# Evidencia Digital y Cadena de Custodia

Juan P. Vanegas, Estudiante, Universidad Piloto de Colombia

***Abstract*—This article relates to computer forensics as a means of support for the identification of the chain of custody process, which is taken into account from the point of identification of the scene, through the collection and packaging of evidence until completion of the process, so that it does not lose the probative value, thus ensuring a greater extent, the standards for the preservation of the integrity and authenticity of information.**

***Key Word— P.M.E. (Probative Material Element), P.E. (Physical evidence), forensic Image, Chain of custody.***

***Resumen*—El presente artículo relaciona la informática forense como un medio de apoyo para la identificación del procedimiento de cadena de custodia, el cual es tenido en cuenta desde el momento de identificación de la escena, pasando por la recolección y embalaje de la evidencia hasta el momento de finalización del proceso, con el propósito de que ésta no pierda el valor probatorio, garantizando así, en mayor medida, los estándares para la conservación de la integridad y autenticidad de la información.**

***Palabras Clave— EMP (Elemento Material Probatorio), EF (evidencia Física), Imagen forense, Cadena de custodia.***

## I. INTRODUCCIÓN

En los últimos años se ha visto un alarmante aumento en el acceso a medio informáticos, lo que podría tomarse como un aumento en la calidad de vida y mejoras para las personas en términos de desplazamiento y facilidades, pues de las actividades que anteriormente era necesario hacerlas de forma presencial, muchas de ellas ha sido posible realizarlas por medios electrónicos. El acceso a la información es cada vez mayor, hecho que hace atractivo su uso para actividades delictivas. Anteriormente los asaltantes cargaban un arma para algún robo, ya esta actividad es para asaltantes obsoletos y anticuados que vivieron en un tiempo que casi no se recuerda. Actualmente, con los favores de la globalización, acceso a la información y facilidades comerciales, las actividades delictivas también han tomado su puesto en el sector, ahora se habla de compras electrónicas fraudulentas, transferencias millonarias de dinero, y todo se realiza a través de sistemas informáticos.

En el presente artículo se presentan los sistemas informáticos como contenedores de evidencias, y su procedimiento para poder ser llevado a un estrado judicial.

[1]Manuscrito recibido el 24 de Abril, 2013. El presente artículo es parte del material de entrega para la especialización en seguridad Informática, Universidad Piloto de Colombia

J. P. Vanegas es estudiante de la universidad Piloto de Colombia en la especialización de Seguridad Informática (jpvs@synapsis-it.com).

En II. *Informática Forense* se presenta una introducción a la informática forense y algunas definiciones que hay que tener en consideración. En III. *Evidencia* se establecen los parámetros que definen a una evidencia digital y la diferencia con la evidencia electrónica. En IV *Lugar de los hechos* se presenta el procedimiento para el aseguramiento del lugar de ubicación de los hechos. En V Recolección y análisis de la evidencia se presentan dos herramientas forenses muy conocidas y aceptadas por la comunidad, EnCase y FTK. En VI *Cadena de custodia* se presentan algunas consideraciones que hay que tener en cuenta para el manejo de evidencias digitales y su correcto seguimiento.

## II. INFORMÁTICA FORENSE

La informática forense, de acuerdo a su enfoque técnico, se podría interpretar de diferentes maneras. Jeimy Cano [1] logra identificar tres definiciones básicas que acompañan las informática forense, como lo es la computación forense, digital forensics (forensia digital) y network forensics (forensia en redes).Cada uno de estos términos presenta connotaciones particulares en su medio de acción, sin embargo todos pretenden lograr, como método forense, identificar la verdad respecto a un hecho o suceso ocurrido y, en caso de requerirse, lograr judicializar al responsable de los actos.

No en todos los casos es posible identificar de forma contundente el o los responsables que participaron en el suceso, sin embargo, a través de la informática forense se pueden dar indicios del método con el que se cometió la conducta y las posibles vulnerabilidades en el sistema informático por medio del cual se materializó el incidente, en caso de presentarse alguno, o la recolección y análisis de evidencia proveniente de dispositivos electrónicos, como diferentes tipos de medios de almacenamiento (memorias USB, discos duros), datos volátiles (tablas de enrutamiento, procesos activos, datos almacenados en memoria RAM), para el caso del acceso a equipos informáticos encendidos.

El presente artículo presenta un enfoque hacia el procedimiento de recolección y cadena de custodia de la evidencia digital soportado por la Fiscalía General de la nación en su “Manual de procedimientos para cadena de custodia” [3], por lo que se obtienen tres líneas de proceso claramente identificables:

- Aseguramiento del lugar de los hechos
- Recolección de evidencias
- Aseguramiento y cadena de custodia de evidencias.

## III. EVIDENCIA

Al referirnos hacia la evidencia tomada en una escena hay

que tener en consideración dos características importantes de ésta, la parte física del equipo y la parte lógica. La parte física está ligada al hardware que almacena la información, el contenedor, la *evidencia electrónica*, mientras que el contenido de información, los datos, software almacenado en estos dispositivos, hacen parte de la *evidencia digital*. Es fundamental tener presente estas características en el momento de la evidencia y del proceso de cadena de custodia, ya que es diferente el tipo de trato que se le debe dar a cada una de ellas. Por ejemplo, es posible realizar una copia idéntica a la información almacenada en un contenedor (imagen forense), sin embargo no es posible duplicar un contenedor, por otro lado, al poder generar imágenes forenses, éstas se pueden almacenar en diferentes contenedores y, de seguirse el debido procedimiento documental, se puede tomar la evidencia de la imagen forense y cargarla en diferentes contenedores y hacerla pasar como información la original.

Teniendo en cuenta las diferencias entre una evidencia electrónica y una digital, se han establecido diferentes procedimientos para su recolección y proceso de cadena de custodia. El presente artículo se enfoca en el procedimiento propuesto por la Fiscalía General de la Nación, en el libro titulado “Manual de procedimientos para cadena de custodia”[2].

## IV. Lugar de los hechos

De acuerdo al procedimiento descrito en el “Manual de procedimientos para cadena de custodia” de la Fiscalía general de la Nación, se deben seguir unos lineamientos antes de la toma de evidencias para que éstas tengan validez legal. Los pasos que se deben tener a mayor consideración, luego de tener validada la ubicación de la escena de los hechos es:

- Aseguramiento del lugar de los hechos: Se observa el lugar de los hechos para identificar los límites y ubicaciones de los EMP y EF. En caso de ser necesario se acordona el área de acuerdo a la distribución de la evidencia.
- Fijación de los hechos: Se realiza el levantamiento del lugar de los hechos, toma de fotos y grabación.

Para poder tener un soporte de gran validez se recomienda la captura del lugar de los hechos por medio audiovisual, en el que se aprecie la continuidad de los hechos. Esto permite identificar y registrar que la escena no ha sido comprometida y conserva su integridad. Adicionalmente es una forma de validación entre lo que se esta diciendo acerca de la escena y lo que realmente este allí.

## V. Recolección y análisis de la evidencia[3][4]

La toma de la evidencia digital es un procedimiento en el que hay que realizar cuidadosamente ya que una pequeña afectación a la evidencia podría dejarla inservible, por lo que, en caso de ser necesaria la recolección de información directamente sobre la evidencia, es necesario documentar todo el procedimiento para que no se presenten dudas al respecto.

En el momento de la toma de evidencias, es muy importante que se cuente con testigos que puedan dar fe del procedimiento realizado, aunque también es de gran utilidad realizar grabaciones audiovisuales de este procedimiento. Algunas de las consideraciones para la recolección de las evidencias digitales son:

- En caso de encontrarse un equipo de cómputo, tener en cuenta que antes de la manipulación de éste es necesario contar con guantes de látex, impidiendo que se borren huellas que posiblemente se encuentran en la evidencia física, afectar con las huellas propias o la descarga de energía estática en el elemento.
- Se el equipo se encuentra apagado, por ninguna circunstancia encenderlo, ésto alteraría la evidencia de forma significativa y podría perder valor probatorio.
- Si se presume que el equipo esta destruyendo la evidencia se debe desconectar inmediatamente.
- Si el equipo se encuentra encendido, realizar la captura de datos volátiles, como tablas de enrutamiento, conexiones establecidas, volcado de memoria.
- En caso de requerir conectar un dispositivo externo, asegurarse que se cuente con bloqueador de escritura, para ello tener en cuenta que existen soluciones tanto de hardware como de software. Los de hardware son externos a la evidencia, en cuanto que los de software habría que modificar registros en el equipo de la evidencia. Esto se podría hacer sin afectar la integridad de la evidencia, aunque hay que tener en cuenta de siempre documentar lo realizado en el procedimiento.
- Si el equipos Desktop/portátil se encuentra encendido y ya se le realizó la extracción de los datos volátiles, su apagado se requiere de forma súbita, retirando toda alimentación de energía al equipo, ya sea desconectando el cable de poder y/o retirando la batería del portátil.
- En lo posible llevar las herramientas forenses en unidades de CD, grabadas en discos de solo lectura.

### *A. Copias de seguridad*

Como se mencionó con anterioridad, en lo posible no realizar intervención directa sobre la evidencia ya que ésta se podría afectar y comprometer su integridad, lo que podría llevar a su nulidad, sin embargo, para la recolección de datos volátiles es algo totalmente necesario, ya que es información que se encuentra disponible solo en el momento y que se borraría luego del apagado del equipo. Para solucionar el inconveniente de la intervención a la evidencia, es necesario realizar una documentación muy detallada sobre el procedimiento realizado.

Para la realización de copias de seguridad se debe en cuenta:

- La copia de la evidencia debe ser de tipo forense, no una copia lógica. La diferencia entre estas dos copias es que la lógica solo almacena los datos visibles de

las particiones, mientras que las imágenes forenses son una réplica exacta de los datos de la evidencia, incluyendo estructura de bloques y espacios libres en disco.
- Dado que el algoritmo MD5 ha presentado vulnerabilidades en cuanto a generación de colisiones, se está haciendo uso de algoritmos HASH mas robustos, como el SHA-1. Es indispensable que la imagen forense cuente con el mismo valor de HASH que la evidencia original.
- Se deben generar mínimo dos copias forenses, una para el investigador y la otra para la contra parte. A la evidencia del contenedor original se le debe hacer la respectiva cadena de custodia.

### *B. Análisis de la evidencia*

Para la extracción de la información de la evidencia digital no se cuenta con un método estándar, lo cual sugiere que está orientado a los resultados obtenidos siempre y cuando se conserven las propiedades de la evidencia, como lo es su integridad.

Antes de dar inicio a la presentación de algunas herramientas forenses, es necesario conocer el método de análisis de los equipos.

- Live Forensics: En este tipo de análisis se extrae la evidencia mientras el equipo se encuentra encendido, lo cual es de gran utilidad para la validación de algunas características de comunicación y procesos que solo se encuentran con el equipo encendido. Por ejemplo, enrutamiento, sesiones activas, procesos, datos almacenados en memoria, información volátil. La realización de la extracción de información por este medio hay que realizarlo con el mayor cuidado posible ya que se trabaja directamente sobre la evidencia, por lo que la información es sensible a modificación. Para atenuar el impacto que pueda causar éste método en un proceso jurídico, es necesario documentar absolutamente todo el procedimiento realizado, tomando evidencias de ello. De ser posible contar con un testigo que corrobore las acciones tomadas en el procedimiento.
- Post Mortem: Éste análisis se realiza con dispositivos pasivos, discos duros, dispositivos USB, entre otros. Es un método muy útil para la extracción de información que ha sido eliminada, registros del sistema, información oculta. Es una técnica que permite la creación de imágenes forenses, por lo que es posible trabajar con una copia original sin tener que trabajar sobre la evidencia directamente.

### *C. Herramientas Forenses*

Algunas de las herramientas forenses más utilizadas son:

- FTK [5]: Es una suit forense de altas prestaciones y capacidades, fabricada por Access Data. Dentro de sus características se encuentra:
  - Dentro de las soluciones forenses ofrece la creación de copias forenses, análisis de archivos de correo, registros y generación de reportes.
  - Los datos son almacenados en una base de datos independiente, por lo que en caso de presentarse una falla en la interfaz gráfica, ésta no afectaría el procesamiento de los datos.
  - Captura y análisis de datos volátiles de sistemas operativos Windows, Apple, Unix y Linux.
  - Mejoras en la velocidad de procesamiento.
  - Descifra información de forma automática.
  - Habilidad de identificación y clasificación de imágenes, como por ejemplo de tipo pornográfico.
  - Generación de reportes en diferentes formatos.

- EnCase Forensic [6]: Es una suit forense de altas prestaciones y capacidades. Dentro de sus características se encuentra:
  - Adquisición de datos de múltiples dispositivos y equipos electrónicos. La última versión cuenta con la posibilidad de análisis de tablets y teléfonos inteligentes.
  - Permite la creación de imágenes forenses y la generación hash para validación de la igualdad de copia.
  - Recuperación de archivos y particiones.
  - Permite la vista previa en la medida que se va generando el descubrimiento en el momento del análisis de la evidencia.
  - Soporta multitud de formatos y la capacidad de ordenarlos cronológicamente.
  - Generación automática de reportes.
  - Generación de reportes a la medida.
  - Protección de los hallazgos por contraseña.

Adicionalmente a las características prestadas por la solución de EnCase, es posible la implementación de la evidencia por medio de un bloqueador de puertos, el cual puede conseguirse a través de EnCase o de un distribuidor externo.

## VI. CADENA DE CUSTODIA

El éxito de los hallazgos presentados de la evidencia solo es proporcional al cuidado y seguimiento que se le de a ésta, documentando cada acción, cada traslado, cada acceso a la información y, en el momento de ser llevado a juicio, se tenga claro el responsable de cada gestión y manipulación de la evidencia. Para ello, la Fiscalía presenta un formato para el seguimiento de la cadena de custodia, el cual tiene que ser diligenciado a cabalidad por las personas involucradas, y de forma veraz. Este documento no admite errores, tachones ni enmendaduras. De ser diligenciado de forma incorrecta, el análisis investigativo sobre la evidencia, por más documentado que se encuentre, podría perder peso ante el estrado.

A continuación se presenta el formato de la cadena de custodia aprobado por la Fiscalía [2] en el momento de la presentación del presente artículo.


Figura 1. Formato Cadena de custodia, hoja 1 de 2

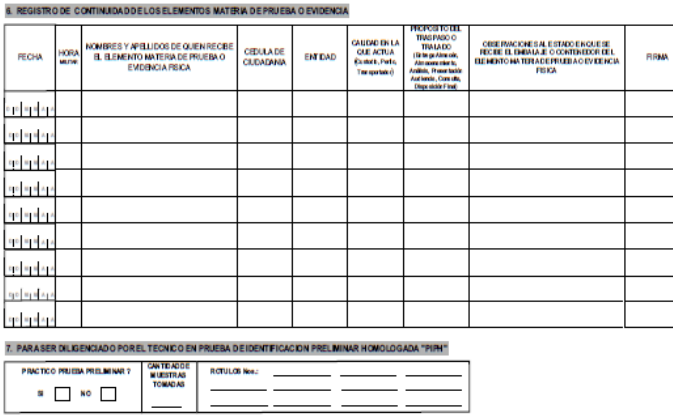


Figura 2. Formato Cadena de custodia, hoja 2 de 2

Como se comentó, es necesario diligenciar el registro de continuidad de las figuras 3 y 4, con datos reales, sin cometer errores, pues es en este formato que se identifica la ubicación exacta de la evidencia que, de haber una anomalía, se podría argumentar que se pierden garantías sobre la veracidad e integridad de la evidencia, lo cual podría tumbar la carga probatoria de ésta.

## VII. Conclusiones

Por medio de un análisis forense se puede identificar información que ha sido oculta o borrada de un sistema informático, facilitando la captura de datos volátiles, ocultos o eliminados de un sistema de información.

En el mercado existen múltiples herramientas de análisis forense, sin embargo, para un proceso jurídico, es necesario el uso de herramientas avaladas por la comunidad, en el presente artículo se presentaron dos herramientas, FTK y EnCase, sin embargo hay distribuciones Linux enfocadas en este tipo de análisis que, al ser herramientas de libre desarrollo, no están aprobadas por la comunidad ya que son susceptibles a modificación en su código fuente.

Para poder llevar la evidencia de un proceso jurídico a juicio, es necesario documentar totalmente un formato de cadena de custodia. En éste formato se documenta el responsable de la evidencia en un momento determinado. Un espacio cronológico faltante en la documentación podría tumbar el valor probatorio de la evidencia.

En un proceso no es valorado trabajar directamente sobre la evidencia, por ello es necesaria la creación de copias forenses de ésta, una para cada parte interesada.

## Referencias

[1] C. Jeimy J. “Introducción a la informática Forense”. Disponible online: *www.acis.org.co/fileadmin/Revista_96/dos.pdf*

[2] Fiscalía General de la Nación, “Manual de procedimientos para cadena de custodia”. Fiscalía General de la Nación.

[3] G. R. Juan L.”Un forense llevado a Juicio”, Flu-Project, Sidertia.

[4] A. Del Pino, Santiago. “Manual de manejo de evidencias digitales y entornos informáticos, versión 2.0”

[5] AccessData, “FTK AccessData Digital Forensics Software”. Disponible online en: http://www.accessdata.com/products/digital-forensics/ftk

[6] EnCase Forensic v7. “The industry-standard computer forensic solution. Fast, powerful, and proven in courts”. Disponible online en: http://www.guidancesoftware.com/encase-forensic.htm#tab=1