ANÁLISIS FORENSE EN DISCOS DUROS MAGNÉTICOS Y DE ESTADO SÓLIDO

Jorge Helí Espitia Ruiz
Jorge.espitia.ruiz@gmail.co
Wilmer Espitia Muñoz
Wespitia84@gmail.com
Profesor: Alvaro Escobar

Abstract

Technological advances, increased access to computer resources, increasing services offered through the network, mass internet access, e-commerce increase, make the techniques will increase in cyber-attacks on websites looking for obtain personal information, passwords, etc. access to the systems.

Nowadays are very common and frequent, because there are hackers that exploit vulnerabilities in web applications for companies and / or organizations, and the lack of good practice by the users for the use of these new technologies, which is why and based on the law 1273 of 2009, which is necessary to implement a science such as forensics to gather all the necessary evidence to lead us to present the evidence properly and help us prosecute the different types of computer crimes to which they are exposed.

So it's very important to have the necessary knowledge and process to collect the necessary evidence to report computer crime, collecting evidence in the best way possible and avoid failures in the methods of collection of evidence that lead us to alter evidence and be rejected by the procedure performed on the collection, custody and storage.

In the development of this article will focus on forensic analysis techniques, tools and procedures for obtaining, keeping and existing packaging for managing physical storage devices such as hard disk magnetic HDD (Hard Disk Drive) and Hard Drive Solid State SSD (Solid State Drive).

Keywords: Forensics, HDD (Hard Disk Drive) SSD (Solid State Drive), hash, data recovery,

Resumen

Los avances tecnológicos, el aumento en el acceso a medios informáticos, el aumento a servicios ofrecidos a través de la red, la masificación de acceso a internet y el aumento de comercio electrónico, hacen que se incrementen las técnicas en ataques informáticos a sitios web en busca de obtener información personal, contraseñas de acceso y acceso a sistemas etc.

En la actualidad estos ataques son muy comunes y frecuentes, debido a que existen delincuentes informáticos que se aprovechan de las vulnerabilidades de las aplicaciones web de las compañías y/o organizaciones, y la falta de buenas prácticas por parte de los usuarios para la utilización de estas nuevas tecnologías, es por esto y con base en la ley 1273 de 2009, que se hace necesario implementar una ciencia como es el análisis forense para poder recopilar todas la evidencias necesarias que nos lleven a presentar las pruebas de forma correcta y nos ayuden a judicializar los diferentes tipos de delitos informáticos a los que se está expuesto.

Por esto es muy importante contar con el conocimiento y proceso necesario para recaudar las pruebas necesarias y así poder reportar un delito informático, recolectando las pruebas de la mejor

forma posible y evitar fallas en los procedimientos de recolección de evidencias que nos lleven a alterar las evidencias y ser rechazadas por el procedimiento realizado en la recolección, custodia y almacenaje.

En el desarrollo de este artículo se hará énfasis en las técnicas de análisis forense, herramientas y procedimientos para la obtención, custodia y embalaje existentes para el manejo de dispositivos de almacenamiento físico como son Disco Duro magnético HDD (Hard Disk Drive) y Disco Duro de estado sólido SSD (Solid State Drive), hash.

Palabras claves: Análisis forense, HDD (Hard Disk Drive), SSD (Solid State Drive), hash, recuperación de datos

1. INTRODUCCIÓN

El avance tecnológico, la masificación de acceso a Internet, la masificación de servicios ofrecidos a través de la web, las políticas implementadas por el estado para poder llevar internet a todo el país, donde se evidencia el aumento de adquisición de estos servicios como y el auge de estas tecnologías, donde según informe presentado en la pagina del ministerio de tecnologías de la información y las comunicaciones MinTic, 8 de cada 10 colombianos acceden a internet en ciudades de más de 200 mil habitantes y un promedio de edad entre 15 y 55 años de edad, El 54 por ciento de colombianos, usuarios de internet, lo utilizan todos los días y lo hacen en un promedio de 2,6 horas al día, 300 por ciento creció el comercio electrónico entre 2010 y 2012. En 2010, el 4 por ciento de usuarios de internet realizaron compras on line y para 2012, el 16 por ciento lo hizo, El 64 por ciento de los hogares de ciudades de más de 200 mil habitantes están conectados a Internet.

El avance en las tecnologías en los dispositivos móviles y su integración con las diferentes actividades cotidianas, donde a través de estos dispositivos hoy en día se puede acceder a la gran mayoría de servicios como son pago de servicios, ingreso a correos electrónicos, redes sociales, acceso a aplicativos empresariales entre muchas otras facilidades, todos estos avances además de facilitar las tareas rutinarias y acceso a la información y muchos otros servicios, también son utilizados por personas para realizar actividades ilícitas, como se definió en la ley 1273 de 2009 donde se tipifica delitos como son acceso abusivo a un sistemas informático, obstaculización ilegitima de sistemas informático o red de telecomunicaciones, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, y demás delitos informáticos.

Es por esto que se debe contar con herramientas, procedimientos, metodologías que nos permitan recopilar todas las evidencias necesarias para poder llevar ante un juez y castigar los diferentes delitos que se cometan utilizando dispositivos electrónicos, siempre cumpliendo con los principios de integridad de la información.

2. CONTENIDO

- Objetivos.
- Tipificación delitos informáticos
- Herramientas para la recuperación de información.
- Disco Duro Magnético HDD, Discos Duros de Estado Solido SSD.
- Conclusiones y Recomendaciones.
- Referencias Bibliográficas.

3. OBJETIVOS

Los objetivos de este artículo están fundamentados en el planteamiento de un objetivo general y unos objetivos específicos que buscan dar conocimiento sobre las mejores prácticas en la recolección, recopilación, y embalaje de pruebas forenses en delitos informáticos. A continuación se describirán el objetivo general y los objetivos específicos.

- **Objetivo General.** Analizar los avances tecnológicos en los medios de almacenamiento y las herramientas utilizadas para la obtención de pruebas periciales.

- **Objetivos Específicos.** Realizar una descripción actual de los medios de almacenamiento y sus avances tecnológicos.

- Realizar una descripción de las herramientas utilizadas para la recolección de evidencias.

- Identificar las ventajas y desventajas de los discos duros magnéticos y los de estado sólido al momento de realizar un análisis forense.

4. TIPIFICACIÓN DELITOS INFORMÁTICOS.

Así como se aumenta el desarrollo tecnológico, aumentan los delitos informáticos, donde los más importantes y que van en aumento podemos encontrar delitos de pornografía infantil, robo de contraseñas y acceso a sistemas no autorizados, robo de información personal, clonación de tarjetas etc.

Como se puede evidenciar en el informe presentado por el universal el acceso a bases de datos de bancos o otras entidades no permitidos, sustraer archivos de computadores y sistemas informáticos, ingresar a redes sociales y correos personales sin autorización y la clonación de las tarjetas bancarias son algunos de los delitos informáticos que se presentan en el país y que según la fiscalía van en aumento.

En otro informe presentado por el universal el 2 de octubre de 2011 se pueden evidenciar los altos costos que deja el cibercrimen en el mundo, estos delitos tienen un costo de 114 billones de dólares al año, adicional 274 billones de dólares que sería el costo en tiempo invertido para tramitar y denunciar el delito al que fue sometido.

Para combatir estos delitos se crea la ley 1273 de 2009, el 5 de enero de 2009 por el congreso de la republica de Colombia el cual es llamado "de la protección de la información y de los datos", donde se evidencian los siguientes delitos:

269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena

de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

5. HERRAMIENTAS PARA LA RECUPERACIÓN DE INFORMACIÓN.

A continuación se relacionan herramientas forenses que nos ayudad en la obtención, recuperación y análisis de la información.

Existen gran cantidad de herramientas forenses que nos ayudan a realizar los procedimientos forenses como son herramientas para la recuperación de datos, sistemas de ficheros, malware, para análisis de registro, recuperación de contraseñas, herramientas de análisis de red, análisis de memoria, herramientas para análisis de correo electrónico, montaje de disco, algunas de ellas son:

- Encase, FTK Imager utilizadas para la extracción de imágenes forenses.
- USB Write utilizada para bloquear puertos USB.
- Forensic, Incident para el manejo de datos volátiles.
- Encase, FTK Imager programas utilizados para el análisis.
- Get Data Back. PandoraRecovery programa para recuperación de archivos.
- Encase, FTK Imager programas para extracción de imágenes forenses.
- Existen gran cantidad de herramientas forenses que nos ayudan en las tareas de recuperación, análisis, presentación y embalaje de pruebas, pero lo más importante es elegir las herramientas que cumplan con los estándares y requisitos técnicos para la presentación de las pruebas sin tener problemas al momento de presentar estas evidencias ante el juez.

6. DISCO DURO MAGNÉTICO HDD, DISCOS DUROS DE ESTADO SOLIDO SSD.

Discos Magnéticos HDD: (Hard Disk Drive), es un dispositivo de almacenamiento no volátil, donde se encuentran instalados todos los programas e información necesarios para poder interactuar con el computador, este dispositivo está compuesto por platos o discos unidos por un eje que gira a gran velocidad dentro de una caja metálica sellada, estos dispositivos dependiendo del tipo de conexión puede ser SATA, IDE, SCSI, SAS, con los avances tecnológicos encontramos discos de diferentes tamaños desde gigas hasta teras. En estos tipos de discos se ha avanzado en las herramientas de análisis forense, donde encontramos diferentes tipos de herramientas para recuperación, restauración de la información, herramientas que nos permiten recuperar datos borrados, poder realizar copia de la información sin alterar los datos originales, recuperar sectores dañados y acceder a la información que se encuentra en estos sectores que son algunas de las técnicas utilizadas por los delincuentes para ocultar las evidencias, una de estas herramientas es el AccesData Forensics Toolkit (FTK).

Unidades de estado sólido: (*Solid Disk Drive* – SSD en inglés) es un elemento electrónico basado en memorias flash NAND, el cual define un tipo de memoria no volátil diseñado como almacenamiento auxiliar. Todo este sistema es gobernado por un controlador, que establece un conjunto bloques de memorias NAND que actúan como un arreglo en miniatura, lo cual permite aumentar la velocidad de acceso, ya que es posible realizar varias lecturas y escrituras al mismo tiempo, haciendo que el dispositivo sea más resistente a fallos.[1] (SÁNCHEZ IGLESIAS).

Las unidades de estado sólido a diferencia de los discos duros magnéticos tradicionales, no tienen componentes mecánicos, ni tiempos de latencia de rotación, sino componentes electrónicos basados en memorias no volátiles que a través de controladores como el FTL, es posible interpretarlos como discos magnéticos para efectos de acceder a ellos de manera tradicional.

A la fecha se advierten múltiples ventajas de estas unidades sobre los discos magnéticos dentro de las cuales se tienen: (BLOG Happy SysAdmin 2011).

[1] SÁNCHEZ IGLESIAS, A. (?) ¿Qué es un disco duro SSD? Disponible en:http://computadoras.about.com/od/preguntas-frecuentes/a/Que-Es-Un-Disco-Duro-Ssd.htm (Consultado: 21-01-2014)

- Mayor rapidez de lectura, incluso 10 veces más que los discos duros tradicionales más rápidos gracias a arreglos internos de memorias en una misma unidad.
- Baja latencia de lectura y escritura, cientos de veces más rápido que los discos mecánicos.
- Lanzamiento y arranque de aplicaciones en menor tiempo - Resultado de la mayor velocidad de lectura y especialmente del tiempo de búsqueda. Pero solo si la aplicación reside en flash y es más dependiente de la velocidad de lectura que de otros aspectos.
- Menor consumo de energía y producción de calor, resultado de no tener elementos mecánicos.
- Sin ruido: La misma carencia de partes mecánicas los hace completamente inaudibles.
- Mejorado el tiempo medio entre fallos, superando 2 millones de horas, muy superior al de los discos duros.
- Seguridad, permitiendo una muy rápida "limpieza" de los datos almacenados.
- Rendimiento determinístico - a diferencia de los discos duros mecánicos, el rendimiento de las unidades de estado sólido es constante y conocido a través del almacenamiento entero. El tiempo de "búsqueda" es constante.
- El rendimiento no se deteriora mientras el medio se llena. Son inmunes a la fragmentación propia de los discos magnéticos
- Menor peso y tamaño que un disco duro tradicional de similar capacidad.
- Son resistentes: soportan caídas, golpes y vibraciones sin estropearse y sin des calibrarse como pasaba con los antiguos discos duros, gracias a carecer de elementos mecánicos.
- Borrado más seguro e irrecuperable de datos; es decir, no es necesario hacer uso del Algoritmo Gutmann para cerciorarse totalmente del borrado de un archivo.

No obstante lo anterior, estas nuevas unidades de almacenamiento presentan algunas limitaciones conocidas a la fecha que deben ser tenidas en cuenta frente al uso de las mismas, como advertencias que motiven acciones de seguridad y control frente a la pérdida de datos que puede presentarse.

Los principales inconvenientes son:

- Alto costo por gigabyte almacenado.
- El tiempo medio de vida entre fallos (*Mean Time Between Failures*): la longevidad de este tipo de unidades es más corto que el de disco duro estándar por el hecho de que el número de ciclos de escritura a cualquier celda de memoria es limitada y una vez que se han consumido su cuota para ese bloque, el disco empieza a ser poco fiable.
- El tamaño de almacenamiento disponible en gigabytes. Es una situación que conforme evolucione la tecnología se irá superando

Retos de las unidades de estado sólido para la computación forense (WIEBE 2013): Como quiera que las unidades de estado sólido, establecen bondades tecnológicas importantes, muchas de ellas implican limitaciones importantes para adelantar investigaciones forenses en informática dado que, como hemos visto previamente cualquier operación de escritura en una memoria flash exige una acción de borrado previo.

De otra parte, como anota WIEBE "el sistema operativo puede acelerar la degradación en el funcionamiento de la unidad de estado sólido, mediante el uso del comando TRIM. Este comando es una innovación reciente en la arquitectura de almacenamiento, que permite al sistema operativo indicarle al dispositivo de almacenamiento de estado sólido que un área particular del mismo está disponible para la limpieza y la reutilización. Por ejemplo, después que un archivo ha sido eliminado por el usuario, el sistema operativo le indicará a la unidad de estado sólido a través de TRIM el área que abarca el archivo eliminado. Después de recibir la orden de TRIM, el SSD moverá el archivo al espacio reservado para provisión, donde finalmente será liberado y marcado para su reutilización"[2].

Esto significa que a diferencia de los discos magnéticos donde se indicaba a través de una marca del sistema operacional la condición del espacio disponible o no asignado, en las unidades de estado

[2] WIEBE, J. (2013) Forensic Insight into Solid State Drives. *Digital Forensic Investigator*. Summer. Disponible en:http://www.dfinews.com/articles/2013/05/forensic-insight-solid-state-drives (Consultado: 23-01-2014).

sólido el comando TRIM elimina la capacidad de recuperar datos sobre los SSD, purgando los datos borrados antes que el sistema operacional llegue allí. (BELL y BODDINGTON 2010, REGAN 2009).[3]

Por otro lado, tenemos las limitaciones propias del controlador FTL que puede ser utilizado por los atacantes para manipular la forma de acceso y distribución de los bloques de las memorias flash disponibles, logrando generar estrategias de ocultamiento de información como marcado de bloques defectuosos, fallas en los algoritmos de recolección de basura o lo que es peor, disminuir el tiempo de vida útil de las unidades de estado sólido, acelerando los ciclos de escritura sobre los bloques disponibles.

Un desafío adicional es el ejercicio de limpieza eficaz de los SSD, toda vez que "los programas existentes de limpieza de discos no son efectivos a la hora de ingresar a fondo en los discos para eliminar la existencia de información allí disponible, dado que todo el tiempo se está moviendo información de bloques ocupados a bloques libres. Para ello se proponen variaciones del controlador FTL, con el fin de establecer funciones adicionales para borrado seguro que eliminan todos los restos de información en los bloques reservados de la unidad de estado sólido. (LEE, HEO, CHO, HONG y SHIN 2008; WEI, GRUPP, SPADA y SWANSON 2011; SHEWARD 2012)"[4]

Por lo tanto, herramientas como EnCase® que van a la vanguardia con los cambios (en cada versión mejora la capacidad de soportar éste tipo de tecnología), conjuntamente con los investigadores y a través de las herramientas, se están enfrentando al desafío de establecer qué se puede recuperar en los SSD.

Los investigadores forenses deben conocer, qué tanto el proveedor de sistemas operativos y los fabricantes de discos duros SSD, implementaron el comando TRIM que prolonga la vida útil de los SSD e impide la degradación de su rendimiento.

Formas de evitar el comando TRIM: Hay que tener en cuenta que si tenemos conectado un disco SSD a un bloqueador de escritura el recolector de basura continuará funcionando y por lo tanto destruyendo información.

La única opción sería desconectar físicamente el controlador integrado chip flash y acceder a la información directamente, utilizando la técnica conocida como Chip off. Pero hay que tener en cuenta que la técnica del Chip off no es para nada sencilla y hay muchas probabilidades de que no se obtenga absolutamente nada.

En un estudio llevado a cabo por la Universidad Carnegie Mellon, se encontró que en los discos que no usaron TRIM, la recuperación de datos fue posible en casi todos los casos, pero en los discos con TRIM la recuperación fue únicamente del 27% en promedio. Igualmente un grupo de científicos de la universidad de California dice haber diseñado un dispositivo basado en FPGA que ofrece un acceso directo a la memoria flash sin pasar por el controlador. De todas maneras no hay información y no se sabe si es válido para todos los modelos SSD o para sólo uno en concreto.

Las condiciones previamente establecidas, "supone que las herramientas forenses actuales deben ser revisadas para identificar y analizar en detalle el funcionamiento de las unidades de almacenamiento de estado sólido, para comprender la nueva ilusión del sistema de archivos a través del FTL, entender que el borrado efectuado sobre este tipo de medios es irreversible por la limpieza intrínseca de la tecnología para aumentar su velocidad y ahora sus sustentaciones técnicas no podrán basarse en la lógica de los discos tradicionales de cilindros, pistas y sectores, sino relacionadas con direcciones de bloques

[3] BELL, G. y BODDINGTON, R. (2010) Solid state drives: the beginning of the end for current practice in digital forensic recovery. *The Journal of Digital Forensics, Security and Law*. Vol 5. No. 3. Disponible en: http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf (Consultado: 10-01-2014)

[4] LEE, J., HEO, J., CHO, Y., HONG, J. y SHIN, S. Y. (2008) Secure deletion for NAND flash file system. *Proceedings of SAC'08 – 2008 ACM Symposium on Applied Computing*. Disponible en:http://eoslab.ssu.ac.kr/pdf/2008-5.pdf (Consultado: 10-01-2014)

lógicos asociados con compuertas NAND, que de manera secuencial se asignan y liberan."[5].

7. CONCLUSIONES Y RECOMENDACIONES.

- Al analizar un SSD se puede tornar complicado acceder a los archivos borrados, dado que siempre hay que tener en cuenta realizar una copia lógica de este para poder comprobar su paridad con el original en un futuro.

- Lo único cierto es que la tecnología seguirá avanzando y los investigadores forenses se enfrentarán a éste y otros retos más en cuanto análisis forense se trata.

- Los investigadores forenses en informática deben comenzar a entender en profundidad esta tecnología (SSD) toda vez que lo que conocen sobre medios de almacenamiento magnético, no podrá ser extrapolado a esta nueva tecnología.

- Es muy importante y esencial escoger muy bien las herramientas a utilizar en el proceso del análisis forenses estas pueden ser un factor determinante en el fallo del juez ante la presentación de las pruebas de los diferentes delitos informáticos.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] Ministerio de las comunicaciones MINTIC, Nivel de digitalización y acceso a nuevas tecnologías. Disponible en: http://www.mintic.gov.co/index.php/8-sabia/1908-8-de-cada-10-colombianos-acceden-a-internet (Consultado 24-01-2014)

[2] Noticia publicada en eluniversal "Fiscalía advierte aumento de delitos informáticos en Colombia", Disponible en:http://www.eluniversal.com.co/cartagena/nacional/fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia-102898 (Consultado el 24-01.2014)

[3] Ley 1273 de 2009, Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html (Consultado el 25-01-2014)

[4] Herramientas forenses, Disponible en: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html (Consultado el 25-01-2014)

[5] Diferencias Forenses Entre Discos Duros de Estado Solido Discos Duros de Platos. Disponible en: http://www.andresvelazquez.com/diferencias-forenses-entre-discos-duros-de-estado-solido-y-discos-duros-de-platos/ (Consultado el 26-10-2014).

[6] Unidades de estado sólido. El reto de la computación forense en el mundo de los semiconductores. Disponible en: http://insecurityit.blogspot.com/2013/06/unidades-de-estado-solido-el-reto-de-la.html (Consultado el 26-01-2014)

[7] BELL, G. y BODDINGTON, R. (2010) Solid state drives: the beginning of the end for current practice in digital forensic recovery. The Journal of Digital Forensics, Security and Law. Vol 5. No. 3. Disponible en: http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf (Consultado: 10-01-2014)

[8] BLOG Happy SysAdmin (2011) Solid State Drives, some theory and a selection of videos. Disponible en:http://www.happysysadm.com/2011/07/solid-state-drives-some-theory-and.html (Consultado: 9-01-2014)

[9] LEE, J., HEO, J., CHO, Y., HONG, J. y SHIN, S. Y. (2008) Secure deletion for NAND flash file system. Proceedings of SAC'08 – 2008 ACM Symposium on Applied Computing. Disponible en:http://eoslab.ssu.ac.kr/pdf/2008-5.pdf (Consultado: 10-01-2014)

[10] OLSON, A. y LANGLOIS, D. (2008) Solid state drives. Data reliability and lifetime. Imation research document. Disponible en:http://www.csee.umbc.edu/~squire/images/ssd1.pdf (Consultado: 20-01-2014)

[11] REGAN, J. (2009) The forensic potential of flash memory. Naval Postgraduate School. Unpublished Master Thesis. Disponible en:http://simson.net/clips/students/09Sep_Regan.pdf (Consultado: 20-01-2014)

[5] SÁNCHEZ IGLESIAS, A. (?) ¿Qué es un disco duro SSD? Disponible en:http://computadoras.about.com/od/preguntas-frecuentes/a/Que-Es-Un-Disco-Duro-Ssd.htm (Consultado: 21-01-2014)

[12] SÁNCHEZ IGLESIAS, A. (?) ¿Qué es un disco duro SSD? Disponible en:http://computadoras.about.com/od/preguntas-frecuentes/a/Que-Es-Un-Disco-Duro-Ssd.htm (Consultado: 21-01-2014)

[13] SHEWARD, M. (2012) Rock solid: Will digital forensics crack SSD?Infosec Institute Resources. Disponible en:http://resources.infosecinstitute.com/ssd-forensics/ (Consultado: 22-01-2014)

[14] TAL, A. (2002) NAND vs. NOR flash technology. The designer should weigh the options when using flash memory. Disponible en:http://www.electronicproducts.com/Digital_ICs/NAND_vs_NOR_flash_technology.aspx (Consultado: 22-01-2014)

[15] WEI, M., GRUPP, L., SPADA, F. y SWANSON, S. (2011) Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of 9th USENIX Conference on File and Storage Technologies. Disponible en:http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf(Consultado: 23-01-2014)

[16] WIEBE, J. (2013) Forensic Insight into Solid State Drives. Digital Forensic Investigator. Summer. Disponible en:http://www.dfinews.com/articles/2013/05/forensic-insight-solid-state-drives (Consultado: 23-01-2014)

[17] El Reto Forense En Discos De Estado Sólido (SSD) – EnCase Forensic. Disponible en: http://recorriendo-los-caminos-de-encase.blogspot.com/2013/08/el-reto-forense-en-discos-de-estado.html (Consultado: 24-01-1024).

[18] Empirical analysis of solid state disk data retention when used with contemporary operating systems. Disponible en: http://www.dfrws.org/2011/proceedings/17-349.pdf (Consultado: 25-01-2014)

[19] Definiciones discos duros, Disponible en: http://es.wikipedia.org/wiki/Disco_duro. (Consultado el 27-01-2014).

[20] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Documentación. Presentación de Tesis, Trabajos de Grado Y Ortos Trabajos de Investigación. NTC 1486, Sexta Actualización. Bogotá D.C. ICONTEC, 2008. 41 p.

[21] Referencias Bibliográficas. Contenido, Forma y estructura. NTC 5613. Bogotá D.C. ICONTEC, 2008. 38p.