FRAMEWORK PARA LA COMPUTACIÓN FORENSE EN COLOMBIA

Andrés F. Álvarez Serna
Universidad de San Buenaventura
pipesalvarez@hotmail.com

Oscar D. Marín Rivera
ETICAL SECURITY
oscar.marin@une.net.co

Juan D. Victoria Morales
COMPUREDES
juan.victoria@compuredes.com.co

(Tipo de Artículo: **Investigación**. Recibido el 19/11/2012. Aprobado el 28/12/2012)

RESUMEN
Este FRAMEWORK es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar la problemática a la que se enfrentan los investigadores forenses al momento de procesar las evidencias digitales.

Este artículo se refiere a la forense digital en conceptos generales y ubica al lector en el presente de esta ciencia y muestra una guía de pasos a seguir para la recolección y tratamiento de las evidencias enmarcadas en las leyes colombianas y servirá como material de apoyo a estudiantes interesados en el tema y/o quienes ya estén en el medio.

Palabras clave
Evidencias, Forense, MD5, SHA, Memoria virtual, RAM, Swap.

FRAMEWORK FOR COMPUTER FORENSICS IN COLOMBIA

ABSTRACT
This Framework is a standardized set of concepts, practices and criteria for approaching the problems that must face forensics researchers when processing digital evidences. This article deals with digital forensic through basic concepts and brings the reader to the present of forensic science, it also shows a guide of proposed steps for the collection and processing of evidence based in Colombian laws, aiming to serve as support material for students interested in this subject and professionals in the field.

Keywords
Evidences, Forensic, MD5, SHA, Virtual Memory, RAM, Swap.

CADRE DE REFERENCE POUR L'INVESTIGATION NUMÉRIQUE LÉGALE DANS COLOMBIE

Résumé
Ce cadre de référence est un ensemble standardisé de concepts, pratiques et critères pour faire une approche à la problématique que doivent affronter les chercheurs légales dans le moment de traiter les évidences numériques.

Cet article s'occupe de l'investigation numérique légale avec des concepts généraux et place au lecteur dans l'actualité de cette discipline, montre une guide à suivre pour la collecte et traitement des évidences d'après la loi colombienne et supporte aux étudiants intéressés sur le thème et aussi aux professionnels.

Mots-clés
Évidences, Numérique Légale, MD5, SHA, Mémoire virtuel, RAM, Échange.

1. INTRODUCCIÓN

La ciencia forense informática es una disciplina moderna que busca en un incidente, fraude ó uso de recursos informáticos responder a los cuestionamientos ¿quién?, ¿cómo?, ¿dónde? y ¿cuándo? sucedieron los hechos, mediante la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de los hechos como material probatorio sólido.

2. CARACTERÍSTICAS GENERALES

Gracias al crecimiento en el uso del internet y a los masivos problemas de seguridad que esto acarrea, el crimen digital se ha convertido en un reto para los investigadores. Es aquí donde comienza una nueva forma de mirar la ciencia forense en la tecnología y nace la computación forense. El objetivo del investigador forense es aportar evidencia sólida a los administradores de justicia quienes son los encargados de determinar las responsabilidades civiles, administrativas y penales.

Dentro de los objetivos de la computación forense encontramos la necesidad de determinar los hechos ocurridos en un evento donde se interactúa con equipos de cómputo, buscando esclarecer los hechos, determinando la magnitud del incidente y los implicados. La finalidad de la ciencia informática forense en la mayoría de los casos, busca identificar material probatorio que pueda ser utilizado en un tribunal o simplemente apoye la gestión de riesgos mejorando la prevención de futuros incidentes [1].

3. REPOSITORIOS DE EVIDENCIAS

En entornos digitales la evidencia de cada operación podría estar en diversos componentes que pueden variar abruptamente según las características del sistema, es allí donde es fundamental la pericia del investigador y conocimiento especializado del sistema que se está evaluando. Una de las primeras recomendaciones es iniciar buscando en los repositorios más comunes de evidencia como los sistemas de archivos, archivos temporales, registro de Windows, archivos eliminados, slack space, memoria virtual.

Sistema de Archivos: Son los encargados de estructurar la información guardada en una unidad de almacenamiento que representa los datos en bits.

El conjunto de bits almacenados en una unidad es conocido como archivos o ficheros, estos son representados por nombres y son equivalentes a documentos físicos, que pueden ser encontrados en medios de cómputo internos o externos como teléfonos móviles, cámaras digitales, memorias USB, discos duros, unidades de almacenamiento externo, en general en cualquier dispositivo electrónico que permita almacenar información.

Archivos temporales: se crean en el sistema de archivos cuando inicia un programa para respaldar la información antes de ser guardado o bien para poderse ejecutar si el equipo no tiene suficiente memoria. Estos archivos normalmente se borran después de utilizar el programa, siempre y cuando el programa este configurado de esta manera. Casi siempre los archivos temporales se guardan en diferentes carpetas según el sistema operativo, por ejemplo en Windows se almacenan en la ruta C:\Windows\Temp, y en C:\Users\"usuario"\AppData\Local\Temp, la carpeta temporal de cada usuario se almacenan con extensión .TMP. En UNIX se guarda con el nombre original y extensión del archivo anteponiendo un carácter especial ~ y son almacenados en la ruta /tmp.

Registro de Windows: Sirve para almacenar los perfiles de los usuarios, las aplicaciones instaladas en el equipo y los tipos de documentos que cada aplicación puede crear, las configuraciones de las hojas de propiedades para carpetas y los iconos de aplicaciones, los elementos de hardware que hay en el sistema y los puertos que se están utilizando.

En el registro se encuentra información valiosa que es utilizada como evidencia digital Ej.: programas instalados o desinstalados, modificación sobre ellos etc.

Archivos Eliminados: Cuando se elimina información de los discos duros, estos desaparecen del sistema de archivos y son marcados en las unidades de almacenamiento como espacio libre, entonces existen bloques que contienen la información borrada o datos no usados. Lo anterior significa que la información permanece en el disco hasta que los datos son sobrescritos físicamente permitiendo la recuperación de información que el usuario final considera eliminada [1].

Slack space: es el espacio inutilizado en un sector del disco, que pueden ser utilizados para investigación porque puede contener información. Este espacio se encuentra al final de cada sector [1].

Memoria virtual: es una memoria temporal creada mediante la mezcla de hardware y software para realizar la carga de programas ayudando a la memoria RAM.

La memoria virtual se combina entre el disco duro y la memoria RAM, cuando la memoria RAM está saturada lleva datos a un espacio asignado al disco duro, llamado memoria virtual. En este espacio del disco el investigador encontrará información importante de los programas que se ejecutaron sin importar que el computador se encuentre apagado o encendido.

El común de las personas piensa que realizar daños a los sistemas se pueden realizar sin ser descubiertos y que necesitan gran conocimiento para realizarlos, por esta razón veremos unos mitos y prejuicios a los que se ven enfrentados.

4. MITOS Y PREJUICIOS

- ¿La persona que realiza un ataque informático requiere de un conocimiento grande en informática?
  No es así. Anteriormente se requería de un conocimiento amplio, pero hoy en día los atacantes con poco conocimiento realizan ataques con grandes impactos. Como ejemplo tenemos que antes se necesitaba realizar gran investigación y desarrollo de aplicativos (xploits) que finalmente realizan el ataque aprovechando una vulnerabilidad; ahora con solo descargar archivos desde la web como: http://www.exploits-msn.com/ encontramos programas que con solo un click pueden realizar ataques significativos incorporando nuevas motivaciones como el hacktivismo como muestra la figura 1.

- ¿Los hackers o crackers tienen un coeficiente intelectual superior al normal?
  Cualquier persona con conocimientos básicos en informática puede convertirse en hacker o cracker, gracias a las herramientas que se encuentran en internet, libros, conferencias etc.

- ¿Los criminales cibernéticos son expertos en computadores y con alta habilidad técnica?
  Ya no es necesario ser experto cualquiera con acceso a un computador e internet puede lograr ataques; con tan solo ingresar a foros como: http://www.taringa.net/posts/info/1697890/Ejemplo-de-Como-Funciona-un-Exploit.html, encontrará los pasos para realizar y ejecutar xploits fácilmente.

- ¿Puedo pasar desapercibido si realizo un ataque?
  Los investigadores forenses trabajan arduamente para hallar las evidencias necesarias que lo lleven a establecer cuándo?, cómo? y dónde? se realizó un ataque.

- ¿Si formateo el equipo se borra toda la evidencia?

  No, el forense especialista tiene las herramientas necesarias para recuperar la información como por ejemplo: ENCASE (http://www.guidancesoftware.com).

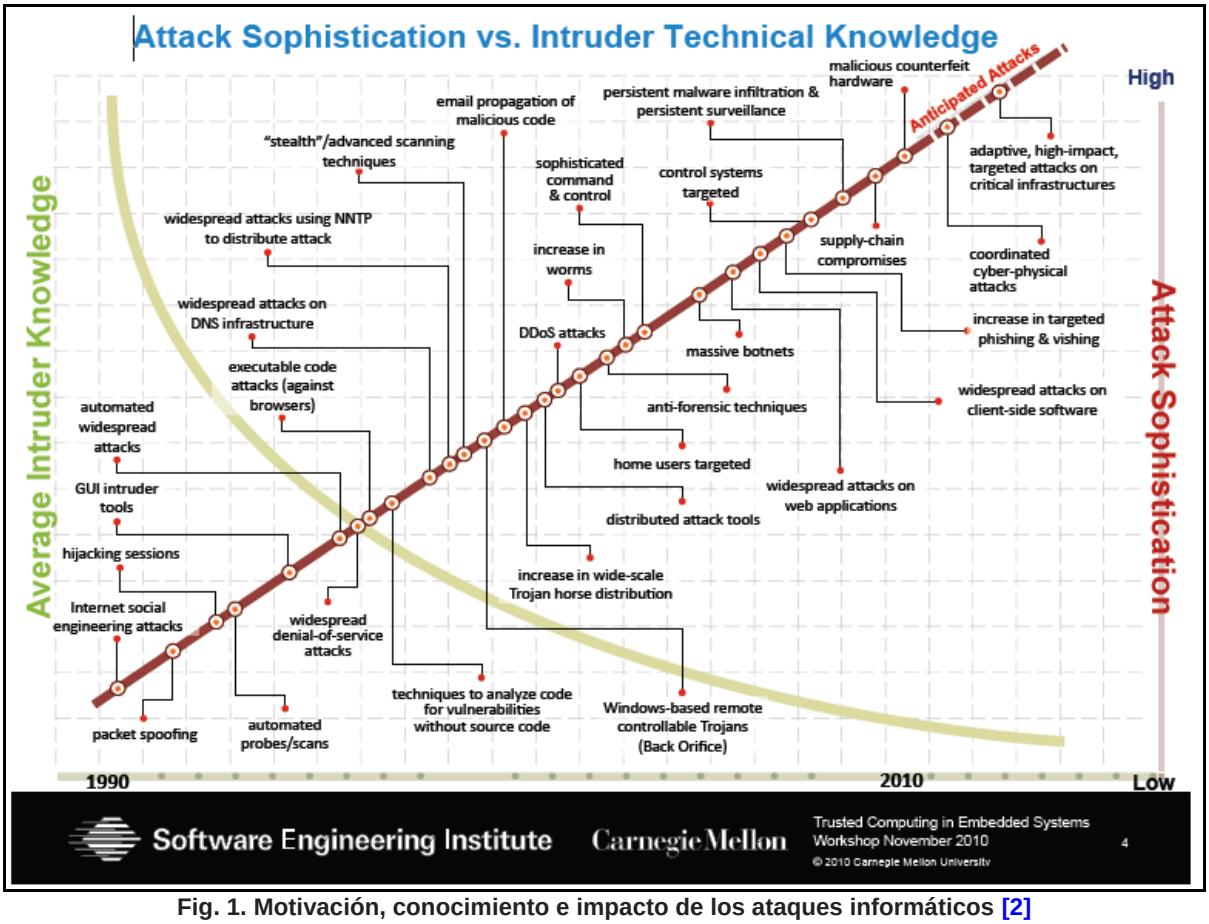

Fig. 1. Motivación, conocimiento e impacto de los ataques informáticos [2]

5. CIENCIA FORENSE

5.1. Principio de Locard

Edmon Locard fue uno de los pioneros de la criminalística a principios del siglo XX y su tratado consistió en la siguiente apreciación: "Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto" [3]. Este principio ha permitido obtener notables evidencias en lugares insospechados de esos tiempos, como por ejemplo huellas dactilares, huellas en arcilla y barro, sangre, cabello o restos en partes del cuerpo humano. Basado en lo anterior podemos deducir que un criminal siempre dejará un rastro en una escena o una acción

cometida, por lo tanto la forense digital ha aprovechado este principio como un apoyo a la gestión de la recolección de las evidencias digitales dejadas en un sistema informático después de realizar un acto ilícito.

5.2. Clase de Evidencia

Evidencias Físicas: es la evidencia tangible que puede ser tomado de una escena del crimen que ayude a obtener datos informáticos, como lo son equipos de cómputo, router, memorias, unidades de almacenamiento externo, cámaras, equipos móviles y cualquier tipo de dispositivo electrónico que pueda contener información.

Evidencia volátil: La evidencia volátil como su nombre lo dice es aquella que permanece solo por un tiempo determinado y no es para siempre.

La información transitoria se encuentra normalmente en la memoria **RAM, en la swap ó en la memoria virtua**l, la información contenida en estas áreas es temporal mientras el equipo este encendido. Otro tipo de evidencia transitoria se puede dar cuando estamos realizado una conexión o se tiene sesión abierta en internet, esta evidencia debe ser tomada en el acto.

Evidencia digital: Es la información o datos obtenidos en los equipos tecnológicos para su posterior análisis y puedan ser presentadas como evidencias.

Esta información tiene la característica de ser copiada exactamente realizando una copia bit a bit utilizando herramientas de análisis forenses con las cuales se puede determinar que la información copiada no ha presentado modificaciones en su contenido y que permita verificar que la copia es exacta; para esto podemos utilizar algoritmos MD5 y SHA1 para generar el archivo HASH.

5.3. Principio de Admisibilidad

Según la legislación colombiana para garantizar la validez probatoria de la evidencia digital se tienen en cuenta los criterios de: autenticidad, confiabilidad, suficiencia y conformidad con las leyes y reglas de la administración de justicia, que dan lugar a la admisibilidad de la evidencia. Es importante aquí explicar puntualmente el significado de cada una de estas características:

Autenticidad: que la información obtenida se haya adquirido en la escena del acontecimiento con el fin de no alterar los medios originales. Para esto se realiza una imagen bit a bit y se utiliza el algoritmo MD5 o SHA1 para demostrar que no fue modificado.

Confiabilidad: En este paso se verifica que la evidencia obtenida proviene de una fuente verificable y creíble. En este paso se debe asegurar que los registros y logs del sistema del equipo utilizado para la recolección de la evidencia estén sincronizados y puedan ser verificados e identificados; crear una línea de tiempo donde muestre paso a paso como se realizó la recolección de la evidencia y que los medios utilizados para almacenar la evidencia sean estériles.

Suficiencia: Todas las evidencias se deben presentar y estar completas para poder adelantar el caso; se debe realizar una correlación de eventos que afiance la presentación y desarrollo de las evidencias.

Conformidad con las leyes y reglas de la administración de justicia: la forma como es obtenida y recolectada la evidencia digital se enmarca claramente en las leyes y procedimientos vigentes en Colombia.

6. COMPUTACIÓN FORENSE

La computación forense hace parte de las disciplinas de las ciencias del derecho y de la computación y se enfoca en el análisis de los datos que pueden provenir de un equipo de cómputo o de una infraestructura informática como una red o subred que puede incluir cualquier medio de almacenamiento fijo o removible y que cumple con el principio de admisibilidad ante una entidad investigativa y pueda ser admisible en una audiencia frente a una corte. La evidencia digital puede ser utilizada en:

- Investigaciones de fraude
- Robo de identidad o de propiedad intelectual
- Fuga de información
- Pleitos civiles
- Demandas
- Delitos informáticos.

6.1. Ciencias forenses de la computación

La ciencia forense de la computación ofrece ventajas competitivas en el mundo de la investigación digital, que han permitido avances significativos en el mundo tecnológico con los logros importantes que se citan a continuación:

- Analizar evidencias en formato digital, lo que antes era un mito.
- Verificar la integridad de la evidencia en mención.
- Reconocimiento de la evidencia digital.
- Estudio de los diferentes formatos en que se encuentra almacenada la información.
- Identificación de los propietarios de la información, cómo se modifica, quién la modifica, quien tiene perfil para manipular la información.
- Habilidades técnicas y procedimientos forenses.
- El manejo y control de los documentos electrónicos.

6.2. Características de las evidencias digitales

La evidencia digital es el componente fundamental de cualquier investigación forense. Los profesionales de la computación forense tienen algunos retos con la información a intervenir y los atributos de éstos es así como se debe de entender las siguientes características de la evidencia digital, que pueden ser: eliminadas, copiadas, alteradas, volátil, duplicables.

Al sistema de archivos del equipo a investigar es factible obtenerle la línea del tiempo, para comprobar la transformación cronológica de los datos. También es importante anotar que existen herramientas que permiten identificar si las evidencias han sido alteradas.

Al final de este documento se explica paso a paso el análisis forense y hace énfasis en las características de las evidencias digitales.

6.3. Actividades de la computación forense

Las actividades de la computación forense se realizan siguiendo un orden secuencial como se muestra a continuación en la figura 2.

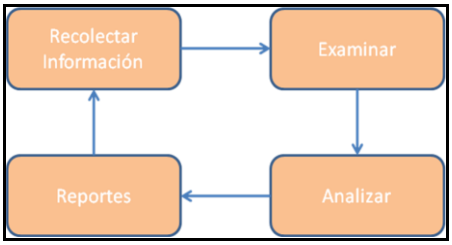

Fig. 2. Elaboración propia

- **Recolección**: Realizar la identificación de las posibles fuentes de datos y realizar una adecuada recolección de las evidencias encontradas en un equipo de cómputo, unidades externas, redes de datos, equipos móviles, etc. Luego de la identificación de los potenciales datos se debe desarrollar un plan para adquirir la información y verificar la integridad de éstos [4].

- **Examinar**: En esta etapa se examinan los datos encontrados utilizando técnicas y herramientas para ayudar al investigador a determinar cuáles datos son realmente importantes y le aportan a la investigación, también se puede obtener información de que sistema operativo utilizó, que tipo de conexión obtuvo, detalles como origen y contenido, tipos de datos digitales como gráficos, documentos de textos, aplicativos, o rastros (logs) del sistema que puedan ayudar a dar fuerza a la evidencia [4].

- **Análisis**: En el análisis se revisa la información examinada y determina lugares, objetos, eventos, relación entre las evidencias halladas y se llega a alguna conclusión para determinar quién, cómo, cuando y donde sucedieron los hechos [4], [5].

- **Entrega de informes:** Esta es la parte final del proceso donde se entrega la presentación basada en lo encontrado en la fase de análisis. El informe debe ser claro y conciso utilizando un lenguaje entendible y sin tecnicismos cuidándose solo de presentar las evidencias encontradas y no dar o sugerir culpables. Debe contener un orden cronológico y vincular los datos probatorios con fechas y horas detalladas, si es del caso hacer referencia a la ley correspondiente que se está violando. [4], [5].

7. LEGISLACIÓN

Existe normatividad desde tres frentes: la legislación informática, legislación penal y la legislación civil.

La legislación civil permite responder a personas y a sus bienes si es de carácter patrimonial o moral. Por su lado la legislación penal vela por los daños a los bienes jurídicos protegidos por el estado.

El análisis de la evidencia digital deberá cumplir con los requisitos de admisibilidad, pertinencia, suficiencia y legalidad establecidas por la ley, los documentos electrónicos deben ser aceptados por el juez sin valorar antes su autenticidad y seguridad. Para que los documentos digitales sean admitidos como evidencias se deben de tener en cuenta las siguientes leyes:

- La Ley 527 de 1999 conocida como la ley del comercio electrónico y su decreto reglamentario 1747 de 2000, reconoció fuerza probatoria como documentos a los mensajes de datos.
- El artículo 10º de la Ley 527/99 regla: "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil. Lo anterior satisface el requisito de que la información conste por escrito, equiparándolo así al documento escrito tradicional
- La Corte Constitucional en sentencia C-662 de junio 8 de 2000, con ponencia del Magistrado Fabio Morón Díaz, al pronunciarse sobre la constitucionalidad de la Ley 527 de 1999, hizo las siguientes consideraciones: (...) "El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento [6].
- Con la promulgación de la ley 1273 de 2009 se da mayor admisibilidad a las evidencias digitales, en esta ley se modifica el código penal buscando la preservación integral de los sistemas de información y las comunicaciones.
- La ley 1273 de 2009 “De la Protección de la información y de los datos”

7.1. Capítulo I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación

Artículo 269C: Interceptación de datos informáticos

Artículo 269F: Violación de datos personales

- Artículo 269G: Suplantación de sitios web para capturar datos personales.

- Artículo 269H: Circunstancias de agravación punitiva

7.2. Capítulo II
De los atentados informáticos y otras infracciones.

- Artículo 269I: Hurto por medios informáticos y semejantes
- Artículo 269J: Transferencia no consentida de activos
- Artículo 58. Circunstancias de mayor punibilidad.

8. PROBLEMAS PARA LA ACEPTACIÓN DE LAS EVIDENCIAS DIGITALES
Uno de los grandes obstáculos para la aceptación de evidencia digital en Colombia, es la carencia en los códigos procesales penales de normas especializadas destinadas a salvaguardar la cadena de custodia y admisibilidad de la evidencia digital. Esta falencia afecta a todas las partes involucradas incluyendo al juez encargado de administrar justicia que en algunos casos por el desconocimiento e incertidumbre técnica prefiere apartarse del material probatorio digital.

La factibilidad técnica que existe para alterar la evidencia digital conocida como técnica anti forense es utilizada comúnmente por la defensa para desvirtuar la solidez del material probatorio, por lo cual es fundamental que cada operación realizada sobre la información y medios sea según los procedimientos oficiales establecidos, utilizando las mejores practica descritas por los organismos oficiales que incluyen la estricta documentación y toma de evidencia de cada proceso de manipulación. Existen mecanismos tecnológicos que permiten sustentar la solidez de la evidencia y sus alteraciones, para esto el perito informático debe apoyarse en los sistemas de correlación de eventos, logs de auditoría, sistemas de detección de intrusiones, registro de autenticación, autorización y estampas de tiempo para sustentar sus apreciaciones.

Quizás uno de los retos más importantes que tiene la administración de justicia en el mundo en este momento es que no existen barreras geográficas para los delitos informáticos donde la jurisdicción de un solo incidente involucra múltiples legislaciones de estados y países, obligando a la parte acusatoria a ligarse al ámbito local en el que tiene autoridad sin que se dispongan de mecanismos sólidos de cooperación internacional.

Otro obstáculo para la aceptación de la evidencia digital podría denominarse “tecnicismo” que consiste en utilizar un lenguaje científico y tecnológico que resulta en muchas ocasiones indispensable para describir de forma clara y concisa un evento. Es estrictamente necesario que el perito informático utilice un lenguaje comprensible y didáctico que le permita al juez entender los procedimientos y resultados de la investigación forense digital.

Según la sentencia C–334/10 de la corte constitucional la evidencia digital es *“frágil y volátil”, además de fácilmente manipulable. “Luego, al aportar elementos digitales en un caso, es preciso que el aparato judicial cuente con una base formal y clara sobre la admisibilidad de la evidencia digital presentada. Es decir, que la justicia pueda contar con características básicas de esta evidencia, estableciendo procedimientos básicos que le permitan verificar su autenticidad, confiabilidad, suficiencia (completitud) y en conformidad con las leyes establecidas”* [7].

9. PASO A PASO EN LA RECOLECCIÓN DE LAS EVIDENCIAS

9.1. Factores críticos de éxito
La computación forense debe enfocarse como una estrategia para combatir los delitos informáticos, en este sentido al manipular los equipos informáticos debemos tener presente lo siguiente:

- Ajustar el sistema donde se realiza el análisis *antes* de la recolección de la evidencia.
- En el análisis de los medios se debe verificar que los medios son vírgenes y que nunca han sido utilizados para no distorsionar la integridad de la información.
- Adicionar datos propios al sistema de archivos del equipo que se pretende analizar.
- Evitar afectar procesos del sistema.
- Evitar accidentalmente, tocar las líneas del tiempo.
- Utilizar Herramientas o comandos que no alteren la imagen y para su visualización realizar el montaje como solo lectura.
- Las evidencias se utilizan principalmente para encontrar datos específicos concernientes a la actividad criminal.
- Utilizar máquinas forenses y herramientas automatizadas para examinar gigabytes de datos.
- Utilizar técnicas que enfaticen la recolección de la evidencia digital de una adecuada que cumplan con mecanismos aceptados por quien los utilicen como prueba aceptable en investigaciones o en tribunales.
- Minimizar la pérdida de datos y evidencias.

10. GUÍA DE TRABAJO

10.1. Pasos para el análisis forense en Colombia
Antes de iniciar la recolección de la evidencia es necesario tener muy claro los procedimientos que garanticen la cadena de custodia del material probatorio. La Fiscalía General de la República de Colombia, publica en el 2004 el MANUAL DE PROCEDIMIENTOS DEL SISTEMA DE CADENA DE CUSTODIA, “Este manual contempla las normas, el proceso y los procedimientos del sistema de cadena de custodia que permitirán alcanzar niveles de efectividad para asegurar las características originales.

Cabe resaltar que este manual está enfocado al manejo de evidencia física por lo cual es necesario tomar acciones para salvaguardar la evidencia digital,

por ejemplo en “aseguramiento del lugar de los hechos” se contempla un aislamiento físico del material con el propósito de que este no sea alterado, en un entorno digital este aislamiento debe contemplar la desconexión total de la red y de los mecanismos de acceso remoto sin caer en el error de apagar el sistema o prender si se encuentra apagado.

En el mismo manual la “Recolección, embalaje y rotulado del elemento de prueba o evidencia” no se tiene en cuenta los mecanismos tecnológicos necesarios para el embalaje de evidencia digital que podrían ocasionar la pérdida de la información, se deberían contemplar mecanismos de control para fuentes de energía estática y electromagnetismo, condiciones extremas de calor y humedad que podrían generar incluso Geotrichum (hongos) en los medios de almacenamiento.

De igual manera en la “Presentación del elemento en diligencia judicial” es necesario el acompañamiento del perito informático forense para la valoración científica, se recomienda que el perito cuente con el reconocimiento de alguna organización reconocida [8].

La evidencia digital podría estar representada en archivos, proceso en ejecución en el sistema, archivos temporales, registros, tiempo de encendido del sistema, fechas de accesos a recursos, imágenes y videos etc.

Para recolectar la evidencia es muy importante considerar las buenas prácticas debido a que no existe un procedimiento único oficial abalado para estos fines, el RFC 3227 - Guidelines for Evidence Collection and Archiving se convierte en una buena guía de la cual destacamos en principio el orden en que debe ser recolectada la evidencia iniciando con la información más volátil almacenada en medios de este tipo como memoria RAM, memoria cache, tablas de procesos, tablas de enrutamiento, entradas ARP y sistemas de archivos temporales. Para terminar finalmente recolectando la información menos volátil como los sistemas de archivos y topologías de red [9].

El paso siguiente después de la recolección de la información es establecer un mecanismo mediante el cual podamos asegurar la integridad de los datos, para este propósito son utilizados los algoritmos de resumen como el MD5 y SHA1 que arrojan como resultado un valor alfanumérico de longitud fija llamado HASH, estos algoritmos pueden recibir como entrada una cadena de caracteres ó archivos de cualquier tamaño y permiten asegurar que los documentos digitales no han sido alterados durante la investigación. Los algoritmos más comúnmente utilizados son:

Tabla 1. Algoritmos de HASH

Algoritmo	Tamaño del resultado en bits
MD2	128
MD4	128
MD5	128
PANAMA	256
RIPEMD	128
RIPEMD-128	128
RIPEMD-160	160
RIPEMD-256	256
RIPEMD-320	320
SHA-0	160
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512
Tiger2-192	192
WHIRLPOOL	512

En la utilización de los algoritmos de hash no podemos dejar pasar por desapercibido la baja probabilidad que existe que al menos dos entradas arrojen un valor de resultado idéntico esto es conocido como colisión y afecta a todos los algoritmos debido a que se pueden utilizar como entrada del algoritmo un número infinito de cadenas de caracteres pero como resultado siempre obtendremos un valor de longitud limitado en el caso de MD5 de 128 bits lo que quiere decir 2^{128}=3’402823669 * 10^{38} de posibles combinaciones.

Es importante resaltar que los medios de almacenamiento, no manejan la información a niveles tan pequeños como bits o bytes, sino que la manejan en grupos llamados clúster, sector o bloque. La cantidad de bytes agrupados en estos depende del “sistema de archivos” es decir el formato que tenga el medio de almacenamiento. Por ejemplo, el que usa Windows se llama NTFS (New Technology File System) en este el tamaño de sus clúster es de 512 bytes. La importancia de estos clúster es que el medio de almacenamiento lleva un registro de qué clúster pertenece a qué archivo o si éste no ha sido asignado a un archivo. Esto no se hace por dejar evidencia, si no porque los medios de almacenamiento, necesitan para un adecuado funcionamiento dichos registros y se llevan en la MFT (tabla de asignación de archivos por sus siglas en ingles File Asignation Table).

Un hecho significativo es que cuando se borra un archivo éste realmente no es borrado del medio de almacenamiento, lo que ocurre es que se registra en la MFT que estos clúster no están asignados y por esta razón no se puede acceder a él directamente. Pero los bits que conformaban este archivo siguen intactos en el medio de almacenamiento y por tanto el archivo que fue borrado puede ser recuperado

Para asegurar la aceptabilidad de la evidencia recomendamos utilizar mínimo dos algoritmos de

HASH simultáneamente o utilizar los algoritmos que arrojan como resultado cadenas de mayor longitud como SHA-512, WHIRLPOOL.

Para garantizar la aceptabilidad en el análisis forense es necesario realizar una copia exactamente idéntica a los datos originales, para esto se utilizan las copias en la unidad de almacenamiento más pequeño que existe como lo es la ***copia bit a bit***.

Para estas copias bit a bit existen innumerables herramientas y equipos físicos que tiene un alto nivel de fiabilidad pero recomendamos utilizar el programa "dd" que está incluido en la mayoría de compilaciones de Linux y permite en compañía de NETCAT realizar copias incluso por red.

Una vez adquirida la imagen es necesario obtener la línea de tiempo que contiene cronológicamente la creación, modificación, acceso y eliminación de los archivos contenidos.

Para una correcta interpretación cronológica es necesario comparar el reloj interno del sistema del cual se extraen los datos y un servidor de tiempos NTP para definir la hora real de los eventos. También es una buena práctica utilizar un servidor NTP para documentar con hora exacta cada una de las operaciones realizadas sobre los datos.

Para el procesamiento de la evidencia es necesario utilizar herramientas y comandos que no alteren la información analizada de ser posible en modo solo lectura. Sin las herramientas adecuadas, con solo abrir un archivo pueden ser alteradas las fechas de última modificación.

Para el análisis de la evidencia resulta muy útil la búsqueda de palabras claves dentro de todos los archivos para lo cual se recomienda crear un diccionario de palabras concernientes al caso investigado.

Otro de los pasos que nos encontramos al momento de una investigación forense es enfrentar investigaciones que en muchos casos pueden traspasar las fronteras nacionales y que por tal motivo están regidas por legislación muy diferente a la colombiana. Por esta razón es necesario utilizar procedimientos estandarizados que puedan responder a cualquier legislación por lo cual cabe recomendar la utilización de los estándares conocidos para el manejo de incidentes de seguridad informático que no son precisamente para análisis forense como la ISO/IEC 27002:2005.

Una de las partes más útiles para el análisis forense son los datos que deben ser levantados al momento de encontrar evidencia digital resaltamos los siguientes de la norma:

- ¿Qué es la evidencia encontrada?
- Son las pruebas como archivos que conducen al esclarecimiento del delito.
- ¿Quién encontró la evidencia?
- La evidencia debe ser encontrada por especialistas informáticos forenses.
- ¿Cómo encontró la evidencia?
- La utilización de técnicas que permiten el análisis mediante las líneas de tiempo.
- ¿Cuándo encontró la evidencia?
- En el momento del análisis.
- ¿Dónde encontró la evidencia?
- En Memoria volátil, sistemas de archivos, redes de cómputo.
- ¿Quién recuperó la evidencia?
- Forense informático.
- ¿Cómo recuperó la evidencia?
- Utilizando herramientas que garanticen la admisibilidad de los archivos digitales.
- ¿Dónde recuperó la evidencia?
- En equipo y medios estériles donde previamente se realizó copia bit a bit del medio incautado.
- ¿Cómo preservar la evidencia?
- En medios estériles, y el embalaje en recipiente que permitan conservar la integridad del dispositivo, además de realizar un MD5 o SHA1.

También se puede utilizar el SP800-61 del NIST "*National Institute of Standards and Technology*" en su guía de manejo de los incidentes de seguridad en computadores de donde pueden ser extractados algunos principios claves para sustentar la admisibilidad de la evidencia encontrada [4], [10].

Más importante aunque la misma evidencia es la presentación que se realiza de los resultados para ser abalados como material probatorio. Es recomendado utilizar un lenguaje sin tecnicismos, claro y amable sin emitir juicios con una impecable redacción, se debe tener muy claro que sus interlocutores son en su mayoría abogados y personas del común que no tiene conocimientos técnicos para asimilar la contundencia de la evidencia.

Finalmente es muy importante presentar el reporte en orden cronológico narrando de forma ordena y fluida cada uno de los hallazgos encontradas durante el análisis, evitando emitir juicios.

10.2. Resumen paso a paso

1. La incautación debe realizarse por el informático forense para asegurar la admisibilidad de la evidencia.
2. Recolectar, incautar, aislar y asegurar la evidencia.
3. Tomar una imagen bit a bit de los discos, memorias USB, encontradas, si es el caso.
4. Conservar la integridad de la evidencia. Sacar un Md5 o sha1 para la imagen, archivo o fichero encontrado.
5. Procesamiento de la evidencia al ser embalado, rotulado, firma y fecha del funcionario que hace la incautación.
6. Todos los procedimientos realizados deben ser documentados y catalogados con fechas y descripción del procedimiento

7. No modificar la evidencia de ninguna forma, evitar romper la cadena de custodia de la evidencia o del medio.
8. Análisis de la evidencia
9. Cuando tenga una imagen de cualquier medio de almacenamiento (discos, memorias, dispositivos móviles, cámaras etc.) sacar línea de tiempo de las imágenes. En estas encontramos creación, modificación, acceso y eliminación de los archivos contenidos.
10. Montar la imagen para ver su contenido, tener en cuenta que cuando monte la imagen no se realicen modificaciones de su contenido en ninguna de sus formas, para realizar su análisis.
11. Realizar reporte con fechas, orden cronológico de lo encontrado y entregar conclusión de lo sucedido en el mismo orden.
12. Generar un registro de seguridad de todo el procedimiento antes, durante y después para ser presentado ante un juez.

11. CONCLUSIONES

La combinación de diferentes técnicas empleadas en el análisis forense ofrece al investigador las evidencias necesarias para demostrar un hecho ocurrido en un sistema tecnológico.

Todo evento realizado en sistema deja un registro del suceso y puede ser obtenido por el especialista así haya sido borrado por el atacante.

Las bitácoras y la correlación de eventos son la fuente más importante de los investigadores forenses. Se denota que estamos obligados a fortalecer más estas herramientas para una labor más integral de quienes estamos en este mundo de la forense digital.

Cada vez más nos acercamos a los hechos reales de los delitos informáticos y uno de los factores ha sido la utilización de herramientas forenses.

REFERENCIAS

[1] J. Cano. Computación forense descubriendo los rastros Informáticos. Online [En. 2009].

[2] Software Engineering Institute. Carnegie Mellon University. Trusted Computing in Embedded Systems - Challenges. Online [Nov. 2010].

[3] G. Zucarddi & J. D. Gutiérrez. "Informática Forense". Online [Nov. 2006].

[4] K. Kent, S. Chevalier, T. Grance & H. Dang. National Institute of Standards And Technology. "Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86", Online [Aug. 2006].

[5] J. E. Bonilla. Computación Forense. Online [Nov. 2009].

[6] Congreso de la República. Ley 527 de 1999. Online [Mayo. 2012].

[7] Corte Constitucional de Colombia. Sentencia C-334/10 corte constitucional. Online [Junio. 2010].

[8] Fiscalía General de la Nación. Manual de procedimientos para cadena de custodia, Fiscalía General de la Nación, p. 23, ISBN 958-97542-8-7.

[9] D. Brezinski & T. Killalea. Guidelines for Evidence Collection and Archiving. IETF. Online [Feb. 2002].

[10] Norma técnica Colombiana NTC-ISO/IEC 27001. Online [Jul. 2006].