bloqueador de lectura.

13. Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

14. Conectar la alimentación eléctrica del dispositivo de disco rígido master.

15. Conectar el dispositivo que se utilice como destino para hacer la duplicación del disco rígido dubitado como *slave* —esclavo o secundario—, ya sea una controladora SCSI, un disco IDE esclavo o una unidad de cinta, o cualquier otro hardware utilizado para la duplicación de tamaño superior al disco original o dubitado. Si el almacenamiento secundario original es demasiado grande o es un arreglo de discos, efectuar la copia en cintas.

16. Verificar que en el dispositivo de arranque seleccionado se encuentren los controladores del hardware para la duplicación, en caso de que sean requeridos.

17. Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

18. Efectuar la certificación matemática del dispositivo dubitado.

19. Guardar el resultado en un dispositivo de almacenamiento.

20. Registrar el resultado en el formulario verificación de la evidencia.

21. Duplicar el dispositivo de los datos con la herramienta de software y hardware seleccionada.

22. Efectuar, acorde al requerimiento de la pericia una o dos copias de la evidencia. En el caso de realizar dos copias, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio del perito informático forense y el original se deja en depósito judicial o si la pericia ha sido solicitada por un particular, registrarlo ante escribano público y guardarlo, según lo indicado por el solicitante de la pericia y el escribano público.

23. Efectuar la certificación matemática de la o las copias del dispositivo dubitado.

24. Guardar el resultado generado por las copias duplicadas en un dispositivo de almacenamiento.

25. Registrar el resultado generado por las copias duplicadas en el formulario de recolección de la evidencia.

26. Apagar el equipo.

27. Retirar los tornillos de sujeción del dispositivo de disco rígido.

28. Retirar el disco rígido con cuidado de no dañar el circuito electrónico.

3. Recolección y registro de evidencia virtual

a. Equipo encendido**:** En el caso de que se deba acceder a un equipo encendido, se debe considerar la obtención de los datos en tiempo real y de los dispositivos de almacenamiento volátil. Los dispositivos de almacenamiento volátil de datos pierden la información luego de interrumpirse la alimentación eléctrica, es decir al apagar la computadora la información almacenada se pierde.

Los datos que se encuentran en el almacenamiento volátil muestran la actividad actual del sistema operativo y de las aplicaciones, como por ejemplo: procesos en el estado de ejecución, en el estado de listo o bloqueado, actividad de la impresora (estado, cola de impresión), conexiones de red activas, puertos abiertos, (puerto es una estructura a la que los procesos pueden enviar mensajes o de la que pueden extraer mensajes, para comunicarse entre sí, siempre está asociado a un proceso o aplicación, por consiguiente sólo puede recibir de un puerto un proceso, recursos compartidos, estado de los dispositivos como discos rígidos, disqueteras, cintas, unidades ópticas.

Los datos volátiles están presentes en los registros de la unidad central de procesamiento del microprocesador, en la memoria caché, en la memoria RAM o en la memoria virtual.

Conjunto de tareas a realizar en el acceso a los dispositivos de almacenamiento volátil

1. Ejecutar un intérprete de comandos confiable o verificado matemáticamente.
2. Registrar la fecha, hora del sistema, zona horaria.
3. Determinar quién o quienes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.
4. Registrar los tiempos de creación, modificación y acceso de todos los archivos.
5. Verificar y registrar todos los puertos de comunicación abiertos.
6. Registrar las aplicaciones relacionadas con los puertos abiertos.
7. Registrar todos los procesos activos.
8. Verificar y registrar las conexiones de redes actuales y recientes.
9. Registrar la fecha y hora del sistema
10. Verificar la integridad de los datos.
11. Documentar todas las tareas y comandos efectuados durante la recolección.

Posteriormente, en lo posible, se debe realizar una recolección más detallada de los datos existentes en el almacenamiento volátil, efectuando las siguientes tareas:

1. Examinar y extraer los registros de eventos.
2. Examinar la base de datos o los módulos del núcleo del sistema operativo.
3. Verificar la legitimidad de los comandos del sistema operativo.
4. Examinar y extraer los archivos de claves del sistema operativo.
5. Obtener y examinar los archivos de configuración relevantes del sistema operativo.
6. Obtener y examinar la información contenida en la memoria RAM del sistema.

Procedimiento

En la computadora, con el equipo encendido, acceder al recurso acorde al orden de volatilidad de la información, con las herramientas forenses almacenadas en disquete o cd-rom y de acceso de solo lectura:

1. Ejecutar un intérprete de comandos legítimo.
2. Obtener y transferir el listado de comandos

utilizados en la computadora, antes de la recolección de datos.

3. Registrar fecha y hora del sistema.
4. Recolectar, transferir a la estación forense o medio de recolección forense y documentar.
   a. Fecha y hora del sistema.
   b. Memoria principal.
   c. Usuarios conectados al sistema.
   d. Registro de modificación, creación y tiempos de acceso de todos los archivos.
   e. Listado de puertos abiertos y de aplicaciones escuchando en dichos puertos.
   f. Listado de las aplicaciones asociadas con los puertos abiertos.
   g. Tabla de procesos activos.
   h. Conexiones de red actuales o recientes.
   i. Recursos compartidos.
   j. Tablas de ruteo.
   k. Tabla de ARP.
   l. Registros de eventos de seguridad, del sistema, de las aplicaciones, servicios activos.
   m. Configuración de las políticas de auditoría del sistema operativo.
   n. Estadísticas del núcleo del sistema operativo.
   o. Archivos de usuarios y contraseñas del sistema operativo.
   p. Archivos de configuración relevantes del sistema operativo.
   q. Archivos temporales.
   r. Enlaces rotos.
   s. Archivos de correo electrónico.
   t. Archivos de navegación en internet.
   u. Certificación matemática de la integridad de los datos.
   v. Listado de los comandos utilizados en la computadora, durante la recolección de datos.
   w. Recolectar la topología de la red.

4. Si es factible, apagar el equipo.

b. Equipo apagado: En el caso que el perito informático forense efectúe la recolección de la evidencia en un equipo apagado, deberá previamente asegurarse que el dispositivo de inicio del equipo no se realice a través del disco rígido o dispositivo de almacenamiento secundario dubitado. Así mismo, deberá utilizar dispositivos de arranque en el modo solo lectura, con herramientas informáticas forenses para realizar la detección, recolección y registro de indicios probatorios.

Procedimiento

7. Apagar el equipo desconectando el cable de alimentación eléctrica
8. Retirar disquetes, PenDrive, Zip.
9. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.
10. Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.
11. Desconectar la alimentación eléctrica del dispositivo de disco rígido.
12. Ingresar al CMOS (complementary metal oxide semiconductor) o configuración del BIOS (sistema de entrada y salida de la computadora):

a. Encender la computadora

b. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

c. Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia. y documentar todo tipo de dato que el perito informático forense considere relevante y documentarlo con fotografía, filmadora o en la lista de control.

d. Modificar la unidad de inicio o arranque del sistema operativo, es decir seleccionar la unidad de disquete, CD-ROM/DVD o ZIP de solo lectura con las herramientas informáticas forenses.

e. Guardar los cambios al salir.

8. Colocar la unidad de arranque, disquete, cd-rom/dvd o zip en el dispositivo de hardware pertinente.

9. Verificar el inicio desde la unidad seleccionada.

10. Apagar el equipo.

11. Acorde a la decisión del perito informático forense o a lo solicitado en la requisitoria pericial, se podrá realizar el *Procedimiento de duplicación y autenticación de la prueba,* explicado anteriormente o continuar con la lectura del dispositivo original, configurando el mismo con los jumpers que el fabricante indique como solo lectura o colocando un dispositivo de hardware de bloqueo de escritura.

12. Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

13. Conectar la alimentación eléctrica del dispositivo de disco rígido.

14. Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

15. Colocar el dispositivo de almacenamiento forense.

16. Efectuar la certificación matemática del dispositivo dubitado.

17. Guardar el resultado en un dispositivo de almacenamiento forense.

18. Registrar el resultado en el formulario de recolección de la evidencia.

19. Por medio del conjunto de herramientas informático forense, obtener la siguiente información del disco dubitado, documentarla y almacenarla en dispositivos de almacenamiento forense, para su posterior análisis, ya sea en el lugar del hecho o en el laboratorio:

a) Tipo de sistema operativo

b) Fecha, hora y zona horaria del sistema operativo

c) Versión del sistema operativo

d) Número de particiones

e) Tipo de particiones

f) Esquema de la tabla de particiones

g) Listado de todos los nombre de archivos, fecha y hora

h) Registro del espacio descuidado o desperdiciado.

i. Incluido el MBR

ii. Incluida la tabla de particiones

iii. Incluida la partición de inicio del sistema y los archivos de comandos

i) Registro del espacio no asignado

j) Registro del espacio de intercambio

k) Recuperación de archivos eliminados

l) Búsqueda de archivos ocultos con las palabras claves en el:

i. espacio desperdiciado

ii. espacio no asignado

iii. espacio de intercambio

iv. MBR y tabla de particiones

m) Listado de todas las aplicaciones existentes en el sistema

n) Búsqueda de programas ejecutables sospechosos

o) Identificación de extensiones de archivos sospechosas.

p) Listado de todos los archivos protegidos con claves.

q) Listado del contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios

r) Verificación del comportamiento del sistema operativo:

i. Integridad de los comandos

ii. Integridad de los módulos

iii. Captura de pantallas

20. Generar la autenticación matemática de los datos a través del algoritmo de hash al finalizar la detección, recolección y registro.

21. Conservar las copias del software utilizado

22. Apagar o dejar funcionando el equipo, esto dependerá de la requisitoria pericial.

Procedimiento para el resguardo de la prueba y preparación para su traslado

1. Disponer, según sea el caso, las pruebas obtenidas en una zona despejada, para su posterior rotulado y registro.

2. Registrar en el formulario de registro de la evidencia cada uno de los elementos dubitados, acorde a lo especificado en dicho formulario y agregando cualquier otra información que considere pertinente el perito informático forense.

3. Proteger:

   a. en bolsas antiestáticas los elementos informáticos de almacenamiento secundario, registrando: Fecha y hora del secuestro, tipo, número de serie del elemento si se puede obtener, capacidad de almacenamiento, apellido, nombre y documento de identidad del perito informático forense, firma del perito informático forense.

   b. en bolsas manufacturadas con filamentos de cobre y níquel para prevenir la interferencia de señales inalámbricas —celulares, GPS, etc.—

4. Proteger con plástico o con bolsas estériles cualquier otro elemento que considere relevante el perito informático forense y rotularlos con los datos pertinentes al elemento, apellido, nombre y documento de identidad del perito informático forense, firma del perito informático forense.

5. Elaborar el acta de secuestro acorde al formulario del recibo de efectos.

6. Colocar los elementos identificados y registrados en una caja o recipiente de traslado que asegure la suficiente rigidez, aislamiento térmico, electromagnético y protección para evitar daños accidentales en el traslado de los elementos probatorios.

7. Trasladar, en lo posible, los elementos secuestrados reunidos en un único recipiente, evitando la confusión, separación o pérdida durante su almacenamiento posterior.

5. Traslado de la evidencia de informática forense

El traslado de la evidencia tendrá como destino el laboratorio de informática forense correspondiente al organismo establecido en la requisito-

ria pericial. La permanencia en este laboratorio puede ser temporal, pero será necesario mantener la cadena de custodia mientras la prueba sea analizada por las entidades involucradas. Acorde a la evolución del proceso judicial donde se encuentra involucrada la prueba de informática forense, la prueba podrá ser posteriormente entregada y resguardada en un lugar o destino específico para su resguardo y depósito final o definitivo.

Nota importante: Es sumamente importante considerar que si bien la prueba documental informática constituye una especie del género prueba documental clásica (bibliográfica, foliográfica y pictográfica), de la cual solo difiere en el soporte (papel vs. digital), no significa que por esto escape a las consideraciones generales que le aporta la criminalística en su sentido más amplio.

Conclusiones

Suele ocurrir que como la realización de la certificación *in situ* por digesto matemático de los discos secuestrados (*hash*) es una tarea que consume mucho tiempo, se prefiere secuestrar los equipos, clausurarlos y dejar la tarea de validación y *hash* para un momento posterior, generalmente en el laboratorio pericial. Sin embargo, se suele preservar la prueba en las mismas condiciones en que fue encontrada en el momento de la recolección. Este criterio hace que al secuestrar equipos informáticos, se mantenga el disco conectado a su fuente de alimentación y a su cable de datos para *"no modificar la prueba y preservar las condiciones de secuestro"*.

Sin embargo, este es un error, pues pone en riesgo la integridad de los datos recolectados en el disco referido. En efecto, si el aislamiento posterior del equipo con las correspondientes fajas de clausura, deja resquicios accesibles, cualquier persona de manera intencional o accidental podrá acceder al disco y modificar su contenido. La experiencia indica que muchas veces es posible incluso retirar el disco o acceder al mismo sin romper las fajas de clausura colocadas. De ahí que sea preferible abrir el gabinete y desconectar físicamente el disco (alimentación y datos) —hecho que debe ser registrado en el acta de secuestro—, para protegerlo de accesos indeseados hasta el momento de la ruptura formal de las fajas, para realizar las tareas técnico-periciales encomendadas.

Esta apertura debe ser ejecutada con todos los requisitos procesales pertinentes: acta de apertura, presencia de testigos, comprobación de integridad de las fajas de clausura y desconexión de los discos insertos en el gabinete, todo lo cual debe quedar registrado en un acta de apertura, que constituye la contrapartida del acta de secuestro. Al finalizar la labor pericial, debe desconectarse nuevamente el disco y dejar registro de esta circunstancia en el acta que corresponda (tareas periciales efectuadas, registro, comprobación, etc.).

Haciendo una analogía, cuando se secuestra un arma, se privilegia la seguridad sobre la protección de la prueba, es decir, se descarga y se envían por separado los proyectiles, las vainas y la munición intacta, en especial para evitar accidentes; esto en nada afecta a la prueba. La misma atención se debe aplicar a la prueba documental informática resguardada en el disco: se debe privilegiar la protección de los datos sobre el mantenimiento de las condiciones de recolección a ultranza; basta con aclarar la acción efectuada para que el juez tenga conocimiento de lo ocurrido y su razón de ser técnica y procesal.

Algunas definiciones pertinentes

En referencia a estos actos, téngase en cuenta el correcto empleo de los siguientes vocablos o palabras claves para fines de lo explicado aquí:

> ***Expropiar*** (paras. de propio): Desposeer legalmente (de una cosa) a su propietario por razón de interés público.
>
> ***Confiscar:*** Apropiarse las autoridades competentes de lo implicado en algún delito: *"confiscar mercadería de contrabando"*.

Secuestrar: Ordenar el juez el embargo o retirada de la circulación de una cosa: *"secuestrar la edición de un periódico"*.

Decomisar: Incautarse el Estado como pena de las mercancías procedentes de comercio ilegal o los instrumentos del delito: *"se ha decomisado un kilo de heroína"*.

Incautar(se) (no existe el verbo incautar): (de *in* y *cautum*, multa) Dicho de una autoridad judicial o administrativa. Privar a alguien de sus bienes como consecuencia de la relación de estos con un delito, falta o infracción administrativa. Cuando hay condena firma se sustituye por la pena accesoria de comiso.

Referencias

[1] Arellano, Enrique y Darahuge, María E. (2011). Manual de informática forense. Buenos Aires: Errepar.

[2] Borghello, Cristian (2001). Seguridad informática. Implicancias e implementación. [versión electrónica] Disponible en: http://www.segu-info.com.ar/tesis/ [Consultado: octubre, 2012].

[3] Castañeda, Carlos M. (2012) Cibercriminal. s.l., s.e.

[4] Lucena, Manuel J. (2000). Criptografía y seguridad para computadores. 3ª. ed., [PDF] Disponible en: http://iie.fing.edu.uy/ense/asign/seguro/Criptografia.pdf [Consultado: octubre, 2012].

[5] Sies, John (2011). Delitos emergentes. s.l., s.e.