



CARRERA DE ANÁLISIS DE SISTEMAS

TEMA:

Análisis de recuperación de información usando la metodología “SANS” para dispositivos de almacenamiento.

AUTOR:

Henry Wilfrido Morocho Morocho
Daniel Fernando Segarra Fajardo

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
TECNÓLOGO EN ANÁLISIS DE SISTEMAS

TUTORES:

- Ing. Marco Guamán
- Ing. Juan Pérez

CUENCA – ECUADOR, 2020

Resumen

A medida que pasa el tiempo los dispositivos de almacenamiento van evolucionando conjuntamente que la tecnología, y como consecuencia de esto surgen los ataques a dichos dispositivos, siendo reconocidos como una amenaza real, que vulneran la seguridad y disponibilidad de la información contenida en los equipos de resguardo; en donde se almacenan datos personales como corporativos importantes que son de absoluta confidencialidad pero por consecuente pueden ser manipulados, clonados y desviados por gente que son ajenas a la información sensible que se tiene, produciendo un mal uso y perjudicando en un punto importante a la imagen.

Los ataques y estrategias que se generan para obtener esa información sensible van evolucionando día tras día, lo cual ha generado que las personas se enfoquen en el desarrollo de metodologías, como una respuesta eficiente ante los incidentes en cuanto a la pérdida de información de los dispositivos de almacenamiento, todo esto es parte de la informática forense la cual integra metodologías y procedimientos que son indispensables en el procesamiento de evidencias mediante el correcto uso de la cadena de custodia, permitiendo a los peritos informáticos recopilar indicios y protegiéndolos, por que pueden a llegar ser resultados sustentables o probatorias para resolver cualquier conflicto en el este involucrado los dispositivos de almacenamiento.

Abstract

As time passes, the storage devices are evolving together with the technology, and as a consequence of this, attacks on said devices arise, being recognized as a real threat, which violate the security and availability of the information contained in the equipment of guard; where personal data are stored as important corporate data that are of absolute confidentiality but as a result can be manipulated, cloned and diverted by people who are outside the sensitive information you have, causing misuse and damaging in an important point to the image .

The attacks and strategies that are generated to obtain this sensitive information are evolving day after day, which has generated that people focus on the development of methodologies, as an efficient response to incidents regarding the loss of information from devices of storage, all this is part of the forensic computer science which integrates methodologies and procedures that are indispensable in the processing of evidence through the correct use of the chain of custody, allowing the computer experts to collect clues and protect them, because they can arrive at sustainable or probative results to resolve any conflict in the case involving storage devices.

Palabras clave

Metodología SANS, informática forense, recuperación de archivos, metadatos, extracción, peritos, transporte.

Key words

SANS methodology, computer forensics, file recovery, metadata, extraction, experts, transport.

Dedicatorias

Primeramente quiero agradecer a Dios por haberme concedido la salud y fortaleza hasta este punto de mi vida, la dedicación y esfuerzo de cada día es un sacrificio que toda persona debe hacer para lograr tener éxitos en su vida tanto profesional como personal, el desempeño que realice por alcanzar mi sueño se ve reflejado en este documento el cual avalúa mi entrega y dedicación para ser un profesional y dar un orgullo inmenso a toda mi familia y en especial a mí que responde al fruto de tanto tiempo de altos y bajos pero que a partir de todo pronóstico he podido seguir adelante y estar a un paso de obtener mi título anhelado. Agradezco infinitamente a mi madre por su entrega, apoyo incondicional en todo momento ya que es un orgullo haber recibido y seguir recibiendo consejos y buenos deseos, a mi hermana por ser una persona muy especial para mí, las dos son mis pilares fundamentales; y que estoy agradecido en todo momento; no hace falta decir que lo prometido está por cumplir, por que todo ya está cumplido.

Henry Wilfrido Morocho Morocho

Dedico esta investigación primeramente a Dios quién supo guiarme por el camino del bien , darme fuerzas para seguir adelante y sobresalir los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento, a mis queridos padres, por su constante apoyo incondicional, porque siempre creyeron en mí y porque siempre me brindaron todo su apoyo para seguir adelante, dándome claros ejemplos de superación y entrega, porque en gran parte gracias a ustedes, hoy culmino una de mis objetivos de vida planteados, ya que siempre estuvieron sosteniéndome en los momentos más difíciles de mi carrera, y porque el orgullo que sienten por mi hizo que llegue hoy donde estoy. A mi abuelita que también siempre estuvo en todo conmigo, a mis hermanos y amigos que me llenaron de mucha valentía para terminar este proceso. Gracias por haber fomentado en mí el deseo de superación y anhelo de triunfo en la vida.

Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos más difíciles.

Daniel Fernando Segarra Fajardo

Introducción

Los dispositivos de almacenamiento a medida que pasa el tiempo han ido tomando posesión muy importante para los seres humanos pro que, si bien durante la antigüedad no había un método tecnológico para preservar la información, todo el proceso de resguardo lo hacia el cerebro en cierto modo que dicho organismo no puede procesar toda la información solo los puntos más importantes y que se recuerdan más.

Con la aparición de los dispositivos de almacenamiento (disco duro, memoria RAM, USB, cinta magnética, disco duro externo, discos ópticos), todos los datos que se reúnen se pueden almacenar en dichos dispositivos, ya que se pueden encontrar cualquiera de ellos en diferentes capacidades de resguardo.

En la actualidad el activo más importante para las personas es su información, puesto que su perdida es de un valor incalculable. Los dispositivos de almacenamiento a medida que pasa el tiempo son indispensables para el manejo de información a nivel personal y empresarial. Los dispositivos de almacenamiento, ha dejado de ser un lujo para convertirse en una necesidad; la brecha entre funcionalidad y precio de los dispositivos se ha vuelto cada vez más delgada, y por eso su uso es masivo.

En este contexto, es fácil que un dispositivo se encuentre involucrado en algún incidente que describa un delito informático y sea necesario analizar la información contenida en ese dispositivo.

Así mismo, las metodologías de análisis forense cumplen de manera parcial las fases de recuperación de información, esto genera que un análisis quede incompleto al momento de aplicar informática forense. En consecuencia, es necesario evaluar metodologías y herramientas que permita crear un modelo simplificado de análisis forense.

Lo que se presentara a continuación en el documento tratara sobre el análisis de diferentes metodologías de análisis forense los cuales servirán de base para generar una nueva guía la cual se desarrollara de una manera simplificada haciendo constancia de que la guía tendrá fases las cuales serán concretas y directas hacia lo que se pretende llegar que es el resultado

de una investigación de caso, todo esto será enfocado a los dispositivos de almacenamiento por que es hay donde se tiene problemas al momento de solicitar o resguardar la información de entidades y personas.

Sin más preámbulo y esperando que la información y el documento desarrollado sea de suma utilidad, prosigo.

Objetivos

Objetivo General

Aplicar la metodología SANS para la recuperación de información en dispositivos de almacenamiento.

Objetivos Específicos

- Revisar las metodologías de informática forense para formular un nuevo modelo de recuperación de información.
- Implementar un servidor de informática forense que permita utilizar herramientas de análisis de datos
- Describir los resultados de recuperación de la información, utilizando el modelo propuesto de la metodología SANS.

Justificación

El avance de la tecnología en cuanto a los dispositivos de almacenamiento ha dado paso a una nueva generación en la cual, dichos dispositivos son de diferentes tamaños además de que son de diferente capacidad de resguardo lo que los hace más importante para su transporte por las personas.

A medida que esto sucede rápidamente, también, los diferentes problemas suceden en cuanto a la manipulación de los datos por personas ajenas las cuales pueden provocar daños sensibles tanto a nivel corporativo como a nivel personal, siendo de muy alto riesgo la pérdida de información de los dispositivos de almacenamiento.

El tener una guía la cual cumpla con fases simplificadas, utilizando herramientas de acuerdo a su confiabilidad es algo positivo por que todo eso se asocia al manejo de la informática forense la cual representa el desarrollo de fases en las cuales se ven evidencias de algún tipo de pérdida de información de los dispositivos de almacenamiento.

Para ello la justificación del proyecto inicia con el estudio de la metodología SANS, la cual se basa en el correcto manejo y extracción de la información; así también se continuará con el análisis y comparación con otras metodologías del análisis forense, en donde a partir del proceso que se ejecute hasta el momento se analizará las diferentes herramientas de acuerdo al contexto en el que se esté desarrollando el estudio del mismo.

Una vez desarrollado todo lo anterior se generara una nueva guía basada en el estudio de las metodologías de informática forense tomando como guía base la metodología SANS, la cual estará ligada a fases con sus respectivas herramientas de solución para un determinado caso, todo esto basándose en el correcto manejo y extracción de la información, verificando que las evidencias no queden al descubierto y que sean propensas a cualquier tipo de infección la cual podría dañar todo el proceso que se realiza en el ejercicio de resolución.

Una vez realizado todo lo anterior se desarrollará un caso de investigación en la cual se pondrá a prueba la nueva guía desarrollada para el análisis de los dispositivos de almacenamiento, con lo cual se demostrará que una buena y simplificada guía puede ser una forma más directa y concreta de llegar a una solución objetiva.

Capítulo I

1. Problemática

Los dispositivos de almacenamiento a medida que pasa el tiempo son indispensables para el manejo de información a nivel personal y empresarial. Los dispositivos de almacenamiento, ha dejado de ser un lujo para convertirse en una necesidad; la brecha entre funcionalidad y precio de los dispositivos se ha vuelto cada vez más delgada, y por eso su uso es masivo. El objetivo básico de un dispositivo de almacenamiento es el de resguardar y procesar la información, para ello todos sus componentes deben funcionar, así como el sistema operativo en el cual se está ejecutando y donde se puede verificar la información de una manera ordenada.

La información que se maneja dentro de los dispositivos de almacenamiento son un valor de activo muy importante, la posibilidad de que la información pase a manos ajenas o que sea interceptadas por personas ajenas, puede tener repercusiones muy importantes a nivel personal como corporativa.

Hay que tener en cuenta que hoy en día cuando se produce una pérdida de datos ya sea temporal o definitiva puede traer consigo muchos perjuicios los cuales conllevan a los siguientes puntos:

- **Perdidas económicas**
- El dinero y tiempo perdido por los procesos desarrollados para recuperar la información que se ha perdido y se necesita recuperar.
- La pérdida a consecuencia de la indisponibilidad de la información.
- La pérdida temporal de trabajos, así como también de proyectos ya terminados, que pueden llegar a poner en serio riesgo el desarrollo corporativo y profesional.
- **Daño de imagen**
- En caso de pérdida de datos sensibles personales y corporativos.
- Publicación de datos de carácter privado en medios de comunicación masivos.

Las causas por las que se produce la pérdida de información, y que afectan a las partes tales como la integridad y disponibilidad son varias, entre las cuales tenemos las siguientes:

- **Fallos físicos en los dispositivos**

Causados por motivos externos (cortes de energía o diferencias en la intensidad del voltaje), o de manera interna en los mismos dispositivos (degradación de los mecanismos al final de su vida útil).

- **Fallos humanos**

Esto a partir del borrado o formateado de las unidades de almacenamiento o por una manipulación errónea de dichos dispositivos, a consecuencia de la mala preparación del personal y las decisiones fallidas a la hora de intentar la recuperación de información tras un incidente son los causantes de estos fallos.

- **Fallos en el software**

Fallos de manera imprevista por parte de los sistemas operativos por reinicios, o mal funcionamiento de las herramientas de diagnóstico.

- **Virus o Software malicioso**

En ocasiones lo más seguro es que dichos softwares instalados en los ordenadores acrediten un fallo en el sistema o el robo de información donde todos esos datos pasan a un equipo remoto.

En este contexto, es fácil que un dispositivo se encuentre involucrado en algún incidente que describa un delito informático y sea necesario analizar la información contenida en ese dispositivo. Así mismo, las metodologías de análisis forense cumplen de manera parcial las fases de recuperación de información, esto genera que un análisis quede incompleto al momento de aplicar informática forense.

En consecuencia, es necesario evaluar metodologías y herramientas que permita crear un modelo simplificado de análisis forense.

Capítulo II

2. Marco Referencial

2.1. Marco Teórico

2.1.1. Metodología del Instituto SANS

El instituto SANS es una organización cooperativa de investigación y educación para profesionales de la seguridad. El manejo adecuado de una investigación forense es clave para luchar contra los delitos informáticos, requiriendo un profundo conocimiento de muchas áreas para una investigación adecuada.

(Pinto, 2014)

Particularidades	Ventajas	Desventajas
Formatos para establecer la cadena de custodia	Cubre con todas las etapas para hacer una investigación forense.	No propone métodos para realizar la adquisición de evidencia de grandes volúmenes de datos.
Define lugares en donde se puede encontrar información oculta dentro de los sistemas operativos Windows y Linux.	Toma en cuenta el cuidado de la cadena de custodia.	No propone métodos de análisis para volúmenes grandes de datos. Es específica para dispositivos que cuenten con sistemas operativos Windows o Linux.

2.1.2. Metodología Kevin Mandia Y Chris Prosis

Propone un paso llamado prepreparación en el cual el grupo encargado de

Particularidades	Ventajas	Desventajas
Propone un paso llamado pre-preparación en el cual el grupo encargado de reaccionar ante un incidente se anticipa a ellos preparando las herramientas necesarias y conocimientos de la infraestructura	Cumple con todas las etapas generales de una investigación forense	No propone métodos para el análisis de grandes volúmenes de información.
Proporciona una lista de los principales ataques que se presentan hacia una computadora y recomienda una estrategia de respuesta	Proporciona métodos para realizar el análisis de datos.	Está enfocada para la investigación de plataformas Windows NT/2000, UNIX y routers Cisco. Dejando fuera todos los dispositivos que utilicen una plataforma diferente, y deja de lado cualquier otro dispositivo periférico y digital.
reaccionar ante un incidente se anticipa a ellos preparando las herramientas.		

2.2.1 Dispositivo De Almacenamiento

se puede afirmar que es una unidad con la capacidad de leer, escribir y almacenar información. Hoy en día se cuenta con muchas categorías de unidades de almacenamiento, y se puede encontrar una amplia variedad de dispositivos capaces de guardar grandes cantidades de datos.

Existen diversos tipos de dispositivos de almacenamiento. Entre ellos se destacan los llamados dispositivos de almacenamiento secundario; estos son los que pueden almacenar información en su interior, como los discos magnéticos, las tarjetas de memoria y los pendrives; en esta categorías también entran las unidades de almacenamiento óptico, como las grabadoras de Blu-Ray, DVD Rom o CD Rom.

Actualmente, son muy populares los dispositivos construidos sobre memoria flash, que se basa en impulsos eléctricos; esta memoria se usa en gran cantidad de dispositivos, desde unidades externas para PC hasta pequeños aditamentos para móviles.

El almacenamiento de la información siempre ha estado presente en el desarrollo de la humanidad, desde la antigüedad hasta el presente. La necesidad del hombre de salvaguardar su legado para las generaciones futuras ha sido una característica de todas las culturas humanas.

Transmitir el legado histórico de una civilización significa perpetuar su historia y la de los ciudadanos, es por esto que siempre han existido los almacenes de pergaminos o libros, conocidos como bibliotecas.

En esencia la idea permanece, solo que en la actualidad, la preservación de la información se ha extendido a prácticamente todas las áreas humanas. No solo las históricas y la tecnología han jugado un papel fundamental en esta expansión, sino también el desarrollo de dispositivos que han permitido

mantener la memoria particular de cada quién o de una organización, e incluso de una nación, como un activo muy importante de su legado histórico.

Un típico dispositivo de almacenamiento es el denominado disco rígido. El mismo fue desarrollado por IBM para sus equipos hace varias décadas, aunque en ese momento sus características técnicas diferían bastante de las actuales. En efecto, los mismos, a pesar de que conceptualmente eran parecidos a los actuales, tenían un inmenso tamaño y peso, además de tener una capacidad muy reducida. En este sentido, el paso del tiempo fue dando lugar a una mejora en estos aspectos, circunstancia que no obstante parece llegar a su fin. Se componen de platos o discos que se dividen en sectores y sobre los que opera un cabezal a una distancia ínfima. Se encuentran sellados para evitar la entrada de polvo, circunstancia que podría afectar el comportamiento de los mismos. Además, requieren una determinada presión de aire para su correcto funcionamiento, circunstancia que los torna inoperantes en grandes alturas.

Otro tipo de dispositivo de almacenamiento son los dispositivos ópticos, como el CD ROM, el DVD o el Blue Ray. Los mismos consisten en unidades en formas de disco que son leídas de modo óptico, con un láser. También fueron evolucionando con el paso del tiempo en lo que respecta a capacidad de almacenamiento, pudiendo albergar en la actualidad a varios gigabytes de memoria.

En la actualidad se han popularizado dispositivos contruidos sobre memoria flash, que se funda en impulsos eléctricos. La misma se utiliza para todo tipo de dispositivos, desde unidades externas para computadoras hasta pequeños aditamentos para móviles. En el caso de las computadoras hogareñas se postulan para reemplazar al mentado disco rígido con las unidades de estado sólido. No obstante, todavía su costo es elevado por lo que pasará algún tiempo hasta que esta situación sea una realidad.

(MX., 2014)

2.3.1. AUTOPSY

Es una interfaz gráfica para el análisis forense informático, mediante herramientas de líneas de comandos. El cual permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar. Estos análisis se centran en análisis genérico de sistemas de archivos y líneas temporales de ficheros. Se puede analizar los discos de Windows y UNIX y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3).

Autopsy es una plataforma forense digital y una interfaz gráfica para The Sleuth Kit y otras herramientas forenses digitales. Es utilizado por los examinadores de la ley, militares y corporativos para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara.

2.4.1. Modos de análisis

Un análisis de muerte se produce cuando un sistema de análisis específicos se utiliza para examinar los datos de un sistema sospechoso. En este caso, la autopsia y las herramientas Sleuth se ejecutan en un entorno de confianza, por lo general en un laboratorio. Autopsy y TSK apoyo básico testigo, perito, y los formatos de archivo AFF.

Un análisis en directo se produce cuando el sistema sospechoso está siendo analizada, mientras que se está ejecutando. En este caso, Autopsy y las herramientas Sleuth se ejecuta desde un CD en un entorno de confianza. Se utiliza con frecuencia durante la respuesta a incidentes, mientras que el incidente está siendo confirmado. Después de que se confirme, el sistema puede ser adquirido y realizado un análisis de muerte.

2.3.1. Técnicas de Búsqueda de la evidencia

Listado de archivos: Analizar los archivos y directorios, incluyendo los nombres de los archivos borrados y los archivos con nombres basados en Unicode.

Contenido del archivo: El contenido de los archivos pueden ser vistos en hexadecimal, raw, o los caracteres ASCII; los que se puede extraer. Cuando se interpretan los datos, se desinfecta para evitar daños en el sistema de análisis local. El software no se utiliza ningún tipo de lenguajes de script del lado del cliente.

Bases de datos de Hash: Búsqueda de archivos desconocidos en una base de datos de hash para identificar rápidamente como bueno o malo. Autopsy utiliza el NIST Biblioteca Nacional de Referencia de Software (NSRL) y bases de datos creadas por el usuario de los archivos más conocidos.

Clasificación de tipos de archivos: Clasificar los archivos basándose en sus firmas internas para identificar los archivos de un tipo conocido. La autopsia puede también extraer solamente imágenes gráficas (incluyendo miniaturas). La extensión del archivo también se puede comparar con el tipo de archivo para identificar los archivos que pueden haber tenido su extensión cambiada para ocultarlos.

Cronología de la actividad de archivo: En algunos casos, tener una línea de tiempo de actividad de los archivos puede ayudar a identificar las áreas de un sistema de archivos que pueden contener pruebas. La autopsia puede crear líneas de tiempo que contiene entradas para la modificación, acceso, y el cambio (MAC).

Buscar palabra clave: búsquedas de palabras clave de la imagen del sistema de archivos se puede realizar utilizando cadenas de caracteres ASCII y expresiones regulares grep. Las búsquedas se pueden realizar en cualquiera de la imagen completa del sistema de archivos o simplemente el espacio no asignado. Un archivo de índice pueden ser creadas para agilizar las

búsquedas. Las cadenas que son buscados de manera frecuente se puede configurar fácilmente para la búsqueda automatizada.

Análisis de metadatos: Los metadatos estructuras contienen los detalles sobre los archivos y directorios. La autopsia le permite ver los detalles de cualquier estructura de metadatos en el sistema de archivos. Esto es útil para recuperar el contenido eliminado. La autopsia buscará los directorios para identificar la ruta completa del archivo que ha asignado a la estructura.

Análisis de datos de unidades: la unidad de datos es donde el contenido del archivo se almacena. La autopsia le permite ver el contenido de cualquier unidad de datos en una variedad de formatos, incluyendo ASCII, hexdump, y cuerdas. El tipo de archivo también se da y la autopsia buscará los metadatos para identificar las estructuras que ha asignado la unidad de datos.

Detalles de la imagen: Pueden ser vistos los detalles del sistema de archivos, incluyendo el diseño en el disco y el tiempo de actividad. Este modo proporciona información que es útil durante la recuperación de datos.

(contributors, 2019)

(CARRIER, 2003-2020)

2.3.1. OS FORENSIC

La suite OsForensics es una pieza clave en investigaciones forenses digitales (digital forensics, como se conoce en inglés), un todo en uno que permite localizar pistas, mirar en el interior de archivos y sus cabeceras y, finalmente, organizar e indexar todos los datos hallados para un tratamiento posterior y su presentación.

La herramienta te permite investigar cualquier clase de información contenida en un soporte informático, tanto visible como oculta, para adquirir la evidencia necesaria a presentar en un caso ante un jurado, o simplemente para conocer aspectos ocultos de tu ordenador, como contraseñas, metadatos e información oculta en archivos. La herramienta trabaja en 3 fases:

1. Descubrimiento

La herramienta realiza búsquedas de gran rapidez en toda la superficie del disco o dispositivo elegido, creando además un índice de información. Es capaz de extraer contraseñas, descifrar archivos y recuperar elementos borrados de diferentes sistemas de archivos: Windows, Mac y Linux.

2. Identificación

Las evidencias y actividades halladas son comparadas mediante su valor hash contra una base de datos. Además, se analizan todos los archivos y permite crear una línea de tiempo (timeline) de toda la actividad del usuario, para presentarla en orden cronológico.

3. Administración

Finalmente, la suite nos permite organizar todas nuestras evidencias en un guión ordenado, incorporando los datos del examinador forense, presentando los hechos acontecidos y adjuntando datos de otras herramientas forenses si es necesario.

(Sánchez, 2018)

2.3.1. The Sleuth Kit

The Sleuth Kit es una colección de herramientas de análisis forense de volumen de sistema y archivos. Las herramientas del Sistema de Archivos permiten examinar el sistema de archivos de una computadora sospechosa, de una manera no intrusiva. Esto, debido a que las herramientas no confían en el sistema operativo para los procesos del sistema de archivos, de esta manera es posible ubicar contenido borrado y oculto.

Las herramientas de volumen de sistema (manejador de medios) permiten examinar la disposición de los discos y otros medios. The Sleuth Kit soporta particiones DOS, particiones BSD (etiquetas de disco), particiones Mac, partes Sun (Índice de volúmenes) y disco GPT. Con estas herramientas, se puede identificar donde se ubican las particiones y extraerlas, de manera que pueda ser analizadas con las herramientas de análisis del sistema de archivos.

Cuando se realiza un análisis completo del sistema, puede ser tedioso conocer todas las herramientas en línea de comando. Autopsy Forensic Browser, es una interfaz gráfica para las herramientas que se incluyen en The Sleuth Kit, lo cual permite conducir más fácilmente llevar a cabo una investigación. Autopsy proporciona manejo de casos, integridad de la imagen, búsqueda de palabras clave, y otras operaciones automáticas.

Análisis con The Sleuth Kit de una memoria USB

Cuando procedemos a realizar una copia bit a bit de un dispositivo de memoria flash USB hemos de impedir que existan procesos en el sistema host (el Sistema Operativo en sí) que realicen procesos de escritura de manera transparente en el dispositivo, es decir, sin aviso alguno de que están realizando esta acción. Esto puede ocasionar la pérdida o destrucción de la evidencia, por lo tanto hay que tomar las precauciones del caso.

Existen dispositivos que cuentan con un mecanismo que bloquea la acción de escritura en ellos. Pero muchos otros no, con lo que la prioridad en el procesamiento de la evidencia digital es la preservación de la información, y que no tomen lugar cambios o modificaciones cuando se procesa una unidad de memoria flash USB como evidencia. Por ello es necesario la utilización de un bloqueador de escritura que sea preciso y flexible.

Con el objeto de detallar la utilización y los ejemplos del presente artículo, vamos a crear un directorio con el siguiente nombre: `tsk_test/` donde almacenaremos los archivos del análisis. Los únicos datos proporcionados, es que esa trata de una memoria de marca Lacie de 2GB de capacidad. Antes del proceso de copia bit a bit vamos a obtener el hash original de la evidencia, así, aplicaremos el comando `sha1sum` sobre el dispositivo `/dev/sdc` (el de nuestra memoria).

(carrier, 2003 -2020)

(Hornero, 2019)

2.3.1. Informatica Forense

Se se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes.

También puede servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta.

Los naturales destinatarios de este servicio son los estudios jurídicos aunque cualquier empresa o persona puede contratarlo.

La necesidad de este servicio se torna evidente desde el momento en que la enorme mayoría de la información generada está almacenada por medios electrónicos.

En la recuperación de información nos enfrentamos con información que no es accesible por medios convencionales, ya sea por problemas de funcionamiento del dispositivo que lo contiene, ya sea porque se borraron o corrompieron las estructuras administrativas de software del sistema de archivos. La información se perdió por un problema de fallo de la tecnología de hard y/o soft o bien por un error humano. El usuario nos indica su versión de los hechos y a menudo encontramos sobre la falla original otras que el usuario o sus prestadores técnicos agregaron en un intento de recuperación. Así es que debemos figurarnos a partir del análisis del medio qué ocurrió desde el momento en que todo funcionaba bien y la información era accesible.

En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia

para borrar, adulterar u ocultar información. Es por lo tanto esperable que el mismo hecho de esta adulteración pase desapercibido.

La informática forense apela a nuestra máxima aptitud dado que enfrentamos desde casos en que el dispositivo fue borrado, golpeado y dañado físicamente hasta ligeras alteraciones de información que pueden constituir un crimen.

Este servicio es de utilidad a empresas que llevan adelante juicios laborales con sus empleados, o con sus asociados por conflictos de intereses, a estudios jurídicos que necesitan recabar información ya sea para presentarla frente a un tribunal o bien para negociar con las partes un acuerdo extrajudicial de resarcimiento, renuncia, etc. Es de utilidad a los organismos judiciales y policiales que buscan evidencias de todo tipo de crímenes. Es un componente indispensable en litigios civiles.

(TACUARI, 2017)

2.3.1. Seguridad de la Información

La seguridad de la información permite asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización. Es un concepto amplio que no se centra en la protección de las TIC sino de todos los activos de información que son de un alto valor para la institución.

En este sentido, debemos entender a la seguridad de la información como un proceso integrado por un conjunto de estrategias, medidas preventivas y medidas reactivas que se ponen en práctica en las instituciones para proteger la información y mantener su confidencialidad, disponibilidad e integridad de la misma.

Las organizaciones y sus activos de información, sean estos físicos o digitales, se enfrentan de forma creciente a amenazas como: fraude asistido por computadora, espionaje, sabotaje, vandalismo, fenómenos naturales, descuido, desconocimiento o mal uso del tratamiento de la información por parte del recurso humano. Muchas de esas amenazas provienen de ingenieros sociales, *hackers*, empleados negligentes, errores, entre otros, que buscan dañar la integridad de una organización.

Existen dos factores importantes de la seguridad de la información:

- a. La importancia o valor de los datos de acuerdo con los intereses y necesidades de cada persona o institución;
- b. La difusión o acceso, autorizado o no, de los mismos.

vulnerabilidades

Las dimensiones de la seguridad están constituidas por tres conceptos fundamentales, presentados a continuación:

Confidencialidad: propiedad que permite que la información solo esté disponible o sea revelada a personas, entidades o procesos autorizados.

Integridad: propiedad de la exactitud e integridad de la información.

Disponibilidad: propiedad de la información para estar accesible y utilizable al solicitarlo una entidad autorizada.

(Reyes, 2013)

2.10.1. Análisis Forense Digital

El análisis forense digital es una adecuada traducción de algunos nombres o denominaciones que se utilizan en el idioma inglés, como por ejemplo: Computer Forensics, Digital Forensics o Cyber Forensics. En esencia, todas ellas exponen conceptos similares, de esta manera se puede definir el Análisis Forense Digital como un conjunto de principios y procedimientos que se acompaña con una metodología para sus procesos. Entre estos procesos se enumeran: la adquisición, la conservación o preservación, el análisis y su posterior documentación, que incluye la presentación de los resultados del proceso.

El Proceso Forense incluye, pero no se limita a las siguientes fases:

Identificación de la evidencia: La tarea inicial de una investigación es identificar la evidencia que es necesaria para el caso. Sin evidencia no existe mucho más que una opinión. Es obvio que cada caso es diferente, así es que

se necesitan diferentes tipos de evidencia en base al caso. Conociendo que la evidencia necesaria es una parte integral de una investigación satisfactoria. La regla de oro es tomar todo. Desafortunadamente, existen temas legales y logísticos con este enfoque. Siendo más realistas, se debe tomar todo y cualquier cosa que pueda estar remotamente relacionada con el caso. Se debe seguir religiosamente la cadena de custodia y las directrices de etiquetar todo lo que ha sido retirado.

Preservación de la evidencia: Antes de poder probar que se ha mantenido la integridad de los datos presentados como evidencia, se debe probar que se ha mantenido la integridad del Hardware que contiene los datos. Desde el inicio de la investigación, se deben tomar las precauciones y documentar estas precauciones, para proteger, en este caso al Hardware.

El máximo objetivo de la preservación de la evidencia es asegurarse de manera absoluta que no ha ocurrido cambio alguno desde que la evidencia fue recolectada. Se debe examinar el procedimiento de recolección y de manipulación. Tomando todas las precauciones necesarias para proteger la evidencia recolectada de daño que pueda cambiar su estado. Una precaución significativa es la descarga de electricidad estática. Se debe proporcionar protección estática a los dispositivos de la investigación. Se debe utilizarlos y realizar anotaciones que expliquen los pasos que se toman para evitar daños imprevistos.

Durante la investigación se abordarán muchos temas. No se debe manipular la evidencia hasta estar absolutamente seguro de que legalmente se puede adquirir la evidencia y que los procesos de recolección y análisis no modifican la evidencia.

Análisis de la evidencia: Antes de iniciar el examen del medio, se debe crear un hash de la copia que se ha realizado del medio original. ¿Este hash generado concuerda con el hash del medio original? Si es así, se puede proceder. Si no lo es, se debe encontrar la razón. Puede darse el caso de que ocurrió algún tipo de escritura cuando se montó la copia. O tal vez, el

proceso de copia tuvo algún falla. En cualquier caso, no se puede iniciar el análisis hasta que se tenga una copia limpia y fiable.

El proceso de análisis es una mezcla adecuada de ciencia y arte. Se tiene que desarrollar un sentido de donde buscar en primera instancia, y poseer conocimientos técnicos para extraer la información.

Documentación y presentación de resultados: Después de que el análisis se ha completado, es momento de presentar los resultados. El objetivo de cualquier caso es persuadir a la audiencia de utilizar la evidencia. La audiencia puede ser un juez, un jurado, o una junta de gerentes en una sala de conferencias. El objetivo es utilizar la evidencia que se ha recolectado para probar uno o más hechos. Incluso con una gran evidencia, el éxito del caso depende de la efectividad de la presentación.

Comenzaremos con la recopilación de la evidencia, hasta culminar con la fase tres de análisis, donde se utilizará The Sleuth Kit. A continuación de detalla información de esta herramienta.

Hasta este punto se ha expuesto el tema de Análisis forense digital, la parte conceptual, posteriormente hemos considerado la herramienta que constituye el centro sobre el que gira esta entrada; es decir The Sleuth Kit. Ahora es momento de exponer información sobre las denominadas memorias USB.

2.10.1 Memorias USB

Una unidad flash USB consta de una memoria flash tipo NAND de almacenamiento de datos integrado con una interfaz USB (Universal Serial Bus). La unidad flash USB permite escritura muchas veces, es de tamaño mucho menor a la de un disco flexible (de 1 a 4 pulgadas o de 2.5 a 10 cm.), y la mayoría de memorias USB tiene un peso menor a 28 gramos, creo que todos tenemos alguna que siempre viaja con nosotros. Las capacidades de almacenamiento van desde un rango de 64 MB (las más antiguas) hasta 128GB. Algunas permiten un millón de ciclos de escritura y borrado y retención de datos de 10 años, conectados por USB 1.1 o 2.0.

2.12.1 Sistema de Archivos

La mayoría de unidades flash son entregadas con formato para el sistema de archivos FAT o FAT32. La ubicuidad de este sistema de archivos permite que la unidad se encuentre disponible prácticamente para cualquier dispositivo con soporte USB. Además, las utilidades estándar de mantenimiento FAT puede ser utilizada para recuperar o reparar datos dañados. Sin embargo, debido a que una unidad flash aparece como un disco duro conectado al sistema, la unidad puede ser formateada nuevamente a cualquier sistema de archivos soportado por el sistema operativo anfitrión.

Las unidades flash puede ser desfragmentadas, pero proporciona poca ventaja ya que no hay una cabeza mecánica que tenga que moverse lentamente de fragmento en fragmento (las unidades flash a menudo tienen sectores internos de gran tamaño, especialmente cuando se borran, así desfragmentar implica acceder a pocos sectores para borrar un archivo). Desfragmentar, por tanto, acorta la vida útil de la unidad, dado que realiza escrituras innecesarias.

Algunos sistemas de archivos están diseñados para distribuir el uso sobre el dispositivo de memoria completo sin concentrar el uso en parte alguna (ejemplo, un directorio) esto prolonga la vida de dispositivos de memoria flash simples. Algunas unidades flash USB, sin embargo, tienen esta funcionalidad incorporada en el controlador para prolongar la vida del dispositivo, por lo tanto el usuario final debe verificar las especificaciones del dispositivo antes de cambiar el sistema de archivos por este motivo.

Tiene sectores de 512 bytes de longitud, para compatibilidad con discos duros, y el primer sector contiene el Master Boot Record (registro maestros de arranque) y tabla de particiones. Por lo tanto las unidades flash USB pueden ser particionadas como los discos duros.

(Hornero, 2019)

Capítulo III

3. Metodología de investigación

En este capítulo se muestra el desarrollo de las etapas con las que cuenta la metodología, a partir de las 8 con las que se encuentra conformada. Las etapas reflejan el manejo de evidencias, así como que activos de información son los más esenciales para proceder a realizar de manera exitosa por lo cual estas etapas son cruciales para empezar con el desarrollo del proyecto.

3.1 ¿Por qué la utilización de esta metodología?

Los usos de metodologías para un análisis forense son variados y cubren ciertos aspectos en cuanto a custodias, manejo de información, análisis y presentación. La metodología SANS es una de ellas, la cual cumple con pasos específicos que son de suma importancia para dicho análisis, los cuales cumple de una manera ordenada y respetando la línea de proceso lo cual conlleva a un resultado satisfactorio para la recuperación de información de los dispositivos de almacenamiento.

Las metodologías que son de igual similitud para la metodología SANS son las de Brian Carrier y Eugene Spafford, DOJ, DFRW, Reith, Carr y Gunsch, Mandia/ Prorise y Casey.

A continuación, se presenta una tabla en la cual se determina los siguientes aspectos que cumplen las diferentes metodologías

Metodologías							
Etapas de la investigación	Brian Carrier y Eugene Spafford	SANS	DOJ	DFRW	Reith, Carr y Gunsch	Mandia/ Prorise	Casey
Identificación		✓	✓			✓	✓
Recolección	✓	✓	✓	✓	✓	✓	✓
Análisis	✓	✓	✓	✓	✓	✓	✓
Presentación	✓	✓					

Una vez analizado las diferentes metodologías y haber demostrado en la tabla anterior que la metodología SANS cumple con los requerimientos establecidos por las etapas de investigación se acogió como la metodología base, para formar nuestra nueva guía, la cual ostentara por aplicar nuevas formas a la mecánica original de cómo se procede en la metodología.

También se hace uso de nuevas y mejoradas herramientas las cuales cumplen a cabalidad lo que los puntos establecidos de la guía necesitan demostrar.

3.2 Etapas de la metodología

La metodología SANS describe 8 pasos para el proceso forense digital, esto ayuda a mantener una viabilidad muy buena para continuar en el camino y poder asegurar la presentación adecuada de la evidencia de los dispositivos de almacenamiento. Además, es un buen punto de partida para tener un conocimiento muy racional y entendible de los principios forenses; pautas; procedimientos; herramientas y técnicas.

3.2.1 Verificación

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Reconocer el entorno y la situación en la cual se presenta el problema, con todos los detalles.	

Normalmente, la investigación en torno a la informática forense se realiza como parte de un escenario de respuesta ante incidentes; siendo el primer paso el de Verificar.

Esto hace referencia al conocimiento de la situación en donde se haya producido un incidente. Significa cual es la ¿Situación? ¿Cuál es la naturaleza del caso y sus detalles? Este paso es preliminar e importante porque ayudara a determinar las características que presenta el incidente y definir de mejor manera un enfoque para identificar; preservar y recolectar evidencia.

¿Por qué es importante el paso de verificación?

3.2.2 Descripción del sistema

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Adjuntar la información necesaria como parte del estudio en el que interviene el sistema operativo en el que se presenta el problema.	

A partir del primer paso en donde se verifica to lo acontecido al incidente, en este segundo paso se comienza a recopilar los datos sobre el incidente específico iniciando por:

- A) Tomar notas y describir el sistema al cual se va hacer el análisis.
- B) ¿Dónde se adquiere el sistema?
- C) ¿Cuál es el rol del sistema en la organización y en la red?

D) Describir el sistema operativo y su configuración general como el formato de disco, cantidad de RAM y la ubicación de la evidencia.

3.2.3 Adquisición de la evidencia

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Obtener toda la información necesaria a partir de los objetos volátiles y no volátiles que son indispensables para seguir con el procedimiento.	

La mayoría de las pruebas y recolección de información se da principalmente en los medios de almacenamiento, para generar una copia muy precisa del dispositivo hecho en esta etapa se utiliza una unidad llamada **Bit Stream Image** que es una manera diferente al de copiar. “una imagen de flujo de bits de una unidad de almacenamiento es una copia clonada de la misma, incluyendo sectores y clústeres, lo que hace que sea posible recuperar archivos que fueron eliminados de la unidad”. Las imágenes de flujo de bits se usan generalmente cuando se realizan investigaciones forenses digitales para así evitar manipulaciones que alteren la evidencia obtenida, evidencia tal que no se pierde ni se corrompe:

Esta etapa incluye:

- A) Identificar posibles fuentes de datos.
- B) Adquirir datos volátiles y no volátiles.
- C) Verificar la integridad de los datos y garantizar la cadena de custodia.

Puesto que los datos volátiles cambian con el tiempo, el orden en el cual los datos son recolectados es muy importante. Una orden en el proceso de adquisición es “Los datos volátiles deben adquirirse primero”, unos ejemplos de datos volátiles son:

- A) Conexiones de red.
- B) Sesiones de inicio de sesión.
- C) Procesos corriendo.
- D) Abrir archivos.
- E) El contenido de la RAM.

Después de haber terminado con la recopilación de los datos volátiles, se continua con el siguiente paso de recopilación que son los datos no volátiles tales como el disco duro.

“Para recopilar datos del disco duro, normalmente hay tres estrategias para hacer una imagen del flujo de bits”.

- A) Usar un dispositivo de hardware como Write Blocker (en caso de que pueda desconecte el sistema y retire el disco duro).
- B) Usar una respuesta a incidentes y un juego de herramientas forenses que se usaran para arrancar el sistema.
- C) Uso de la adquisición del sistema en vivo (local o remotamente) que podría ser utilizado cuando se trata con sistemas encriptados o sistemas que no se pueden desconectar o solo se puede acceder de forma remota.

Después de haber adquirido los datos, se debe asegurar y verificar su integridad. También se debe ser capaz de describir claramente cómo se encontró la evidencia, como fue su manejo y todo lo que le sucedió, es decir, el proceso de custodia.

3.2.4 Análisis de línea de tiempo

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Determinar una línea de secuencia para concretar desde que tiempo y que cosas del sistema empezaron a modificarse para determinar una secuencia que indique el entorno y el problema al que nos presentamos.	

Después de la adquisición de la evidencia, se procederá a hacer la investigación y análisis, partiendo desde el análisis de la línea de tiempo.

“Esto es un paso crucial y muy útil porque incluye información como cuando los archivos fueron modificados, accedidos, cambiados y creados en un formato legible para personas, conocido como evidencia de tiempo MAC (el acrónimo se deriva del tiempo modificado “mtime”, el tiempo de acceso “atime” y estructuras “ctime” mantenidas por sistemas de archivos Unix)”.

La información se recopila a través de diferentes herramientas y se extraen los metadatos.

“Capa del sistema de archivos (inodo en registros Linux o MFT en Windows), y luego analizado y ordenado para ser analizado”.

Las líneas de tiempo de los dispositivos de memoria, pueden ser muy útiles para la reconstrucción de suceso. El objetivo final de este análisis de línea de tiempo es generar algo rápido e instantáneo de la actividad que se había realizado en el sistema, incluida su fecha, el artefacto involucrado, la acción y la fuente.

“la creación es un proceso fácil pero la interpretación es difícil”. La interpretación ayuda a ser precisa y se convierte en algo fácil cuando se

tiene sistemas completos de archivos y artefactos del sistema operativo de conocimiento.

Para continuar y concretar este paso, existen herramientas comerciales o de código abierto como la estación de trabajo SIFT que es un software gratuito y que se encuentra en constantes actualizaciones.

3.2.5 Análisis de medios

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Analizar y determinar líneas del tiempo en las cuales se determinara los diferentes cambios que se ejecutaron en los archivos que forman parte de los sistemas operativos a estudiar.	

En este paso, se comienza a sentir la pesadez con la cantidad de información que se podría estar observando. A todo ello se debería responder preguntas tales como:

- A) ¿Qué programas se ejecutaron?
- B) ¿Qué archivos se descargaron?
- C) ¿En qué archivos se hizo clic?
- D) ¿Qué directorios se abrieron?
- E) ¿Qué archivos fueron eliminados?
- F) ¿Dónde navegó el usuario?

Los investigadores deben contemplar en usar una técnica que permita la reducción del conjunto de datos para identificar archivos. Esto se realiza utilizando la base de datos, como objeto principal la biblioteca de referencia de software de Nation de NIST y haciendo comparaciones hash a partir de la utilización de herramientas como hfind del kit de detección.

En casos en donde se necesite analizar un sistema Windows, la persona encargada de la investigación puede crear una súper línea de tiempo. “La súper línea de tiempo incorporará múltiples fuentes de tiempo en un solo archivo, donde el analista debe tener conocimiento del mismo, también, de sistemas, artefactos de un sistema operativo y artefactos de registro para aprovechar esta técnica que reducirá la cantidad de datos a analizar.”

Otras cosas que el investigador debe buscar son:

1. Evidencia del uso de la cuenta
2. Uso del navegador
3. Descarga de archivos
4. Apertura / Creación de archivos
5. Ejecución del programa
6. Uso de la llave USB

El análisis que se realiza a la memoria es otro paso clave y muy importante para examinar los procesos no autorizados, conexiones de red, archivos DLL cargados, evidencia de inyección de código, rutas de proceso y demás otros.

Se debe tener cuidado con las técnicas anti-forenses como la esteganografía o la alteración o destrucción de los datos que afectaran en gran parte al análisis y/o conclusiones de la investigación que se realizó.

3.2.6 Búsqueda de cadenas o bytes:

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">•	

Este paso consistirá en priorizar el uso de herramientas que se centrará en buscar el nivel más bajo de imágenes en bruto. Si se sabe lo que se está buscando, se puede utilizar este método para encontrarlo. “En este paso, se utilizará herramientas y técnicas que buscarán firmas de bytes de archivos conocidos como cookies mágicas. También en este paso se realiza búsquedas de cadenas utilizando expresiones regulares.” Las cadenas de búsqueda o firmas de bytes que se buscara serán relevantes para el caso en el cual se estará tratando.

3.2.7 Recuperación de datos:

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Disponer de diferentes herramientas las cuales nos ayudaran a recuperar los datos de los dispositivos de almacenamientos que necesitamos recuperar.	

“Este es el paso en que el investigador buscará recuperar datos del sistema de archivos.” Algunas herramientas que servirán de ayuda en este paso son las que se encuentran disponibles en Sleuth Kit y otras herramientas forenses que se pueden usar para analizar el sistema de archivos, la capa de datos y la capa de metadatos. “Analizar el espacio flojo, el espacio no asignado y el análisis en profundidad del sistema de archivos es parte de este paso para encontrar archivos de interés. Tallar archivos a partir de imágenes en bruto basadas en encabezados de archivos utilizando herramientas como la más importante es otra técnica para reunir más evidencia.”

“Slack Space es el espacio no utilizado en un clúster de disco. Los sistemas de archivos DOS y Windows usan clústeres de tamaño fijo. Incluso si los datos reales ser almacenado requiere menos almacenamiento que el tamaño del clúster, se reserva un clúster completo para el archivo. El espacio no utilizado se llama holgura espacio.”

“Los sistemas DOS y Windows anteriores usan una tabla de asignación de archivos de 16 bits (FAT), que da como resultados tamaños de clúster muy grandes para particiones grandes. Por ejemplo, si el tamaño de la partición es de 2 GB, cada grupo será de 32 K.

Incluso si un archivo requiere solo 4 K, se asignarán los 32 K completos, lo que da como resultado 28 K de espacio libre. Windows 95 y Windows 98 resuelven

este problema mediante el uso de una FAT de 32 bits (FAT32) que admite clúster

tamaños más pequeños que 1K.”

3.2.8 Resultado de informe:

OBJETIVO	RESOLUCIÓN
<ul style="list-style-type: none">• Presentar datos claros y concisos los cuales determinaran el origen del problema que se suscitó.	

La fase final implica informar los resultados del análisis, que puede incluir describir las acciones realizadas, determinar qué se deben realizar otras acciones y recomendar mejoras a las políticas, pautas, procedimientos, herramientas y otros aspectos del proceso forense. Informar los resultados es una parte clave de cualquier investigación.

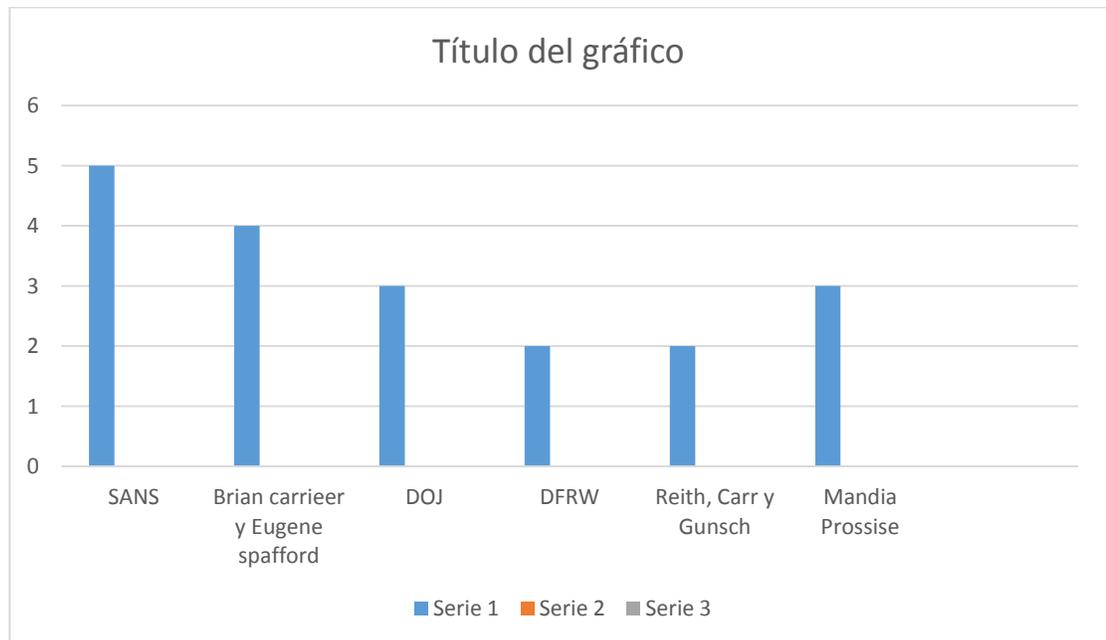
Capítulo IV

4 Análisis e interpretación de resultados

Según los estudios realizados para formalizar la nueva guía metodológica se decidió hacer una tabulación en cuanto a cómo la metodología SANS es nuestro modelo base según el tipo de las etapas de información en las cuales está estructurado nuestro tema.

Para ello se elaborará una estadística con las metodologías que se presentaron en la tabla anterior.

De tal forma que evalúa los aspectos importantes como son la identificación, recolección, análisis y presentación.



Como se puede observar en la imagen nuestra metodología base cumple con todos los requerimientos para generar un análisis completo además de incorporar herramientas y nuevas técnicas tales como los formularios

que harán que el desarrollo de la metodología sea más organizado para llegar a un bien común.

Capítulo V

5 Propuesta de investigación

En este capítulo se presentará los temas relacionados a la nueva metodología propuesta, los puntos con sus descripciones, soluciones, así como las gestiones y resultados finales que apoyan a la ejecución de este nuevo proceso ante la recuperación de la información de los dispositivos de almacenamiento.

En el análisis y comparación de las metodologías se tomó como base a la metodología SANS la cual cumple con aspectos tales como: identificación, recolección, análisis y presentación. El mismo documento consta de ocho etapas las cuales como en nuestro objetivo presentado; realizamos una nueva guía la cual consta solo de siete puntos puesto que simplificamos un punto para que el nuevo documento goce de todas las facilidades de entendimiento para cualquier persona, así como de tener simplicidad, pero siendo objetivo de acuerdo a sus fases de desarrollo.

Lo que nosotros proponemos es en determinar una nueva metodología para la investigación reuniendo en una sola guía los consejos y mejores prácticas que ya se encuentran repartidos en otros documentos que también analizan la situación de los dispositivos de almacenamiento. Transformando el documento en una guía estándar y permitiendo tener un marco común y práctico para las personas que lo necesiten.

5.1 Nueva metodología

La nueva metodología consta de siete puntos los cuales cumplen con una manera organiza de verificación, extracción y manipulación de la evidencia de una manera estricta sin intervención de factores externos, además, busca complementar cuatro puntos básicos los cuales forman parte de una estructura la cual busca preservar y encontrar solución a la perdida de información que contienen los dispositivos de almacenamiento.

5.1.1 Verificación

La primera fase consiste en determinar escenarios en los cuales se desarrolla la situación a la que se presenta como parte del problema a solucionar por parte de la persona que necesita generar su recuperación de información para lo cual es necesario tomar en cuenta la naturaleza, los detalles para poder generar un informe completo.

Para completar con este punto y su desarrollo se ha generado una investigación, presentando como criterio la utilización del programa Autopsy, el cual es una herramienta que viene incluida en el sistema operativo Caine Linux, y sirve como interfaz gráfica para las herramientas de análisis digital de investigación de The Sleuth Kit. Juntos, pueden analizar discos de Windows y UNIX y sistemas de archivos (NTFS, FAT, UFS1/2, Ext2/3). The Sleuth Kit y Autopsy son de código abierto y funcionan con plataformas UNIX/LINUX., es posible conectarse al servidor de Autopsy desde cualquier plataforma usando un navegador HTML. Autopsy provee un Administrador de Archivos y muestra detalles acerca de los datos eliminados y estructuras de sistemas de archivos.

Tal vez la mejor herramienta libre que existe para el análisis de evidencia digital. Su interfaz gráfica es un browser que basado en las herramientas en línea de comandos del Sleuth Kit, permite un análisis de diversos tipos de evidencia mediante una la captura de una imagen de disco.

Formulario de Verificación y levantamiento de información			
Descripción del delito informático			
Fecha del incidente (DD/MM/AAAA)			
Duración del incidente (00:00:00)			
Detalles del incidente			
Información general			
Área			
Nombre de la dependencia			
Responsable afectado del sistema afectado			
Nombres y Apellidos			
Cargo			
E-mail			
Teléfono		Extensión	
N° celular		Fax	
Información de equipo afectado			
Dirección IP		Nombre del Equipo	
Marca y modelo		Capacidad RAM	
Disco duro		Modelo de procesador	
Sistema Operativo		Versión	
Función del equipo			
Información que procesaba el equipo informático			
Anexo de evidencias			

5.1.2 Descripción del sistema

En este paso la persona encargada de realizar el análisis, debe enfocarse en verificar los acontecimientos previos a la ejecución del incidente, en lo consecuente se debe recopilar los datos sobre el problema empezando por tomar en cuenta algunas notas, la cual nos servirá para poder describir el sistema operativo al cual se le va hacer el análisis determinado, siguiendo pautas y ejecuciones que se producen en el paso anterior.

El sistema operativo es crucial por que es de donde parte todo, tanto el problema como la solución, para ello el sistema debe ser algo central y fundamental puesto que sin ello no se pudiera proceder al desarrollo del análisis. Las descripciones del sistema deben ser de una manera muy detallada, describiendo configuraciones generales, los formatos de disco, la cantidad de RAM, para así llegar al centro de la investigación forense.

Formulario Registro de Hardware			
Nombre del Perito			
Fecha			
Hora			
Etiqueta de Registro		Tipo Dispositivo	N° serie
Modelo		Características	N° fotos
Sistema Operativo		Estado	Ubicación
		Encendido	
		Apagado	
Descripción General			
Observaciones			
Firma Forense		Firma Testigo	

Todo el proceso en este punto de la fase se ve reflejado en el documento de formulario el cual nos brinda una manera más amplia de describir los datos que se requieren y son mas importante para llevar a cabo el lineamiento del proceso de recuperación de información.

El formulario consta de manera explícita el llenar datos hacer del sistema operativo implicado para posteriormente describir su sistema operativo, estado en el que se encontró, así como las observaciones

generales del desarrollo de la fase, también una descripción general y concisa; y por último el nombre del perito que se encuentra a cargo de la investigación.

5.1.3 Adquisición de evidencia

Las pruebas que se adjuntan se dan primordialmente a partir del análisis y recopilación de información que se encuentran dentro de los dispositivos de almacenamiento que son las memorias volátiles y no volátiles.

En este paso se deberá identificar las posibles fuentes de datos, las cuales nos proporcionan información útil por que se realizara una hipótesis desde que punto se está saliendo la información, verificando que todo esto sea de una manera íntegra en donde los datos se manejen mediante una cadena de custodia.

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

En lo que respecta al tratamiento de la evidencia digital en la CdC, En ella se incluyen los diferentes aspectos relacionados con el tratamiento de las principales pruebas digitales. Para probar la CdC, es necesario conocer todos los detalles sobre cómo se manejó la evidencia en cada paso del camino. La vieja fórmula utilizada por la

policía, los periodistas y los investigadores de “quien, que, cuando, donde, porque y como, se puede aplicar para ayudar en la investigación forense de la información.

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 fuerza 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.

El formulario de cadena de custodia determina pautas para que la evidencia no sea infectada por cualquier condición externa a la investigación y que tenga como finalidad brindar un soporte veraz de las pruebas que se necesitan para resolver el problema.

Para que dicha cadena se cumpla de una manera efectiva se debe evitar cosas ajenas a la ejecución como las suplantaciones, modificaciones, alteraciones o simplemente la destrucción del mismo. Este procedimiento es debidamente controlado ya que de aquí parte el estado en el que se encuentra el caso, la cadena de custodia se aplica a los indicios materiales y virtuales que hacen parte del desarrollo de la investigación, desde su localización hasta su valoración por las personas encargadas del caso.

Formulario Cadena de Custodia		
Fecha		
Nivel de investigación		
Identificación de Evidencia		
Extracción de evidencia		
Transporte de Evidencia		
Preservación		
Verificación y extracción de datos ocultos		
Persona a cargo de informe final:		
----- firma		

En esta etapa de la investigación el perito informático es la persona la cual deberá salvaguardar la información, puesto que es un profesional con conocimiento en el área, siendo capaz de extraer todas las evidencias con las cuales se va relacionando para llegar a la solución del problema.

Por lo tanto, el siguiente formulario avalara quien es la persona que se desempeña como perito informático el cual deberá guardar absoluta discreción con el caso que se le asigne puesto que una infección externa puede dañar todo el trabajo realizado por el mismo perjudicando varias partes de la investigación inicial.

Formulario Peritos Forenses	
Fecha	
Cedula de identidad	
Nombres	
Apellidos	
Dirección	
Teléfono	
Correo electrónico	
Profesión	
Firma	

5.1.4 Análisis de línea de tiempo

Al haber adquirido la evidencia detallada de la situación, se procederá hacer la investigación, partiendo del análisis del tiempo el cual es una forma de observar y evidenciar cambios suscitados en los dispositivos de almacenamiento desde una fecha específica hasta la actual en la que se está realizando la investigación.

En este momento de la fase de investigación es necesario describir al programa OsForensics, que es una herramienta de investigación forense, permitiendo localizar pistas, mirar en el interior de archivos, y sus cabeceras, y finalmente, organizar e indexar todos los datos hallados para un tratamiento posterior y su presentación.

Esta herramienta permite investigar cualquier información contenida en un soporte informático, donde se encuentra de manera visible u oculta: la cual a partir de la estructura y contenido se divide en tres puntos, los cuales son:

5.1.4.1 Descubrimiento

La herramienta realiza búsquedas de gran rapidez en toda la superficie del disco o dispositivo elegido, creando además un índice de información. Es capaz de extraer contraseñas, descifrar archivos y recuperar elementos borrados de diferentes sistemas de archivos: Windows, Mac y Linux.

5.1.4.2 Identificación

Después de un minucioso descubrimiento las actividades y evidencias encontradas son comparadas mediante su valor hash contra una base

de datos; después se procede a realizar un análisis de todos los archivos encontrados; después se procede a realizar un análisis de todos los archivos encontrados y permite realizar una línea de tiempo de toda la actividad del usuario, para presentarlo en un orden cronológico

Las evidencias y actividades halladas son comparadas mediante su valor hash contra una base de datos. Además, se analizan todos los archivos y permite crear una línea de tiempo (timeline) de toda la actividad del usuario, para presentarla en orden cronológico.

5.4.1.3 Administración

Después de la creación de la línea de tiempo, la herramienta nos permite organizar toda la evidencia, incorporando los datos de la persona encargada de la examinación, presentando lo acontecido y en caso de usar otra herramienta forense anexar los datos en caso de ser necesario

Finalmente, la suite nos permite organizar todas nuestras evidencias en un guion ordenado, incorporando los datos del examinador forense, presentando los hechos acontecidos y adjuntando datos de otras herramientas forenses si es necesario.

5.1.5 Análisis de medios

En este paso se determina todo lo relacionado a la manipulación de archivos y datos que se manejan, de acuerdo a los mensajes de tiempo, modificación, creación y eliminación, los cuales siguen su

secuencia dependiente del punto anterior, donde se maneja la línea de tiempo.

Donde la prioridad es analizar la memoria puesto que es lo más importante en la investigación, dando paso a los procesos no autorizados, conexiones de red, rutas de proceso que se llevan a cabo en el sistema y demás otros; teniendo precaución en la alteración manejo o destrucción de la información que afecten a todo el proceso realizado hasta este punto.

5.1.6 Recuperación de datos

Este es el último paso antes de presentar el resultado final, consiste en utilizar una herramienta llamada sleuth kit la cual es una colección de herramientas de análisis forense de volumen de sistema y archivos. Las herramientas del Sistema de Archivos permiten examinar el sistema de archivos de una computadora sospechosa, de una manera no intrusiva. Esto, debido a que las herramientas no confían en el sistema operativo para los procesos del sistema de archivos, de esta manera es posible ubicar contenido borrado y oculto.

Las herramientas de volumen de sistema (manejador de medios) permiten examinar la disposición de los discos y otros medios. The Sleuth Kit soporta particiones DOS, particiones BSD (etiquetas de disco), particiones Mac, partes Sun (Índice de volúmenes) y disco

GPT. Con estas herramientas, se puede identificar donde se ubican las particiones y extraerlas, de manera que pueda ser analizadas con las herramientas de análisis del sistema de archivos.

Cuando se realiza un análisis completo del sistema, puede ser tedioso conocer todas las herramientas en línea de comando. Autopsy Forensic Browser, es una interfaz gráfica para las herramientas que se incluyen en The Sleuth Kit, lo cual permite conducir más fácilmente llevar a cabo una investigación. Autopsy proporciona manejo de casos, integridad de la imagen, búsqueda de palabras clave, y otras operaciones automáticas; además de ello podemos utilizar otras herramientas.

En cuanto al registro de extracción de las evidencias el siguiente formulario hace referencia a como se debe llenar un documento el cual va ligado a la secuencia de resolución del problema, se toma en cuenta el nombre del perito que se encuentra a cargo de la investigación, además de los datos del sistema.

Cabe recalcar que si no se encuentra desarrollando la solución al problema es necesario transportar toda la información de manera ordenada y sin exposición a cualquier tipo de infección que pueda dañar la evidencia, por lo consecuente también se debe tomar en cuenta el nombre de la persona que va a transportar dichas evidencias, así como las características del vehículo, ara que por lo consecuente esa persona sea responsable en caso contrario de que se presente alguna anomalía en la continuación de la solución.

Formulario de extracción y transporte de evidencia		
Nombre del perito		
fecha		
Hora		
Numero de etiqueta		
Estado de dispositivo	Encendido	
	Apagado	
Hora de apagado de dispositivo	Fecha apagado de dispositivo	
Medio de almacenamiento	Medio de transporte	
Nombre de transportista	Identificación del medio de transporte	
Observaciones		
<p>_____</p> <p>Firma perito forense</p> <p>_____</p> <p>_____</p> <p>Firma Testigo Transportista</p> <p style="text-align: right;">Firma</p>		

Otro punto importante es el resguardo de evidencia que involucra a uno o más peritos informáticos los cuales estén a cargo de la investigación, este formulario hace referencia de una manera actualizada el avance en cuanto a la investigación que se va realizando o sino, si existe algún cambio en cuanto al perito una vez que el anterior haya sido removido de la investigación debe haber constancia de que el nuevo perito tiene el formulario de la investigación del formulario anterior para así con el nuevo documento sustentar una actualización para ver si existen cambios que el haya realizado.

Resguardo de la evidencia	
Nombre del Perito Forense	
Fecha	
Hora	
Número de etiqueta	
Nombre del Archivo	
Tipo de dispositivo	
Tipo de Duplicado	Herramienta de duplicado
Hora de inicio de Duplicado	Hora de fin de duplicado
Fecha de duplicado	
Medio de almacenamiento de duplicado	Número de registro de duplicado
Observaciones	

<div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%; border-top: 1px solid black; border-bottom: 1px solid black; text-align: center;"> <p>Firma Perito Forense</p> </div> <div style="width: 45%; text-align: right;"> <p>Firma Testigo</p> </div> </div>

5.1.7 Resultado de informe

Este es el punto final de todo el proceso de verificación en donde se muestra todo lo obtenido a lo largo del proceso de investigación para lo cual es necesario tener un formulario el cual describe directamente todo lo acontecido al problema que se esa o se va a solucionar, siendo un apoyo importante para determinar que causo la perdida de información en el dispositivo de almacenamiento.

Informe de Resultados
Objeto del informe
Antecedentes
Alcance
Fuentes de información

Manifestaciones
Fundamentos del informe
Resultado de los procedimientos

El formulario que se presenta es una forma más sencilla y directa de que todos los datos obtenidos a partir del ejercicio de las etapas anteriores se reflejen en dicho documento, el cual describe de manera más objetiva todo lo que ha acontecido desde sus antecedentes; que es el punto de partida para el desarrollo de la investigación.

Una vez llenado este formulario se procede a desarrollar de una manera más detallada todos los puntos mismos del documento puesto que ese servirá de informe final para resolver casos en donde se ha irrumpido con la seguridad en los dispositivos de almacenamiento y que producen perjuicios grandes tanto corporativamente como a nivel personal.

Conclusiones

En conclusión, es necesario tomar decisiones ante los incidentes en los cuales están involucrados los dispositivos de almacenamiento, siendo necesario emprender una metodología en el cual intervengan los peritos informáticos, así como la organización en cuanto al desarrollo de resolución del conflicto.

La informática forense es uno de los temas que contiene metodologías ante la recuperación de la información ya que interviene de una manera centrada puesto que no siempre la información es de una recuperación fácil para la persona, ya que las evidencias pueden estar oculta he de ahí la utilización de herramientas que cumplan con los requerimientos que se solicita para que el investigador forense logre llegar al final, con la resolución del conflicto.

Al término de esta investigación cabe recalcar y tomar en cuenta la relevancia de las fases que tiene la nueva guía, la cual consta de un proceso transparente y valido que puede ser tomado como referencia en cualquier caso similar, debo manifestar que al término de esta tesis se alcanzaron los objetivos planteados.

Recomendaciones

Mi recomendación sería que todo lo que haga referencia a perder información sensible que puede dañar su imagen que la cuiden puesto que constantemente hay nuevos métodos en la cuales personas de bien perdemos información y somos víctimas de cualquier extorsión.

Se debe tomar en cuenta que la información debe ser exclusivamente confidencial por que hay personas que divulgan ciertos aspectos que son indicios para que personas de mala manera busquen fórmulas para obtener dichas informaciones

Glosario

IBM: International Business Machines Corporation (IBM) (NYSE: IBM) es una reconocida empresa multinacional estadounidense de tecnología y consultoría con sede en Armonk, Nueva York. IBM fabrica y comercializa hardware y software para computadoras, y ofrece servicios de infraestructura, alojamiento de Internet, y consultoría en una amplia gama de áreas relacionadas con la informática, desde computadoras centrales hasta nanotecnología.

UNICODE: es el estándar de codificación de caracteres universal utilizado para la representación de texto para procesamiento del equipo. Unicode proporciona una manera consistente de codificación de texto multilingüe y facilita el intercambio de archivos de texto internacionales.

DOS: Disk Operating System, lo que en español significa **Sistema Operativo de Disco**, que era utilizado con procesadores de 16 Bits pertenecientes a ordenadores de la compañía IBM, siendo uno de los primeros sistemas operativos con mayor popularidad.

HASH: es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

NAND: tipos de memoria que se emplean en nuestros ordenadores personales y dispositivos móviles. Sin embargo, ambos tipos de memoria, por mucho que ambos sirvan para almacenar datos son fundamentalmente diferentes en su diseño, funcionalidad y, también, en su precio.

FAT: Conocido mayormente por su nombre en inglés de File Allocation Table (FAT), que en español su equivalente sería Tabla de Asignación de Archivos, ese sistema fue desarrollado originalmente para el actualmente dejado de lado sistema operativo Microsoft MS-DOS, aunque también fue empleado en sus ediciones gráficas.

MASTER BOOT RECORD: Un registro de arranque principal, conocido también como registro de arranque maestro (por su nombre en inglés master boot record, MBR) es el primer sector de un dispositivo de almacenamiento de datos, como un disco duro.

INVESTIGACIONES FORENSES: son un conjunto de disciplinas científicas que ayudan a la policía y la justicia a determinar las circunstancias exactas de la comisión de una infracción y a identificar a sus autores. La criminalística se sirve de los conocimientos científicos para reconstruir los hechos.

Bibliografía

- carrier, b. (2003 -2020). *sleuth kit*. Obtenido de <http://www.sleuthkit.org/sleuthkit/index.php>
- CARRIER, B. (2003-2020). *The Sleuth Kit®*. Obtenido de <http://www.sleuthkit.org/autopsy/>
- contributors, E. (20 de JUNIO de 2019). *ECURED*. Obtenido de <https://www.ecured.cu/index.php?title=Autopsy&oldid=3416144>
- EDITORIAL, E. (25 de NOVIEMBRE de 2019). *REPORTE DIGITAL*.
- Hornero, a. (30 de diciembre de 2019). *Ahornero*. Obtenido de <https://ahornero.wordpress.com/2009/06/26/analisis-forense-digital-the-sleuth-kit-2/>
- MX., E. D. (24 de junio de 2014). *Definición MX*. Obtenido de <https://definicion.mx/dispositivos-de-almacenamiento/>
- Pinto, D. (21 de septiembre de 2014). *dspace.ucuenca.edu.ec*. Obtenido de https://dspace.ucuenca.edu.ec/bitstream/123456789/21381/1/TIC.EC_04_Pinto.pdf
- Reyes, E. y. (31 de enero de 2013). *universidad Veracruzana*. Obtenido de <https://www.uv.mx/celulaode/seguridad-info/tema1.html>
- Sánchez, A. (3 de OCTUBRE de 2018). *PROTEGPC*. Obtenido de <https://protegermipc.net/2018/08/23/osforensics-herramienta-informatica-forense-windows/>
- TACUARI. (2017). *INFORMATICA FORENSE*. Obtenido de <http://www.informaticaforense.com.ar/>