HERRAMIENTAS APLICADAS EN EL DESARROLLO DEL ANÁLISIS FORENSE INFORMATICO EN COLOMBIA

Pedreros Martínez Wilson Leonardo Cód. 0800683
Suárez Urrutia Jennifer Catherine Cód. 0800691

Universidad Militar Nueva Granada
Facultad de Relaciones Internacionales, Estrategia y Seguridad
Administración de la Seguridad y Salud Ocupacional
Bogotá D.C., 03 de septiembre de 2016

HERRAMIENTAS APLICADAS EN EL DESARROLLO DEL ANÁLISIS FORENSE INFORMATICO EN COLOMBIA

TRABAJO DE GRADO

Pedreros Martínez Wilson Leonardo Cód. 0800683
Suárez Urrutia Jennifer Catherine Cód. 0800691

Tutor
Sandra Liliana Uribe Montaña
Ingeniera Electrónica

Universidad Militar Nueva Granada
Facultad de Relaciones Internacionales, Estrategia y Seguridad
Administración de la Seguridad y Salud Ocupacional
Bogotá D.C., 03 de septiembre de 2016

TABLA DE CONTENIDO

TABLA DE FIGURAS

RESUMEN DEL PROYECTO

En el desarrollo de este proyecto se dará a conocer en que consiste el Análisis Forense Informático y que papel cumple dentro del tema de seguridad detallando cada una de las acciones, procedimientos y conceptos que conforman este campo de la seguridad informática. Así mismo se explicara cómo esta nueva técnica es parte fundamental en el tratamiento de un incidente informático presentado en una organización contando con el apoyo legal y administrativo de las acciones que resulten de las investigaciones que se realicen dentro y fuera de ella.

Otro punto a tratar serán las herramientas tecnológicas utilizadas en el desarrollo del análisis forense informático en el ámbito público y privado, ayudando de esta manera al investigador a encontrar las pruebas y así mismo proporcionar los medios y protocolos, para una recolección de información más exacta y precisa de la información con el fin de servir como evidencia clara en el debido proceso legal sin que se presenten errores.

Por último se explicaran las fases por las cuales debe llevarse a cabo el análisis forense y como cada una de ellas se interrelaciona con las herramientas utilizadas para lograr el alcance de la investigación, resaltando la importancia de cumplir con los protocolos establecidos para la utilización y aplicación de estas en caso de presentarse un incidente informático.

DISEÑO METODOLOGICO

El enfoque de investigación del trabajo titulado “Herramientas aplicadas en el desarrollo del análisis forense informático en Colombia” será cualitativo porque se realizara un proceso en el cual se explorara y describirá el fenómeno en estudio para obtener otro punto de vista teórico de la investigación que se expone en este documento.

En cuanto al tipo de investigación que se utilizara para el desarrollo de este trabajo será descriptiva y explicativa. En cuanto a la investigación descriptiva se entiende que busca, especifica propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Así mismo describe tendencias de un grupo o población especifica. (Sampieri, 2006. P. 108) y a su vez incluye aspectos o componentes tales como cuerpos legales y normativas vigentes del tema a investigar.

También se hace referencia al tipo de investigación explicativa la cual consiste “en establecer las causas de los eventos, sucesos o fenómenos que se estudian” Es explicativa porque se dará a conocer las definiciones y conceptos legales y técnicos referentes al Análisis Forense Informático, de igual manera se dará a una visión general sobre el tema respecto a la situación actual en la aplicación de esta nueva disciplina en la seguridad informática.

Esta metodología fue escogida por que la explicación de este tema no ha sido muy reconocido y por ser reciente su aplicabilidad en el campo de la seguridad informática, no se evidencian suficientes recursos para realizar una investigación un poco más profunda sobre el tema. De esta manera y apoyados en bibliografía, datos históricos y revistas científicas se explicara la funcionalidad de cada una de las herramientas y las ventajas que tiene la utilización de estas en la realización del análisis forense digital.

I. PLANTEAMIENTO DEL PROBLEMA

Hablar de informática forense es enfrentarse a un reto interdisciplinario que requiere de un conocimiento y un estudio meticuloso que involucra la tecnología, los procesos y personal altamente capacitado y calificado que permitan la conformación de un equipo científico y legal que pueda apoyar directamente la administración de la justicia y la demostración de los hechos que se presenten con un incidente o fraude dentro de una organización.

Es allí donde aparece uno de los principales actores que se relacionan con la informática forense, estos son denominados los intrusos en la seguridad informática. Estas personas son el referente de estudio de los analistas de seguridad para examinar sus estrategias y crear un panorama más amplio de las acciones que se llevan a cabo en cada ataque informático.

Figura 1: Índices digitales en el entorno digital en Colombia

De esta manera se pueden revisar las técnicas y habilidades que utilizan los intrusos permitiendo de esta manera identificar y reconocer las fallas dentro de la infraestructura informática de la organización detectando las posibles vulnerabilidades del sistema y a su vez evitando de esta manera un posible incidente de seguridad. Así mismo permite que los usuarios y

directivos de la organización se concienticen sobre la importancia de informarse, capacitarse y entrenarse para desarrollar un ejercicio adecuado en temas de seguridad informática.

No se puede afirmar que estos ataques se pueden eliminar, debido que los delincuentes cada día se ingenian una manera diferente para atacar el sistema y poder perpetuar sus actos delictivos, así mismo un investigador forense deberá tener la misma capacidad de análisis y el mismo instinto intrusivo para poder detectar las formas de ataque, ayudando de esta manera a mantener las medidas de seguridad acordes con la operación del negocio, brindando protección a los activos de la organización y prepararse para enfrentar y seguir a los intrusos.

Es aquí donde se advierte la exigente labor de cada uno de los especialistas que se encargan de realizar los estudios que implican a la informática forense, tanto en los procedimientos como en las técnicas y cada una de las herramientas tecnológicas utilizadas en el desarrollo de la investigación en la escena del delito, para presentarla como evidencia ante la autoridad competente. Es por esto que se debe conocer al detalle la normatividad y las regulaciones legales relacionadas con las pruebas y el derecho procesal así como la aplicación de técnicas y procedimientos que permitan mantener la confiabilidad de los datos recogidos como evidencia, la integridad de los medios, el análisis detallado de la información y la presentación competente de los resultados arrojados.

Uno de los problemas en la informática forense es la mala manipulación de la evidencia recolectada en las herramientas utilizadas para tal fin, debido que muchas veces estas herramientas no son esterilizadas de acuerdo con los protocolos establecidos los cuales explicaremos más afondo en el desarrollo de este trabajo. Otra de las problemáticas asociadas con el estudio de la informática forense es la verificación de las copias en los medios informáticos para que la evidencia sea copiada igual que la original sin que sufra ningún tipo de alteración y en muchos casos esta copia es manipulada para conveniencia de la persona que comete el delito.

La documentación de los procedimientos utilizados sobre los medios informáticos analizados y el mantenimiento de la cadena de custodia en las evidencias digitales son uno de los pilares fundamentales para dar con el intruso que comete el ataque, no obstante, la investigación actual

que se realiza en este campo es mínima. Es por esto que en este estudio, actual y potencial es la administración legal quien analiza dicho impacto en el campo forense, de acuerdo con el campo que comprende aspectos legales y los ordenadores causantes del conflicto, debido que la Ley aún se encuentra poco especializada y adaptada a la evolución constante del entorno informático.

De esta manera la informática forense es el punto de partida para responder por el aumento de incidentes, fraudes, ataques y ultrajes en medios informáticos y a través de medios informáticos, con el fin de dar detectar las acciones de los intrusos y estar preparados para atender cada incidente que se presente en materia de seguridad.

Es por ello que surge la siguiente pregunta para detectar las falencias de esta problemática ¿Las herramientas utilizadas para determinar las posibles causas de los incidentes informáticos, cumplen con los protocolos establecidos?

II. JUSTIFICACIÓN

Este proyecto se realizará con el fin de identificar las diferentes metodologías de análisis forense en el área, basado en dos principios básicos de la seguridad informática, como la integridad y la autenticidad de la información. La importancia de este trabajo de investigación es poder brindar una información clara y precisa de las diferentes aplicaciones utilizadas en Colombia para la identificación de los posibles intrusos que accedan fraudulentamente a los dispositivos donde de posea información sensible y reservada dentro de una organización.

Las telecomunicaciones y la transmisión de datos de un lado a otro era una actividad que podría tardar días, hoy gracias a la evolución de la tecnología solo se tarda segundos, es por esto que se ha dado paso a un nuevo campo o rama de investigación criminal, la cual consiste en recuperar la información de una manera confiable que sirva como prueba veraz en un caso legal.

El tema de la seguridad informática, no solo debe ser de vital importancia para los investigadores que llevan el caso de intrusión en la información, este tema debe ser de gran importancia para las personas encargadas de seguridad de la empresa, ya que ellos deben enterarse de que fue lo que paso y como se llevó a cabo el incidente presentado.

El análisis forense de la información cada día crece más, debido a la evolución de los dispositivos electrónicos como celulares, tabletas, memorias, portátiles, equipos de sonido, cámaras, que no solo sirven para guardar fotografías, sino que también estas pueden almacenar datos de información importante.

Este crecimiento en dispositivos tecnológicos crea una problemática en la cual el investigador debe desarrollar mecanismos de encriptación cada vez más complejos, los cuales son utilizados por los atacantes de los sistemas informáticos como se ha presentado en países como Estados Unidos. Pero este no es el único problema al que se enfrenta un investigador forense, existe también el vacío legal en donde muchas veces no es posible llevar una investigación criminal de tipo informático debido a la alta complejidad de los mecanismos empleados para cometer este delito

Cabe mencionar que actualmente en el análisis forense se lleva a cabo la ingeniería inversa, que se encarga de desempaquetar archivos que pueden ejecutarse fácilmente dentro de los equipos vulnerados, los cuales pueden ser rootkits o virus polimórficos, al igual que túneles de datos ya sean VPN´s o túneles Ipv6, los cuales son más complejos debido que no existen detectores y analizadores capaces de descifrar este tipo de ataque.

Es por esto que se dará a conocer cómo se lleva a cabo el análisis forense informático, sus fases y como las herramientas descritas en este trabajo se apoyan en la realización de este estudio, el cual nos ayudara a encontrar al autor material de los incidentes de seguridad que se presentan en una organización.

III. INTRODUCCIÓN

En el ámbito de la seguridad informática, el Análisis Forense Informático permite obtener evidencias encontradas en los dispositivos o elementos para determinar las causas de un delito, mediante las cuales se reconstruye el antecedente que desencadeno la vulnerabilidad en dicho sistema. Es fundamental recopilar toda evidencia digital y enlazarla a la cadena de custodia, debido que en los laboratorios forenses se requiere de la utilización de herramientas confiables y eficaces que sirvan de acompañamiento, en la presentación de estas evidencias que sirven como elemento probatorio en los procesos jurídicos quienes son los encargados de atender este tipo de delitos informáticos.

Teniendo en cuenta el constante crecimiento de los reportes por ataques en sistemas de información, aprovechamiento de fallas humanas, procedimentales o tecnológicas sobre infraestructuras informáticas en todo el mundo, los intrusos tienen una gran variedad de posibilidades para cometer sus actos y atacar los sistemas de seguridad para poder conseguir lo que se proponen. Cada uno de ellos posee una serie de motivaciones, alcances y métodos que confunden a los investigadores, consultores y analistas, debido que cada ataque y penetración del sistema es diferente en cada caso.

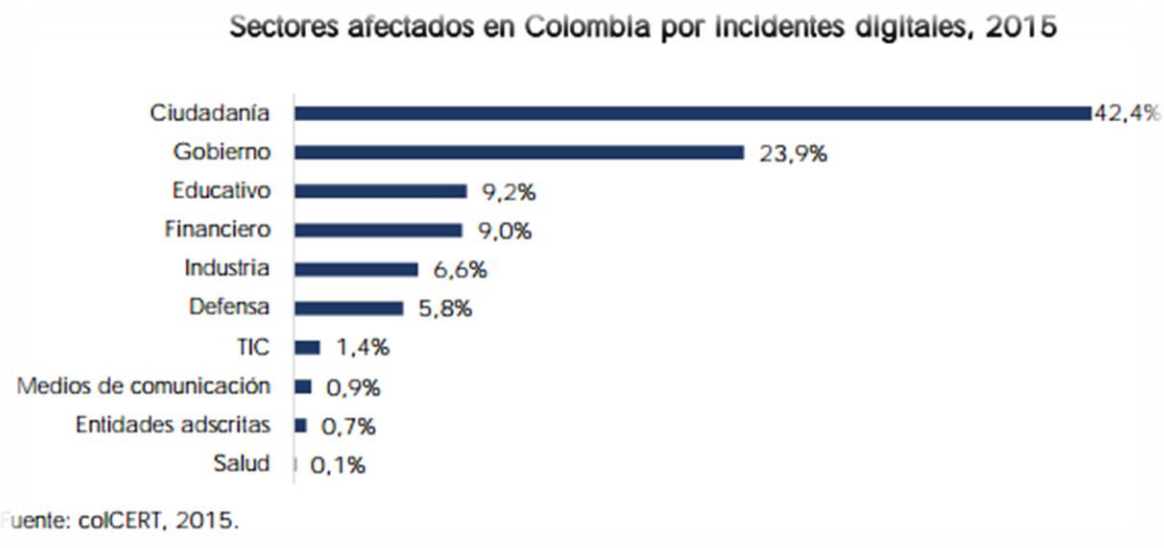

Figura 2: Sectores afectados en Colombia por incidentes digitales. *CONPES 3854(2016) Política Nacional de Seguridad Digital*

Es allí, donde el campo de la criminalística ocupa un lugar muy importante porque ofrece un espacio de análisis y estudio de los hechos y evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. Es en este momento donde se deben establecer una serie de herramientas, acompañadas de acciones y estrategias que permitan investigar a profundidad los medios informáticos y de esta manera obtener la evidencia digital que sustente y verifique las afirmaciones sobre los hechos delictivos sobre los cuales se ha materializado el caso de estudio (Cano, 2015. P.19)

De acuerdo con un informe emitido por la INTERPOL uno de los organismos judiciales encargados de analizar los delitos que se cometen en el área informática es la Organización Internacional de Policía Criminal, la cual afirma que uno de los ámbitos delictivos con más alto nivel de crecimiento en los últimos tiempos es la Ciberdelincuencia. Este delito es común debido que la tecnología moderna ofrece rapidez, comodidad y anonimato lo cual permite que se lleven a cabo diversos tipos de actividades delictivas.

Según Galván (2013), los ataques contra sistemas y datos informáticos incluyen usurpación de la identidad, distribución de imágenes con contenido pornográfico infantil, estafas, subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, redes de ordenadores infectados controlados por usuarios remotos y distintos daños por correo electrónico, como el phishing (adquisición fraudulenta de información personal confidencial) para acceder a la información de los servidores sin control.

La informática forense es una disciplina auxiliar en aspectos legales, para enfrentar cada uno de los desafíos y técnicas de aquellas personas que se dedican a perpetuar ataques informáticos, al igual ayuda a ser garante de la verdad al presentar una evidencia digital para aportar a un proceso legal. Este trabajo va enfocado en explicar la funcionalidad de la Informática Forense y su aplicación en el campo de la seguridad informática, dando pautas para la comprensión de algunos de los términos más usados en este medio y su aplicación utilizando diferentes herramientas software las cuales ayudan a la identificación de ataques en los medios tecnológicos estáticos y móviles.

IV. OBJETIVOS

OBJETIVO GENERAL

Identificar las herramientas que sirven como apoyo en la aplicación del análisis forense informático.

OBJETIVOS ESPECIFICOS

- Explicar la funcionalidad de la informática forense
- Presentar las fases que se llevan a cabo en la aplicación del análisis forense informático
- Conocer las herramientas utilizadas en la informática forense
- Verificar que las herramientas utilizadas en la informática forense cumplan con lo establecido en cada una de las fases

V. MARCO REFERENCIAL

1. Antecedentes Históricos.

La informática forense dio su inicio en el año 1978 en Florida Estados Unidos, es allí donde se reconocen por primera vez los delitos en sistemas informáticos (sabotaje, copyright, modificación de datos). En los años 80´s donde poco después las computadoras portátiles fueron puestas en el mercado para posicionarse como un producto indispensable para os consumidores. En el año 1984 el FBI creo un programa conocido como el Programa de Medios Magnéticos, que hoy en día se conoce como CART (Computer Analysis and Response Team), o análisis de informática y equipo de respuesta.

Al poco tiempo Michael Anderson, quien era un agente especial de la División de Investigación Criminal del IRS, se interesó por la informática forense y empezó a trabajar en este campo a mediados de 1990, fue aquí donde . A partir de este momento el campo de la informática forense ha tenido una gran expansión, incluso la policía y las fuerzas militares empiezan a hacer presencia en las áreas de seguridad de la información y la informática forense.

En el año 1997, se estableció que los especialistas encargados de recoger la evidencia de los equipos de cómputo, debían ser bien tratados de acuerdo con un manifiesto emitido por el G8 en este mismo año. De este modo la INTERPOL celebró un simposio sobre informática forense al año siguiente, y en el año1999, el programa CART del FBI abordó 2000 casos individuales.

Con este programa de la FBI los casos fueron en aumento en este año, sin embargo este programa analizo 17 Tb de datos y para el año 2003 se llegó a examinar casi 782 Tb en un solo año. Debido a los constantes avances de la informática y el crecimiento de acceso a internet en todo el mundo, la informática forense empezó a tomar mayor importancia y más aun con la llegada de los teléfonos inteligentes, medios por los cuales los delincuentes empezaron a tener opciones para romper la ley mediante el uso de dispositivos de computación.

En Colombia, la informática forense surgió a partir del año 2004 con la creación de la Dirección de Investigación Criminal, la cual apoya labores investigativas realizadas por la Policía

Nacional. Es por esto que los casos reportados relacionados con ataques informáticos en el sector privado y el sector bancario en el país se han vuelto importantes por ello su prevención y procesamiento ha aumentado la acción de las autoridades.

En este año no solo se estableció una entidad dedicada a la informática forense, también se involucra la Contraloría General de la República delegada para investigaciones, juicios fiscales y jurisdicción y se creó un laboratorio de informática forense, con el fin de determinar actos ilícitos o fraudes donde el patrimonio del Estado esté en riesgo (Restrepo, A. 2008).

Otro hecho importante que se registra en Colombia data en el año 2006, donde la DIJIN realizo 433 investigaciones relacionadas con ciberdelincuencia y en septiembre del año siguiente se conocieron 85 amenazas virtuales, 25 casos de pornografía, 381 de fraude electrónico, ocho de extorsión y 16 de *pishing*. Según Restrepo (2008) *"*mensualmente se detectan y bloquean 150 páginas con contenido de pornografía infantil y se investigan 50 casos por estafas electrónicas, los cuales aumentaron a 5.000 millones de pesos en el último año y en lo que va corrido del 2007 ya se superan los 6.000 millones."

No solo estos casos son identificados por parte de las autoridades, debido a la expansión del internet y el alto índice de acceso a la red se han identificado otros delitos informáticos dentro de los cuales se encuentran las descargas ilícitas de programas de música, suplantación de identidad, fotomontajes, transferencias ilícitas de dinero por robo de contraseñas, y usos indebidos de información para beneficio propio o empresarial. "Colombia tiene la tecnología disponible en el mercado y eso nos pone a la vanguardia en la lucha contra la criminalidad electrónica en Latinoamérica. Hemos implementado servicios de interacción virtual entre la comunidad y la Policía", explicó el mayor Fredy Bautista.

"Las organizaciones han adelantado análisis de su seguridad, instalado múltiples mecanismos de protección y efectuado múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste

se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente" explica al respecto Cano, J. (2015).

De acuerdo con lo explicado anteriormente, Colombia cuenta con herramientas tecnológicas y personal altamente capacitado y calificado para enfrentar los ataques informáticos que se presenten y capturar a los delincuentes, sin embargo se debe trabajar un poco más en el tema legislativo que le competa a este tema, debido que el poco compromiso y confianza de las empresas dificulta el proceso, ya que muchos de los casos reportados por las diferentes organizaciones no son analizados por la falta de información.

VI. MARCO LEGAL

Para la realización de este trabajo es importante tener en cuenta la normatividad existente en Colombia basada en tres aspectos: la legislación informática, legislación penal y la legislación civil. Dentro de la legislación civil encontramos que esta permite responder a personas y a sus bienes si es de carácter patrimonial o moral en caso de violar alguno de los artículos por los cuales se rige. En cuanto a la legislación penal, esta intercede por los daños a los bienes jurídicos protegidos por el estado.

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

- Decreto 1360 de 1989: Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- La Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto reglamentario 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- Ley 527 de 1999 en su artículo 10 la cual regula "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil. Lo anterior satisface el requisito de que la información conste por escrito, equiparándolo así al documento escrito tradicional. De acuerdo con lo estipulado en este artículo, la Corte Constitucional en sentencia C-662 de junio 8 de 2000, con ponencia del Magistrado Fabio Morón Díaz, al pronunciarse sobre la constitucionalidad de la Ley 527 de 1999, hizo las siguientes consideraciones: (...) "El

mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento (Álvarez, Marín y Victoria, 2012).

- Sentencia C-662 de 2000, la cual expone que los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y en la mayoría de los casos, un mayor grado de confiabilidad y rapidez.
- Ley 842 de 2003 por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesionales auxiliares, se adopta el Código de Ética profesional y se dictan otras disposiciones en sus artículos 29 al 38.
- Ley 1266 de 2008: Por la cual se generan las disposiciones de protección de datos y asegura el manejo de la información contenida en las bases de datos
- La ley 1273 de 2009 "De la Protección de la información y de los datos"
  Capítulo I: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos en los artículos 269A, 269B, 269C, 269F, 269H.
  Capítulo II De los atentados informáticos y otras infracciones, en los artículos 269I, 269J, artículo 58.
- Ley 1453 de 2011: Por la cual se dictaminan algunas disposiciones en materia de seguridad, especialmente en el artículo 236 donde se señala lo referente a recuperación de información producto de trasmisión de datos por medio de redes electrónicas.
- Ley 1564 de 2012: Esta ley expone el código general del proceso, de esta ley puntualmente se tienen en cuenta 2 artículos en los cuales básicamente se trata el tema de aceptación de material probatorio.
- Ley 1581 de 2012: esta medida se dicta para la protección general de datos personales.
- Decreto 1377 de 2013 en uso de sus atribuciones constitucionales, y en particular las previstas en el numeral 11 del artículo 189 de la Constitución Política y en la Ley 1581 de 2012.

VII. TERMINOLOGIA

Delito informático: Es toda acción antijurídica y culpable que tiene como objetivo destruir o dañar ordenadores, medios electrónicos y redes de internet, debido a los constantes abusos informáticos llevados a cabo mediante un elemento informático.

Incidente de seguridad: Cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, extorsión, posesión de pornografía infantil, envío de correos electrónicos ofensivos, fuga de información confidencial dentro de la organización, etc., en el cual está involucrado algún sistema telemático de nuestra organización.

Cadena de Custodia: La identidad de personas que manejan la evidencia en el tiempo del suceso y la última revisión del caso. Es responsabilidad de la persona que maneja la evidencia asegurar que los artículos son registrados y contabilizados durante el tiempo en el cual están en su poder, y que son protegidos, llevando un registro de los nombres de las personas que manejaron la evidencia o artículos con el lapso de tiempo y fechas de entrega y recepción.

Imagen Forense: Llamada también "Espejo" en inglés "Mirror", la cual es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos, áreas borradas incluyendo particiones escondidas.

Análisis de Archivo: Examina cada archivo digital descubierto y crea una base de datos de información relacionada al archivo (metadatos, etc.), consistente entre otras cosas en la firma del archivo o hash (indica la integridad del archivo), autor, tamaño, nombre y ruta, así como su creación, ultimo acceso y fecha de modificación.

Ataque DOS: En seguridad informática, un ataque de denegación de servicios, también llamado ataque DoS (siglas en inglés de Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Sistema Operativo: Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas. "el sistema operativo de la computadora es MS-DOS"

Toolkit: El Toolkit para la creación de productos y servicios de información sobre riesgo y desastres es una "caja de herramientas" que le orientará, paso a paso, en la creación de servicios y productos de información en un entorno virtual, y le proporciona las herramientas para poder desarrollarlos. Para ello cuenta con cinco módulos y una Plataforma de Gestión de Productos y Servicios de Información.

Hash: Se llaman funciones hash criptográficas a aquellas funciones que se utilizan en el área de la criptografía. Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que confían en la criptografía para dotarse de seguridad.

Puertos TPC: Números de **puerto** bien conocidos usados por **TCP** y UDP. Enrutamiento y Acceso Remoto para VPN con L2TP. Enrutamiento y Acceso Remoto para VPN con PPTP. iRDMI por lo general, usado erróneamente en sustitución de 8080.

User Datagram Protocol (UDP): es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

Dirección IP: Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora,

tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Ficheros: Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

1. ¿QUÉ ES LA INFORMATICA FORENSE?

Sobre este tema nos encontramos con varias definiciones, una de ellas según Cano (2015, p.2) nos indica que esta disciplina se conoce con términos diferentes entre los cuales se mencionan los siguientes: computación forense, forensia digital, forensia en redes, informática forense, entre otros. Cada uno de estos términos puede ser confundido dependiendo en el ámbito que se utilicen, debido que cada uno de ellos trata puntualmente temas de interés en las ciencias forenses aplicadas a los medios informáticos.

Dentro de este contexto es conveniente aclarar cada uno de los términos mencionados anteriormente para aclarar la especificidad de cada uno de ellos. La computación forense se refiere a la disciplina de las ciencias forenses, que ayudan a esclarecer e interpretar la información extraída de los medios informáticos como prueba principal para la justicia y para la informática.

La forensia digital por su parte, aplica los conceptos, estrategias y procedimientos de la criminalística común a los medios informáticos especializados con el fin de servir a la justicia para esclarecer los hechos de los eventos catalogados como fraudes, incidentes o usos indebidos en la actuación de la administración legal.

Por último, la forensia en redes se encarga de capturar, registrar, almacenar y analizar los eventos de la red, con el fin de determinar la fuente de uno o varios ataques o las posibles vulnerabilidades existentes en ella.

Como se pudo observar cada una de estas definiciones apuntan a un mismo fin, identificar, preservar, extraer, analizar, interpretar, documentar y presentar la evidencia digital para validar un evento que se haya presentado y sobre esto arrojar hipótesis que ayuden a identificar las causas del ataque. Así mismo, se debe tener en cuenta que las personas dedicadas a la aplicación de esta técnica, deben contar con altos niveles de ética y respeto pues en ellos está el soporte para la toma de decisiones sobre los hechos que ya han sido analizados.

Para aclarar un poco la funcionalidad de la informática forense, es necesario definir el término evidencia digital que se refiere a “cualquier información sujeta a manipulación humana u otra semejante, extraída de un medio informático” (Cano, 2015. P, 3). En este orden de ideas podemos definir que la evidencia digital es cualquier dato que sirva como prueba para ser presentado para llevar a cabo un proceso legal.

La evidencia digital puede ser dividida en tres partes:

1. Registros informáticos almacenados en el equipo, bien sea por medio de correos electrónicos, archivos digitales, imágenes, etc.
2. Registros generados por los equipos tecnológicos como auditorias, registros de transacciones, registros de eventos, etc.
3. Registros generados y almacenados en equipos tecnológicos como consultas a bases de datos, hojas de cálculo con información financiera, etc.

Es así como la evidencia digital se considera la materia prima de un investigador dedicado al análisis forense informático, debido que la tecnología es una parte fundamental de este proceso. De acuerdo con Cano (2015), la evidencia digital posee unas características que hacen de ella un desafío porque:

- Es volátil
- Es anónima
- Es duplicable
- Es modificable
- Es eliminable

Es por esto que se resalta la importancia de tener un conocimiento detallado de la normatividad asociada con las pruebas y el derecho procesal así como de los procedimientos, técnicas utilizadas en el tratamiento de la información extraída.

1.1 Procedimientos

Teniendo en cuenta que la informática forense es una disciplina compleja en su manejo, se deben extremar las medidas de seguridad al personal especializado en el manejo de estas evidencias con el fin de evitar que se cometa cualquier error que implique fallas en un proceso legal.

Algunos de los elementos que deben considerarse al momento de adelantar un procedimiento de informática forense son los siguientes:

1. **Esterilidad de los medios informáticos de trabajo**. Cada elemento utilizado por los investigadores debe estar certificado para garantizar que no se haya vulnerado su integridad, debido que si este elemento fue expuesto a vibraciones magnéticas u otro tipo de exposición, la evidencia recolectada en este medio quedaría contaminada y no sería confiable en ningún procedimiento forense. Este se relaciona con la medicina forense en donde una mala interpretación o análisis de las pruebas recogidas puede determinar una falsa hipótesis sobre la muerte de un paciente.
2. **Verificación de las copias en medios informáticos**. Al momento de extraer las copias de información de los medios tecnológicos, estas deben ser exactas a la original y deben estar asistidas por un método y un procedimiento utilizando algoritmos y técnicas basadas en firmas digitales que comprueben su veracidad. De esta misma manera, el software utilizado debe estar probado por la comunidad científica para que la tasa de efectividad de la misma sea validado antes de presentarse ante una instancia legal.
3. **Documentación de los procedimientos, herramientas y resultados de los medios informáticos utilizados**. La custodia de todas las evidencias y los procedimientos ejecutados durante el análisis de las evidencias recolectadas, están a cargo del investigador y deben estar debidamente documentados, con el fin de que una persona externa pueda validar la información obtenida de dicho análisis. De esta manera se puede tener un parte de confianza y tranquilidad al investigador evitando que un tercero utilice la misma evidencia.

4. **Mantenimiento de la cadena de custodia de las evidencias digitales.** Este punto es complemento del anterior teniendo en cuenta quien entrego la información, cuando, en qué estado, como, entre otras preguntas para poder rendir cuentas de la correcta administración de las pruebas a cargo del investigador.
5. **Informe y presentación de resultados de los análisis de los medios informáticos.** Una adecuada presentación de los resultados es fundamental para la interpretación de las pruebas extraídas, si este requisito no se cumple, el investigador puede poner en entredicho su idoneidad y experticia en el manejo de la información. Es por esto que la claridad en la redacción y la ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones, entre los cuales encontramos los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.
6. **Administración del caso realizado.** Una vez sean recopiladas, analizadas y documentadas las pruebas, los investigadores forenses en informática deben prepararse para declarar ante un jurado o juicio, con el fin de servir en los procesos judiciales como declarante en ese mismo momento o en un tiempo determinado. Es por ello la importancia de mantener documentado y bajo extrema seguridad y control todos los expedientes que contienen información puntual sobre el caso en el cual el profesional ha participado.
7. **Auditoría de los procedimientos realizados en la investigación.** Por último es recomendable que el investigador autoevalúe los procedimientos realizados para contar con la evidencia de una buena práctica en su investigación, aplicando el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, y de esta manera incrementar la confiabilidad de las técnicas aplicadas en la práctica de esta disciplina.

En resumen, el análisis forense informático sirve para garantizar la efectividad de las políticas de seguridad implementadas en una organización y a su vez para proteger la información y las tecnologías que facilitan la gestión de esta información. A su vez esta técnica consiste en investigar los sistemas de información con el fin de detectar evidencias en la vulneración de los mismos.

La finalidad del análisis permite que cuando una organización contrata servicios de informática forense puede perseguir objetivos preventivos logrando de esta manera anticiparse a los problemas, generando así una solución favorable para este incidente. Las metodologías utilizadas incluyen la recolección de datos de los diferentes medios digitales sin alterar los datos de origen. Estas evidencias rescatadas permiten la elaboración de un dictamen claro y conciso fundamentado y justificado a partir del análisis de las pruebas recogidas.

Todo el procedimiento realizado en el análisis informático debe realizarse de acuerdo con los requerimientos contenidos en la normatividad vigente para no vulnerar los derechos de terceros que puedan verse afectados, para que, llegado el caso, las evidencias sean aceptadas por los tribunales evitando rechazos en los procesos y puedan constituir un elemento de prueba fundamental en un litigio, llegando a alcanzar un resultado favorable.

Cuando se habla de la utilización de la informática forense con una finalidad preventiva, en primer término, la cual sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes.

De esta manera, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas, por medio de la redacción y elaboración oportuna de las políticas sobre uso de los sistemas de información facilitados a los empleados para no atentar contra el derecho a la intimidad de esas personas. De acuerdo con esto, cuando la seguridad de la empresa ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque y determinar si la vulneración es externa y así mismo detectar si las alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa has sido realizadas desde uno o varios equipos específicos.

2. FASES APLICADAS EN EL DESARROLLO DEL ANÁLISIS FORENSE INFORMÁTICO

Para poder entender un poco la metodología del Análisis Forense Informático, se explicaran las cinco fases por las que este análisis debe pasar, para poder mantener un estudio estructurado facilitando la confiabilidad de este análisis.

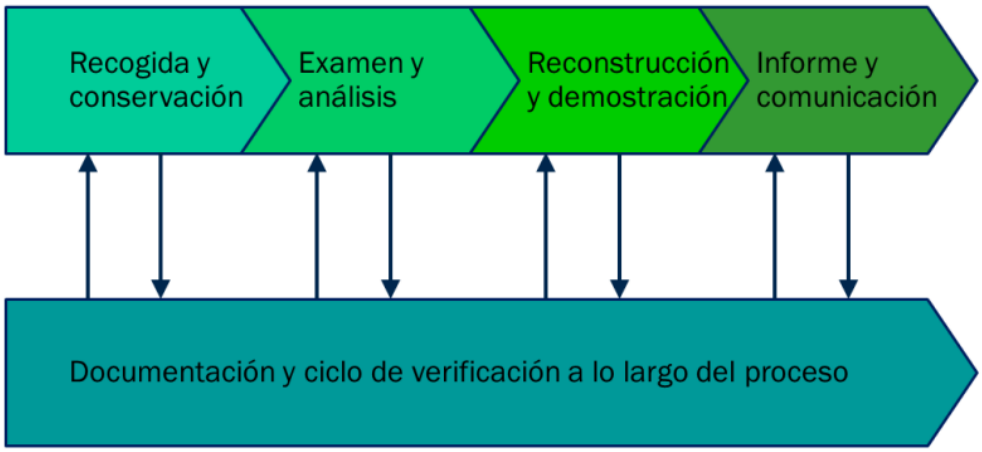

Figura 3:Fases de la informática forense. Tomado de: http://seginformaticacarolinavillamil.blogspot.com.co/p/unidad-1.html

A continuación, se presentaran las fases de un Análisis Forense Informático:

1.2 Identificación de un incidente

Esta primera fase se refiere a la búsqueda y recopilación de evidencias lo cual permite la identificación del incidente en materia de seguridad informática. Para poder llevar a cabo esta primera fase, si se tiene la más mínima sospecha de un ataque a nuestro dispositivo se debe asegurar que no se trate de un problema de software o hardware de la red o servidor para que este no se confunda con un ataque DOS (ataque distribuido denegación de servicio).

Un primer paso para poder descubrir las señales de un posible ataque informático, es mantener la evidencia intacta, es decir, sin ser manipulada y alterada e incluso borrada. Se debe tener certeza de que las aplicaciones instaladas o que estén incluidas dentro del Sistema Operativo se mantengan intactas y no esta demás que se tenga un CD o DVD con herramientas necesarias para

atender cualquier tipo de incidente relacionado con ataques informáticos, para que de este modo se pueda entrar a controlar esta situación de una manera más acertada.

López (2007), nos dice que, si se trabaja en entornos mixtos UNIX/Linux y Windows, se tendrá que preparar un juego de herramientas para cada plataforma. Aunque existen gran cantidad de utilidades a continuación propongo una relación de aquellas que considero debería incluir en su ToolKit (conjunto de herramientas), y que le permitan, al menos, realizar las siguientes tareas:

1. Interpretar comandos en modo consola (*cmd, bash*)
2. Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas (*fport, lsoft*)
3. Listar usuarios conectados local y remotamente al sistema
4. Obtener fecha y hora del sistema (*date, time*)
5. Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (*ps, pslist*)
6. Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (*ipconfig, arp, netstat, net*)
7. Buscar ficheros ocultos o borrados (*hfind, unrm, lazarus*)
8. Visualizar registros y logs del sistema (*reg, dumpel*)
9. Visualizar la configuración de seguridad del sistema (*auditpol*)
10. Generar funciones hash de ficheros (*sah1sum, md5sum*)
11. Leer, copiar y escribir a través de la red (*netcat, crypcat*)
12. Realizar copias bit-a-bit de discos duros y particiones (*dd, safeback*)
13. Analizar el tráfico de red (*tcpdump, windump*)

Después de estar preparados con las herramientas necesarias para actuar ante un eventual ataque, se debe entrar a determinar en donde se va a investigar. Tal como lo menciona López (2007) como primera opción de búsqueda podemos realizar una verificación de integridad de los ficheros del sistema, utilidades como Tripwire (es un programa de computador basado en una herramienta de seguridad e integridad de datos.

Es útil para monitorizar y alertar de cambios en los ficheros de un sistema de ficheros o AIDE (Advance Intrusion Detection Enviroment) o en español Entorno de Desarrollo Integrado de Android, podrán arrojar algo de luz sobre sus sospechas. Otra opción es realizar una serie de verificaciones sobre el equipo.

Para poder detectar alguna huella sobre intrusión o posible hurto de información, es necesario fijarnos en los procesos que lleve a cabo el equipo y en los cuales se consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos y que mantengan conexiones de red en puertos TCP o UDP no habituales, etc.

En este último paso, es importante conocer el funcionamiento normal del ordenador para detectar posibles irregularidades en la actividad normal del sistema, la aparición de listado de procesos sin nombre, pueden ser un factor de riesgo en la aparición de un virus troyano en el equipo, una buena alternativa podría ser documentarnos bien de las características de intrusión de este virus para así mismo identificar los procesos sospechosos.

2.2 Recopilación de evidencias

Después de ver la primera fase de identificación de un ataque informático debemos priorizar entre los siguientes aspectos:

- Tener nuevamente operando sus sistemas rápidamente.
- Realizar una investigación forense detallada.

Para nosotros la prioridad será restaurar nuevamente el sistema para que opere normalmente en el menor tiempo posible, pero esta acción solo hará que el sistema afectado pierda toda la evidencia que los atacantes en su momento pudieron haber dejado en “la escena del crimen”, se pierda y eso haga que se elimine la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo? se comprometió el sistema, e impidiendo incluso llevar a cabo acciones legales posteriores si se diese el caso. (López, p, 13).

Por otra parte, si elegimos el “Plan B”, en cual decidimos que lo primordial en este caso es realizar el análisis forense y cuenta con el conocimiento y las herramientas adecuadas para llevar a cabo esta acción, se tendrán que seguir una serie de pasos que permitan recopilar todas las evidencias que nos permitan descubrir cuál fue el método utilizado para levar a cabo este ataque.

Es importante llevar por escrito todos los pasos que el intruso realizó para entrar a atacar el sistema en donde se debe anotar la fecha y hora de inicio y fin de cada uno de los pasos, también se debe anotar las características como números de serie de cada equipo, de sus componentes, de su S.O., etc. Todo debe estar muy bien descrito y detallado, si se pueden tomar fotografías no está de más que se haga esta tarea por si en algún momento tiene que presentarlas como material probatorio ante un juicio, ya que cualquier evidencia puede ser definitiva.

El autor nos recomienda que durante este proceso seamos acompañados por un testigo de estas acciones y que esta persona sea imparcial en su criterio, esto a su vez será un poco difícil debido que se debe recopilar toda la información y a su vez gran parte de la información vital se perderá si se apaga el equipo de la forma habitual, ya que en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia, pero si además el atacante ha instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros a su antojo durante el apagado, y se “limpiarán” también del equipo las huellas de su atacante.

Es importante que nos mantengamos prevenidos porque es probable que el atacante aún se encuentre en línea, de esta manera podría ver todo lo que hacemos y podría actuar con una acción de huida o peor aún, destructiva eliminando todo tipo de información. Pero si por la severidad del ataque o por la importancia de los datos comprometidos decide apagar el equipo, lo más sensato en esos momentos es desconectar de inmediato el equipo de esta manera se perderá la información volátil de la RAM, micro, etc. Pero conservará aún bastante información sobre el ataque.

Si el equipo sigue encendido podemos empezar a recuperar la siguiente información siguiendo la siguiente secuencia:

- ✓ Registros y contenidos de la caché.
- ✓ Contenidos de la memoria.
- ✓ Estado de las conexiones de red, tablas de rutas.
- ✓ Estado de los procesos en ejecución.
- ✓ Contenido del sistema de archivos y de los discos duros.
- ✓ Contenido de otros dispositivos de almacenamiento.

Durante este proceso de recopilación de evidencias, tendremos que hacer uso de su ToolKit, tal como lo vimos en la primera fase, pero debemos tener mucha precaución porque, tal como le dijimos anteriormente, el atacante aún puede estar espiando el sistema. Por eso es importante estar capacitado en este tema ya que con este entrenamiento podremos ser capaces de recopilar toda la información de una manera muy sutil.

Se recomienda tener preparado un script en Perl para sistemas UNIX/Linux o un archivo de proceso por lotes para entornos Windows que realizase todas estas operaciones de forma automatizada y que, además, enviase la información a un lugar seguro. La mejor manera para poder guardar toda la información recopilada sería usar discos externos USB, muy económicos y que le permiten gran flexibilidad de manejo y transporte de grandes cantidades de información. Esto con el fin de que el atacante no tenga acceso directo a esta información y no pueda eliminar las evidencias recopiladas, en caso de que siga activo en el sistema atacado.

En este punto cabe hacer una aclaración muy importante, cuando se realiza una copia de seguridad de un disco o soporte en general se procede a copiar los archivos tal cual el sistema operativo los reconoce, perdiéndose gran cantidad de información oculta en el disco, así que lo más recomendable es realizar una imagen del disco original preservando toda la información que contenga, siendo esta información solo de lectura la cual no permite modificación alguna.

3.2 Preservación de la evidencia

En esta fase el primer motivo y objeto principal es la recopilación de evidencias sobre el incidente, dichas evidencias serán custodiadas en caso tal de que iniciemos un proceso judicial contra las personal que nos vulneren el sistema, en este caso se deberá documentar de tal

forma que la evidencia sea clara, para así proteger y custodiar las evidencias que son recopiladas. En este proceso, como se expondrá a continuación, es imprescindible definir métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Una vez, tengamos la evidencia del ataque, seguiremos siendo muy metódicos en conservar intactas las "huellas del crimen", debemos asegurar dichas evidencias a toda costa, por lo tanto, el autor nos recomienda no hacer el análisis sobre esa copia. (López, p, 15)

Como primer paso debemos realizar dos copias de las evidencias obtenidas, para generar una suma de comprobación de la integridad de cada copia mediante el empleo de funciones *hash* tales como MD5 o SHA1. Posteriormente debemos incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio CD o DVD, también que incluya en el etiquetado la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "COPIA A", "COPIA B" para distinguirlas claramente del original. Ya para asegurar estas evidencias debemos realizar el traslado de dichos datos a otra etiqueta, pegarlo en la caja contenedora del soporte, e incluso sería conveniente asegurar una copia original para evitar una mala manipulación. (López, p, 16)

Por otra parte, si queremos extraer los discos duros del sistema para utilizarlos como evidencia se deberá seguir el mismo procedimiento, colocando una anotación que diga evidencia original, incluya además las correspondientes sumas *hash*, fecha y hora de la extracción del equipo, dato de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo, se almaceno en una caja fuerte. También debemos tener en cuenta que existen factores externos que nos pueden alterar la evidencia como son cambios bruscos de temperatura o campos electromagnéticos. Toda precaución es importante dado que en caso que, se envié estos discos duros a ser analizados por empresas especializadas debemos solicitar que estas evidencias sean aseguradas en caso de que se genere algún daño en el equipo.

Un último aspecto en tener en cuenta, y que es relacionado con lo mencionado anteriormente es el proceso que se conoce como cadena de custodia, donde hay unos parámetros y establecen responsabilidades y controles de cada persona que manipulan dichas evidencias. Se deberá realizar un documento en donde se muestre los datos personales de todos los implicados en el

proceso de manipulación de copias, desde cuando se recibieron hasta su almacenamiento; Seria de gran Importancia dejar todo documentado:

- ✓ Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, un número identificación, fechas y horas, etc.
- ✓ Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.
- ✓ Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y cómo se produjo la transferencia y quién la transportó. Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo y quede claramente documentado, facilitando detectar y pedir responsabilidades ante manipulaciones incorrectas a intentos de acceso no autorizados.

4.2 Análisis de la evidencia

Una vez que tengamos las evidencias digitales seleccionadas y almacenadas de forma organizada, pasamos a la fase más cuidadosa, que es catalogado como Análisis Forense propiamente dicho, cuyo objetivo es reconstruir todos los datos disponibles que se encuentren en la línea temporal del ataque o llamada *timeline,* una vez tengamos determinado la cadena de sucesos que tuvieron lugar desde el instante anterior al inicio del ataque, hasta el momento de su descubrimiento

Dicho análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. (López, p, 16).

Una vez se describa este proceso de análisis se empleará las herramientas propias del sistema que se emplee como huésped y las evidencias que se recopilen en su ToolKit, Con esto se pretende formar una visión amplia de los procesos que ayudaran a comprender con facilidad el funcionamiento de las herramientas específicas para el análisis forense del sistema.

5.2 Documentación y Presentación de los Resultados

Una vez el incidente haya sido detectado cabe aclara que es importante comenzar a tomar nota de las actividades que se lleven a cabo. Cada proceso deberá ser documentado y fechado desde que se revela el incidente hasta que finalice el proceso de análisis forense, esto hará que sea más eficiente y efectivo al tiempo que disminuirá las posibilidades de error a la hora de gestionar el incidente

Por otra parte, cuando haya finalizado el análisis y durante éste, tendrá que mantener informados a las personas autorizadas de la organización, e implementar algunos métodos de comunicación. Además, debemos tener dispuesto una serie de formularios y adicional a esto un seguimiento de los incidentes los cuales se van a presentar en dos tipos de informes uno técnico y otro ejecutivo.

De acuerdo con López (2007) el diseño del formulario puede ayudar efectivamente el propósito de que cada departamento o área de la organización, de tal manera que será diligenciado y se generará un compromiso por el equipo que revisará el incidente, adicionalmente estos son los formularios que deberían ser utilizados en caso de algún incidente.

- ✓ Documento de custodia de la evidencia.
- ✓ Formulario de identificación de los equipos y componentes.
- ✓ Formulario de incidencias tipificadas.
- ✓ Formulario de publicación del incidente.
- ✓ Formulario de recogida de evidencias.
- ✓ Formulario de discos duros.

De acuerdo a lo mencionado anteriormente el Informe Técnico consiste en una exposición detallada del análisis realizado. Dicho informe se deberá profundizar en metodología, técnicas y hallazgos de la información del equipo forense, por lo tanto, deberá contener, los siguientes puntos.

- ✓ Antecedentes del incidente.
- ✓ Recolección de los datos.
- ✓ Descripción de la evidencia.
- ✓ Entorno del análisis.
- ✓ Descripción de las herramientas.
- ✓ Análisis de la evidencia.
- ✓ Información del sistema analizado.
- ✓ Características del SO.
- ✓ Aplicaciones. Servicios.
- ✓ Vulnerabilidades.
- ✓ Metodología.
- ✓ Descripción de los hallazgos.
- ✓ Huellas de la intrusión.
- ✓ Herramientas usadas por el atacante.
- ✓ Alcance de la intrusión.
- ✓ El origen del ataque
- ✓ Cronología de la intrusión.
- ✓ Conclusiones.
- ✓ Recomendaciones específicas.
- ✓ Referencias.

Dentro del informe ejecutivo consiste en un resumen del análisis realizado, pero teniendo en cuenta que no debe llevar una explicación técnica, si no con un lenguaje común en el que se mostrara todos los hechos destacables que ocurrió en el análisis del sistema. El informe constará entre tres y cinco páginas, para que se sea de fácil entendimiento al momento de exponer lo sucedido al personal no especializado en sistemas informáticos, como Recursos Humanos, Áreas Administrativas e incluso los directivos de la organización. Este informe deberá llevar los siguientes parámetros.

- ✓ Motivos de la intrusión.
- ✓ Desarrollo de la intrusión

- ✓ Resultados del análisis.
- ✓ Recomendaciones.

3. HERRAMIENTAS UTILIZADAS EN EL ANÁLISIS FORENSE INFORMÁTICO.

En esta parte de la investigación, se explicará el uso de las herramientas que utilizan los expertos forenses en materia digital para dar con los intrusos y poder conocer a ciencia cierta qué ataque fue cometido en el sistema de información y sus posibles consecuencias para aquellas personas o entidades que han sufrido ataques mal intencionados.

Estas herramientas ayudan a priorizar y a realizar tareas que ayudan a facilitar e identificar las causas que afectaron el sistema, igualmente se seguirán desarrollando herramientas bastante sofisticadas que vayan en contra de los análisis forenses que intentan no dejar rastros, borrar o ocultar información esencial a la hora de llevar a cabo las tareas in situ por parte del perito o investigador, de tal manera que se dificulte o posibilite el vencimiento de términos en un determinado proceso ya sea este administrativo o judicial, hablamos de esa fracción de tiempo de que dispone un fiscal para presentar dichas pruebas ante un juez que lleve el caso.

Algunas de las herramientas que son usadas con frecuencia en procesos de informática forense utilizados en PC- Escritorio, Red de Servidores y dispositivos móviles son:

1.3 Adquisición y Análisis Forense Digital de la Memoria RAM

Es un Set de utilidades que permite la adquisición de la memoria RAM para posteriormente hacer un análisis con ella.

✓ **Volatility:** El programa del cual vamos a hablar nos sirve para llevar acabo el estudio el cual está programado en Python y ya viene instalado por defecto en algunas distribuciones Linux especializadas y en actividades de pentesting como Kali de la memoria RAM. De esta herramienta podemos obtener:

Información de la captura de la RAM. Nos proporcionará información sobre el sistema operativo, en caso del ejemplo veremos que se trata de un Windows.

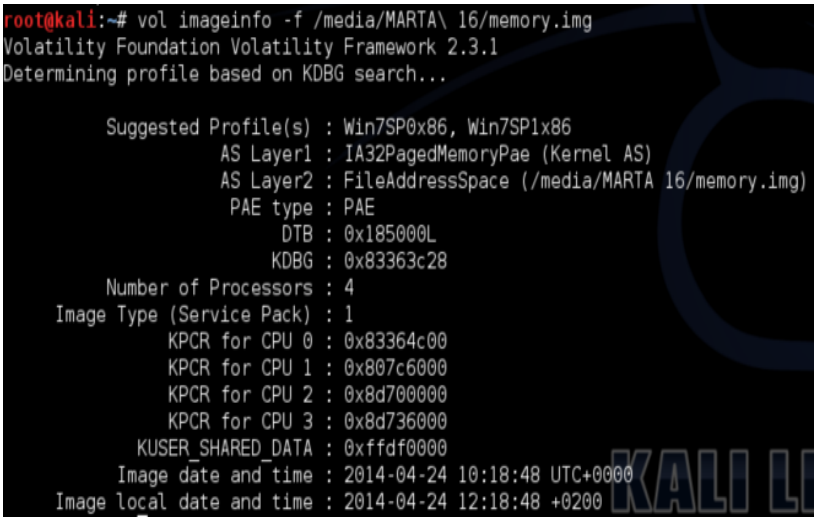

Figura 4: Análisis forense de memoria RAM. Recuperado de http://www. http://wh0s.org/2014/05/05/analisis-forense-de-memoria-ram-ii/

En las direcciones de memoria en las que se encuentran los registros del sistema, nos será muy útil para obtener información de otros comandos, tal como se ve en el comando utilizado denominado *profile* que nos ha proporcionado el comando anterior.

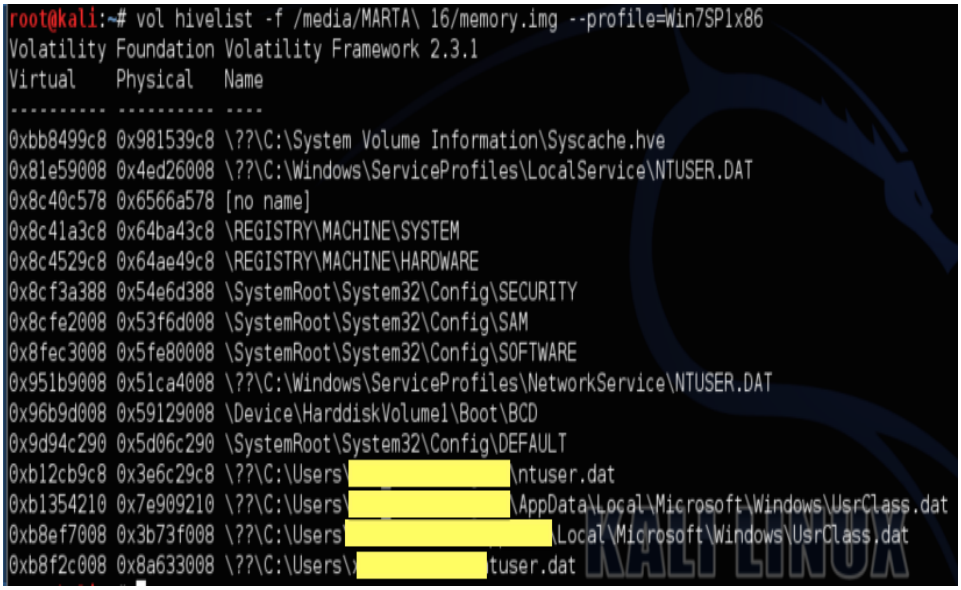

Figura 5: Direcciones del sistema en la memoria RAM. Recuperado de http://www. http://wh0s.org/2014/05/05/analisis-forense-de-memoria-ram-ii/

Hashes de las cuentas de usuario del sistema, utilizando las direcciones de memoria de los registros SYSTEM y SAM obtenemos una lista de los usuarios y su hash correspondiente; También debemos tener en cuenta que a pesar de no tener la contraseña en texto plano se dice

que es suficiente ya que vamos a utilizar una técnica *"Pass The Hash"* por medio del cual se va a obtener el acceso al sistema.

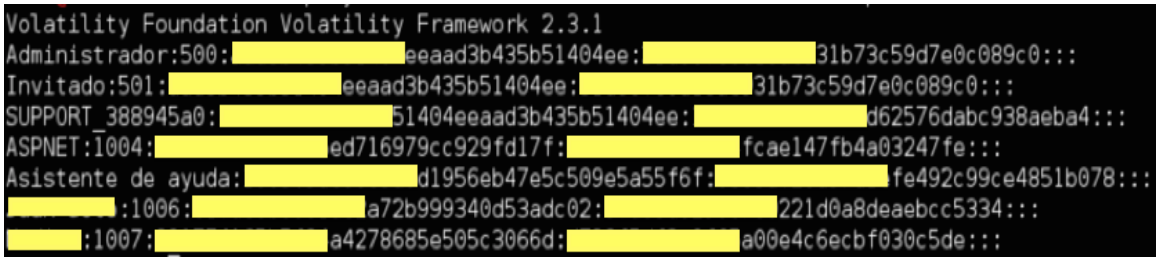

Figura 6: Cuentas de usuario del sistema. Recuperado de http://www. http://wh0s.org/2014/05/05/analisis-forense-de-memoria-ram-ii/

Listado de procesos activos en el momento de la captura de la RAM, esta nos va a servir para que el comando "pstree" nos muestre los procesos que se encuentran activos y eso hace que se relacionen entre ellos, es decir que proceso es pareja de otro proceso.

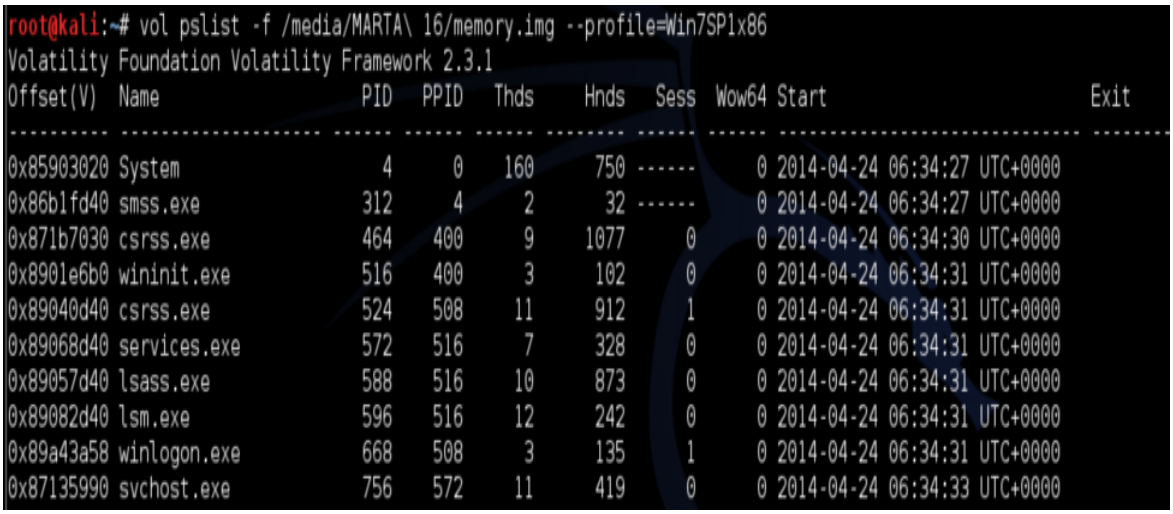

Figura 7: Lista de procesos activos. Recuperado de http://www. http://wh0s.org/2014/05/05/analisis-forense-de-memoria-ram-ii/

✓ **RedLine.** Acelera la captura de la memoria en vivo y permite analizarla para proporcionar una alta capacidad de investigación la cual acoge al usuario de identificar los signos de actividad maliciosa a través de la memoria, el análisis de los archivos y el desarrollo de un perfil de evaluación de amenazas que podemos hacer con por medio de Redline.

Con esta herramienta podemos auditar a fondo y recoger todos los procesos en ejecución y los conductores de la memoria RAM, tales como los metadatos del sistema de archivos, los datos del registro, registros de eventos, información de la red, los servicios y las tareas e historial web. Por otra parte, al analizar y visualizar los datos de auditoría importados, incluyendo la capacidad de filtrar los resultados en torno a un marco de tiempo determinado, podrá ser utilizanda la funcionalidad de la línea de tiempo de Redline con las características TimeWrinkle y TimeCrunch.

Por otra parte, al normalizar el análisis de memoria con un flujo de trabajo se ejecutará el análisis de malware basado en la prioridad relativa, esto hace que al identificar los procesos más relevantes que se van a investigar da uso de la puntuación RedLine malware indicando el índice de riesgos que va a generar el análisis de indicadores de Compromiso (COI). Por lo tanto, se suministra con un conjunto de IOC, el Agente portátil RedLine que se configura automáticamente para recopilar los datos necesarios para realizar el análisis COI lo cual hará que la revisión nos arroje los resultados.

✓ **Memoryze -** Es un software forense de memoria libre que nos ayuda a los usuarios encontrar los incidentes que se encuentran mal en memoria viva. Memoryze puede adquirir y / o analizar imágenes de la memoria y en los sistemas vivos puede incluir el archivo de paginación en su análisis.

- La imagen de la gama completa de la memoria del sistema (sin dependencia de las llamadas a la API).
- Una imagen de proceso "el espacio de direcciones en el disco, incluyendo un proceso de 'cargado DLL, EXE, las escombreras y pilas.
- Una imagen de controlador especificado o todos los controladores cargados en la memoria en el disco.

También podemos decir que con este programa se enumeran todos los procesos activos (al igual que los que están ocultos por rootkits) así como:

- Informe todos los identificadores abiertos en un proceso (incluidos todos los archivos, claves de registro, etc.).
- Listar el espacio de direcciones virtuales de un proceso determinado, incluidos todos los archivos DLL cargados y todas las partes que se asignan de la pila y pila.
- Listar todos los sockets de red que tiene abierto el proceso, incluyendo cualquier ocultos por rootkits.
- Especificar las funciones importadas y exportadas por el EXE y DLL.
- Hash el EXE y DLL en el espacio de direcciones del proceso (MD5, SHA1, SHA256. Este es el disco con base).
- Verificar las firmas digitales de los archivos EXE y DLL (basadas en el disco).
- Salida de todas las cadenas en memoria en función de cada proceso.

Dentro de este programa se puede identificar todos los controladores cargados en la memoria RAM, incluyendo aquellos que están ocultos por rootkits y a su vez están en cada controlador realizando la siguiente función:

- Especificar las funciones de las importaciones y exportaciones de controladores.
- Hash el conductor (MD5, SHA1, SHA256 y. Basada en disco).
- Verificar la firma digital del controlador (basadas en el disco).
- Salida de todas las cadenas en memoria en una base por conductor.
- Dispositivo de Informe y de capas conductoras, que se puede utilizar para interceptar los paquetes de red, las pulsaciones del teclado y actividad de los archivos.
- Identifica todos los módulos de núcleo que se cargan por caminar una lista enlazada. Identificar los ganchos (a menudo utilizados por los rootkits) en la tabla de llamadas al sistema, las tablas de descriptores de interrupción (IDT) dispuestos y tablas de funciones del controlador.

Dicho programa podrá realizar todas estas funciones anteriormente mencionadas para el funcionamiento de la memoria del sistema en vivo o archivos de imágenes que se encuentran en la memoria y que son adquiridos por Memoryze u otras herramientas.

Memoryze trabaja oficialmente en los siguientes sistemas:

- Windows 2000 Service Pack 4 (32-bit)
- Windows XP Service Pack 2 and Service Pack 3 (32-bit)
- Windows Vista Service Pack 1 and Service Pack 2 (32-bit)
- Windows Vista Service Pack 2 (64-bit) *
- Windows 2003 Service Pack 2 (32-bit and 64-bit)
- Windows 7 Service Pack 0 (32-bit and 64-bit)
- Windows 2008 Service Pack 1 and Service Pack 2 (32-bit)
- Windows 2008 R2 Service Pack 0 (64-bit)
- Windows 8 Service Pack 0 (32-bit and 64-bit)
- Windows Server 2012 Service Pack 0 (64-bit)

2.3 Programas para análisis forense en montaje de discos

Estos programas son utilizados para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla.

✓ **OSFMount** - Le permite montar archivos de imagen de disco locales (copias bit a bit de una partición de disco) en Windows con una letra de unidad. El programa, puede analizar el archivo de imagen de disco con PassMark OSForensics mediante el uso de letra de unidad del volumen montado. De forma predeterminada, los archivos de imagen se montan como sólo lectura para que los archivos de imagen originales no se alteren.

También apoya la creación de discos RAM, básicamente un disco montado en la memoria RAM. En general, esto tiene un gran beneficio del cual se beneficia la velocidad sobre el uso de un disco duro. Como tal, esto es útil con aplicaciones que requieren acceso a disco de alta velocidad, aplicaciones de bases de datos, juegos (como los archivos de caché de juego) y navegadores (archivos de caché). Una segunda ventaja es la seguridad, ya que el contenido del disco no se almacena en un disco duro físico sino más bien en la memoria RAM y el apagado del contenido del sistema del disco no es persistente.

OSFMount es compatible con imágenes de CD en formato ISO, que pueden ser útiles en el momento del montaje y cuando se va a utilizar en un CD en particular, para así generar una frecuencia y velocidad de acceso que es lo más importante al momento de abrir un CD.

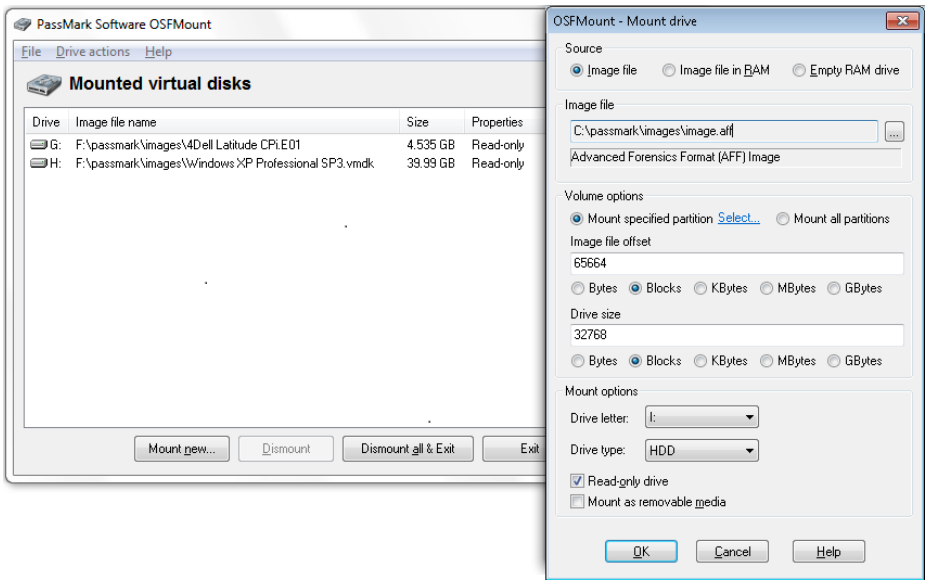

Figura 8: PassMark Software. Recuperado de http://www.osforensics.com/tools/mount-disk-images.html

✓ **LiveView.** Esta herramienta forense gráfica basada en Java que crea una máquina virtual de VMware (al estilo disco duro) genera una imagen de disco en bruto o disco físico, lo cual nos permite que el examinador forense para "arrancar" la imagen o el disco, obtenga una perspectiva interactiva a nivel de usuario del medio ambiente, todo ello sin modificar la imagen de fondo a un disco. Debido a que todos los cambios realizados en el disco se escriben en un archivo separado, el examinador puede revertir al instante todos sus cambios de vuelta al estado originario del disco. El resultado final es que uno no necesita crear adicionales "desechables" es decir, copias del disco o de imagen para crear la máquina virtual.

Dicha herramienta es capaz de arrancar en:

- Disco lleno imágenes en bruto.
- Partición de arranque imágenes en bruto.

- Discos físicos (Se adjunta a través de una USB o Firewire puente).
- Formatos de imagen que son especializados en el cierre de software de montaje utilizado

Estos son los Sistemas Operativos más utilizados:

- Windows 2008, Vista, 2003, XP, 2000, NT, Me, 98
- Linux (soporte limitado) que se caracteriza por las escenas, con visión directa automatizada con una gama amplia de tareas técnicas.

Algunos de estos incluyen la resolución de conflictos de hardware que resultan del arranque en un hardware distinto de aquel en el que se instaló originalmente el sistema operativo, la creación de un MBR personalizado para imágenes de partición, especificando correctamente un disco virtual para que coincida con la imagen original o disco físico.

✓ **ImDisk.** Es un controlador de disco virtual para Windows NT / 2000 / XP / Vista / 7/8 / 8.1 / 10 y Windows Server 2003/2003 R2 / 2008/2008 R2 / 2012/2012 R2, el cual sirve para ediciones de 32 y 64 bits y crea un disco virtual ya sea un CD o un DVD con archivos de imagen o memoria del sistema.

El paquete de instalación genera un programa de control de modo de consola llamada imdisk.exe y un applet de panel de control. Se instalan después de que se haya terminado de instalarse el controlador llamado Imdisk, sin parámetros para la ayuda de sintaxis o doble clic en el icono ImDisk en el Panel de control. También añade un elemento de menú en el Explorador de Windows, por lo que se puede hacer clic derecho sobre un archivo para montarlo como una unidad de disco virtual.

Los usuarios de mdconfig en FreeBSD, probablemente estarán familiarizados con la sintaxis y estarán en línea con los comandos de imdisk.exe. El conductor de servicio y programa de control se pueden desinstalar utilizando la opción Agregar / Quitar Programas en el Panel de control. No es necesario reiniciar para instalar o desinstalar.

Un conductor adicional, awealloc, en este paquete de instalación es compatible con la asignación de memoria más allá del límite de 4 GB en Windows de 32 bits en la extensión de ventana de dirección, AWE; Por lo tanto, el programa nos permite el reenvío de solicitudes de E / S a terceros manejadores de formato de archivo de imagen o de los servicios en otros equipos de la red. Esto hace que sea posible arrancar una máquina con particiones NTFS con un Live-CD y utilizar la herramienta incluida DEVIO dejar ImDisk en otro equipo que ejecuta Windows en la red donde monta la partición NTFS en la máquina con una partición NTFS defectuoso. De esta manera usted puede recuperar la información e incluso podrá ser corrida de unidad en máquinas en las que Windows no arranca.

3.3 Carving y herramientas de disco

Consiste en la recuperación de datos perdidos, borrados, búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes, vídeos, recuperación de particiones y tratamiento de estructuras de discos.

- ✓ **PhotoRec.** Es un software de recuperación de datos de archivos diseñado para recuperar archivos perdidos, incluyendo video, documentos y archivos de los discos duros, CD-ROM, en caso de pérdida de imágenes de memoria de la cámara digital. PhotoRec ignora el sistema de archivos y va después de los datos subyacentes, por lo que seguirá funcionando incluso si el sistema de archivos de sus medios de comunicación ha sido severamente dañada o reformateada.

También podemos decir que dicha aplicación se cataloga como multi – plataforma de código abierto por lo que se distribuye bajo una licencia pública general llamada GNU (GPLV v2 +). PhotoRec es un programa de complemento a TestDisk, una aplicación para recuperar particiones perdidas en una amplia variedad de sistemas de archivos y que permite hacer discos de arranque por lo que se genera un disco en modo arrancables de nuevo.

Para tener en cuenta la seguridad de Photorec, este se considera un acceso de solo lectura para poder manejar la tarjeta de memoria o unidad en donde se va a recuperar los datos perdidos que son de importancia. Al momento que un archivo de imagen se elimina por accidente o se descubre alguna falta, no debemos guardar más fotos ni archivos en el dispositivo de memoria o

una unidad de disco duro; de lo contrario puede sobrescribir los datos perdidos. Esto significa que durante el uso de PhotoRec, no debe optar por guardar los archivos recuperados a la misma partición donde estaban guardados. ¿En que sistemas operativos podemos instalar estos programas?

- DOS/Windows 9x
- Windows NT 4/2000/XP/2003/Vista/2008/7/10
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sun Solaris
- Mac OS X

✓ **NTFS Recovery –** Es una utilidad totalmente automática que recupera datos de discos dañados o formateados. Está diseñado con un usuario doméstico en mente en el cual usted no necesita tener ningún conocimiento especial en la recuperación del disco.

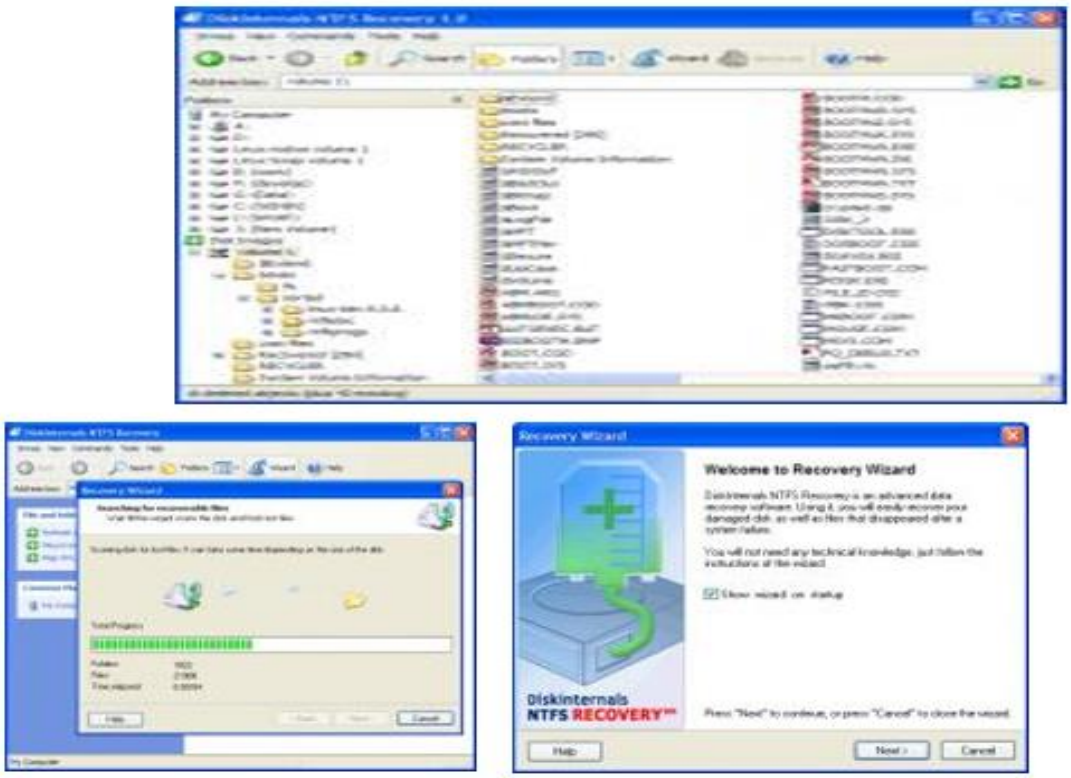

Figura 9: Pasos para recuperar datos dañados en un disco duro. Recuperado de http://www.osforensics.com/tools/mount-disk-images.html

El icono de la "Papelera de reciclaje" en el escritorio de Windows le permite recuperar archivos borrados. Por desgracia, hay muchas situaciones posibles cuando la papelera de reciclaje es inútil, lo cual hará que sea posible la recuperación de un archivo como, por ejemplo:

- Un volumen de disco que contiene valiosa información fue dañado debido a un mal funcionamiento del sistema.
- Un volumen de disco se daña debido por un virus peligroso
- Windows no puede tener acceso a una unidad de disco
- Disco fue dañado
- Por error se ha formateado un volumen de disco
- Los archivos o carpetas no se pueden leer
- Tabla de particiones corruptas o dañadas.

Debemos tener en cuenta que cuando se pierde por completo es porque el usuario sobrescribe en otro archivo, esto se puede observar en los sistemas operativos de XP, Windows 7 y otros sistemas operativos modernos de Microsoft.

✓ **Bulk extractor.** Es una herramienta que nos permite analizar una imagen del disco duro, un archivo o un directorio de archivo y extraer la información útil sin la necesidad de analizar las estructuras que tiene el archivo, por lo que se caracteriza en que es más rápido que otras herramientas disponibles. Uno de los principales resultados que se obtiene del análisis es, la inspección o proceso con otras herramientas especializadas.

Otra de las ventajas que no podemos ignorar para el análisis de archivos es el software el cual se utiliza para procesar cualquier medio digital, incluyendo los discos duros y los medios de almacenamiento SSD, tarjetas de memoria que son expandibles tanto para las cámaras como para los Smartphone, registros de paquetes de red y otros tipos de información digital.

Una de las desventajas en la utilización de la herramienta es la dificultad de uso, por lo que es muy minucioso y su velocidad hace que el análisis de los archivos almacenados se convierta en una herramienta principal, para su buen funcionamiento.

4.3 Utilidades para el sistema de ficheros

Conjunto de herramientas para el análisis de datos y ficheros esenciales en la búsqueda de un incidente.

✓ **INDXParse.** Acepta una serie de parámetros de línea de comandos e interruptores que determinan lo que se analiza de los datos y el formato de salida. Actualmente INDXParse.py soporta tanto CSV (por defecto) y formatos de salida Bodyfile (v3). El esquema CSV es el siguiente:

- Nombre del archivo
- El tamaño físico del archivo
- Tamaño lógico del archivo

- Fecha y hora de modificación
- Marca de tiempo de Acceso
- fecha haya cambiado
- Creada marca de tiempo

Si el programa encuentra un error al analizar el nombre del archivo, el campo de nombre de archivo contendrá una mejor estimación, y generará un comentario "(error de decodificación nombre de archivo)". Si el programa encuentra un error mientras se analiza las marcas de tiempo, una marca de tiempo correspondiente al tiempo UNIX será impreso en su lugar.

✓ **WinPrefetchView.** Cada vez que se ejecuta una aplicación en el sistema, un archivo de Prefetch que contiene información sobre los archivos cargados por la aplicación, es creada por el sistema operativo Windows, lo cual hace que la información contenida en el archivo de Prefetch sea utilizada para optimizar el tiempo de carga de la aplicación la próxima vez que se ejecute.

WinPrefetchView es una pequeña utilidad que lee los archivos de obtención previa almacenados en su sistema y muestra la información almacenada en ellos. Al mirar en estos archivos, puede aprender que los archivos de cada aplicación se están utilizando para que los archivos se carguen en el arranque de Windows.

5.3 Análisis de Malware

✓ **PDF Stream Dumper –** La herramienta se especializa en tratar de analizar por JavaScript y obsfuscated, que son encabezados de pdf y se caracterizan por tener un bajo nivel, lo cual genera que los objetos y códigos sean formateados de los códigos para así generar la depuración en vivo de los Scripts.

Dicha herramienta nos permite crear unas clases de cajas de herramientas para manejar la funcionalidad como un motor de refactorización lo cual hará que sea muy estable en el momento de realizar el análisis en un modo de secuencia de comandos y esto generara el reemplazo como una función aleatoria que arrojara un nombre con unas variables que son versiones lógicas para desinfectar y facilitar la lectura del análisis. PDF Stream Dumper es compatible con Win2k, XP,

Vista, Win7, y su actualización es una secuencia que analiza y optimiza una rapidez del 20% de velocidad.

De acuerdo al análisis con PDF Stream Dumper el Scripts se caracterizará por automatizar la herramienta en:

- **Stats.vbs csv:** Construye archivo csv con los resultados de menor barra de estado para todos los archivos en un directorio.
- **Pdfbox_extract.vbs:** PDFBox uso para extraer todas las imágenes y el texto de archivo actual
- **String_scan.vbs:** Escanear todas las corrientes descomprimidas en todos los archivos en un directorio para una cadena que introduzca
- **Unsupported_filters.vbs:** Escanear un directorio y la lista de todos los archivos PDF que tienen filtros no compatibles construir
- **Filter_chains.vbs:** Recursivamente analiza directorio padre para archivos PDF que utilizan varios filtros de codificación en un arroyo.
- **Obsfuscated_headers.vbs:** Recursivamente analiza directorio padre para los documentos PDF que obsfuscated cabeceras de objetos
- **Pdfbox_extract_text_page_by_page.vbs:** PDFBox utiliza para extraer datos de páginas en archivos individuales

✓ **Captura BAT.** Esta es una herramienta de análisis del comportamiento de las aplicaciones para la familia del sistema operativo Windows 32. BAT captura y es capaz de controlar el estado de un sistema durante la ejecución de las aplicaciones y procesamiento de documentos, lo que proporciona un análisis de ideas sobre cómo el software funciona e incluso si no hay código en la fuente, lo cual hará que esté disponible. Para la captura de BAT y monitoreo de los cambios de estado en un nivel de kernel baja se puede utilizar fácilmente a través de varias versiones y configuraciones del sistema operativo Windows 32.

También podemos decir que proporciona un poderoso mecanismo para excluir el ruido del evento que ocurre de forma natural en un sistema inactivo o cuando se utiliza una aplicación

específica. Este mecanismo es muy fino y permite que un analista tome en cuenta el proceso que causan los diferentes cambios de estado.

Como resultado, este mecanismo permite la captura, incluso para analizar el comportamiento de los documentos que se ejecutan en el contexto de una aplicación, por ejemplo, el comportamiento de un documento de Microsoft Word malicioso.

Para la obtención y un buen comportamiento de Capture BAT se debe tener el sistema operativo Windows 2000, XP y Vista y lo más importante es que no se necesita un paquete de servicio.

6.3 Herramientas de análisis forense informático en la red

Son todas las herramientas relacionadas con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

✓ **Xplico.** El Xplico es una herramienta de análisis forense de red (NFAT) en el cual, su ámbito principal es extraer todo el contenido de datos de la aplicación de una captura de red (archivo pcap o adquisición en tiempo real). Por ejemplo, Xplico es capaz de extraer todos los correos electrónicos realizadas por el POP y SMTP y todo el contenido realizado por el protocolo HTTP de un archivo pcap.

Una de las características de Xplico es:

- Admite los protocolos: HTTP, SIP, FTP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6.
- VoIP códec de audio compatibles: G711ulaw, G711alaw, G722, G729, G723, G726 y MSRTA (x-msrta: Tiempo Real Audio)
- Identificación de Puerto Independiente Protocolo (PIPI) para cada protocolo de aplicación;
- Multihilo.
- Los datos de salida y la información en la base de datos SQLite o base de datos y / o archivos de MySQL.

- En cada uno de los datos reensamblados por Xplico se asocia un archivo XML que identifica de manera única los flujos y la pcap que contiene los datos nuevamente montados.
- elaboración en tiempo real (depende del número de flujos, los tipos de protocolos y por el rendimiento de la computadora --- RAM, CPU, el tiempo de acceso de alta definición.
- reensamblaje TCP ACK con la verificación de cualquier paquete ACK o verificación suave.
- búsqueda de DNS inversa de paquetes DNS contenida en los archivos de insumos (PCAP), no desde un servidor DNS externo.
- No hay límite de tamaño en la entrada de datos o el número de archivos de entrada (el único límite es el tamaño HD).

✓ **NetworkMiner.** Es una herramienta de análisis forense de red (NFAT) para Windows (pero también funciona en Linux / Mac OSX / FreeBSD). Se puede utilizar como una herramienta pasiva de captura de red sniffer con el fin de detectar los sistemas operativos, las sesiones, los nombres de host, puertos abiertos etc., sin poner ningún tráfico en la red.

NetworkMiner también puede analizar archivos PCAP para el análisis fuera de línea y así mismo para regenerar, lo cual hará que se vuelvan a montar los archivos transmitidos y los certificados de los archivos PCAP.

NetworkMiner hace que sea fácil de realizar análisis avanzados de tráfico de red (NAT), proporcionando artefactos extraídos en una interfaz de usuario intuitiva, por lo que la forma de presentar los datos no sólo hace el análisis más simple, sino que también ahorra tiempo valioso para el analista o investigador forense. Su primera versión es de 2007 convirtiéndose una herramienta muy popular entre los equipos de respuesta a incidentes, así como aplicación de la ley y que hoy es utilizado por empresas y organizaciones de todo el mundo.

NetworkMiner puede extraer los archivos y certificados transferidos por la red mediante el análisis de un archivo PCAP u olfateando el tráfico directamente desde la red. Esta funcionalidad se puede utilizar para extraer y guardar archivos multimedia (como archivos de audio o vídeo),

que se transmiten a través de una red de sitios web como YouTube y a su vez admite los protocolos para la extracción de archivos son FTP, TFTP, HTTP, SMB, SMB2 y SMTP.

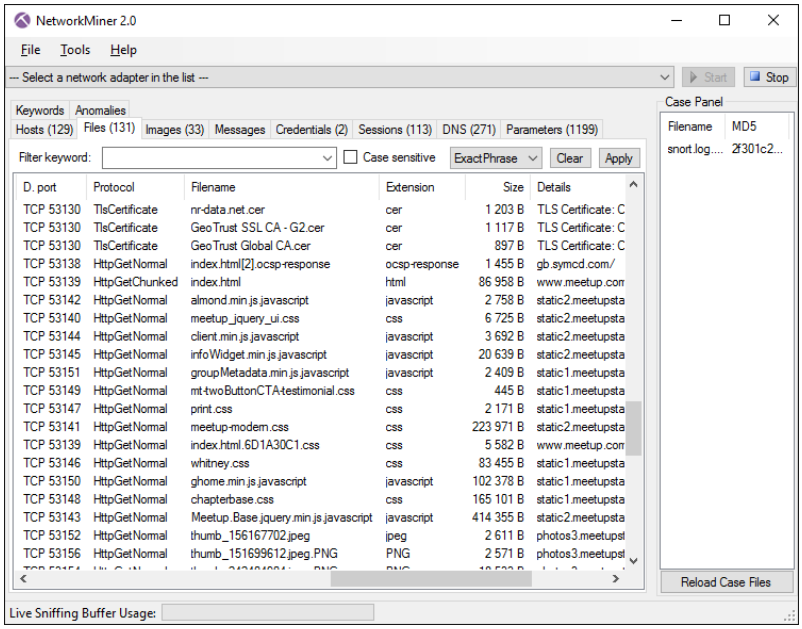

Figura 10: Trafico de red en disco sniff. Recuperado de http://www.forensicswiki.org/wiki/Xplico

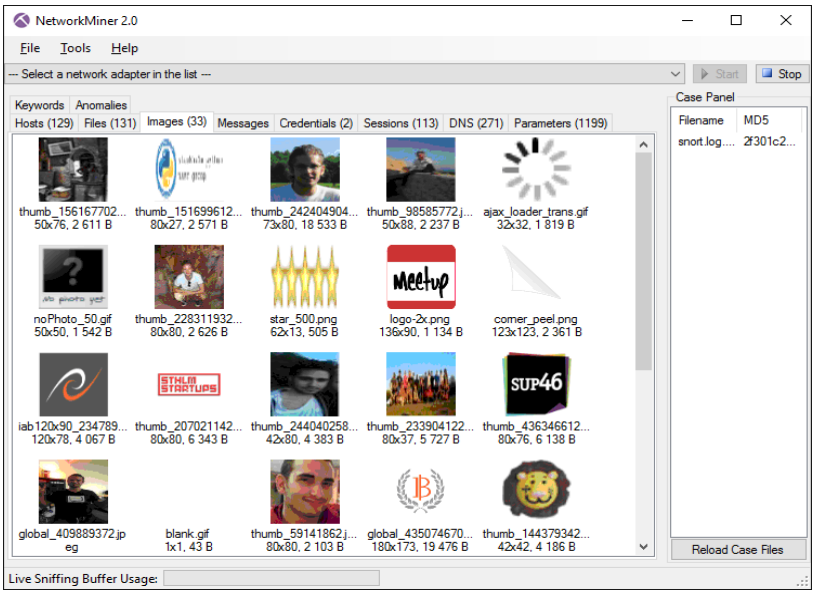

Figura 11: Miniaturas de imágenes extraídas en el disco. Recuperado de http://www.forensicswiki.org/wiki/Xplico

Esta aplicación tiene dos modalidades de cómo obtener la herramienta para el funcionamiento en un PC:

- Una es de la obtención de credenciales el cual vamos a generar un usuario y una contraseña para obtener un protocolo de soportes extraídos. La ficha credencial a veces también muestra información que puede ser utilizada para identificar a una persona en particular, como las cuentas de usuario para los servicios en línea populares como Gmail o Facebook.

- Otra modalidad muy útil, es que el analista puede buscar los datos almacenados o por palabras claves la cual permite al usuario insertar cadena arbitraria o byte-patrones que se han buscado con la funcionalidad de búsqueda por palabra clave.

La modalidad de NetworkMiner Profesional viene instalado en una unidad flash USB especialmente diseñado para la ejecución directa de la unidad flash USB desde NetworkMiner y dicha aplicación portátil no requiere ningún tipo de instalación, tal como lo podemos observar en la siguiente figura:

Figura 12: Unidad flash USB. Recuperado de http://www.netresec.com/?page=NetworkMiner

7.3 Programas y herramientas para Dispositivos Móviles (iPhone, Black Berry y Android.

a) Programas para IPhone.

✓ **IPhone Analyzer.** iOS 6 funciona sólo parcialmente en el momento y en algunas funciones fallan o faltan. Por desgracia, el trabajo remunerado significa que no podemos solucionar este problema en este momento, pero daríamos la bienvenida a cualquier otra persona el envío de parches.

Explorar la estructura de la herramienta de archivos internos de su iPhone o de un teléfono incautado en el caso de los equipos forenses, utilizando cualquiera de los archivos de copia de seguridad propia del iPhone, para iPhone de visualización de plist, SQLite, y hexadecimal son compatibles incluyendo IOS 5 lo que hace que es compatible.

IPhone Analyzer se caracteriza por:

- Explorando iPhone Backup
- de archivo nativo de visualización (plist, SQLite, etc)
- Busca incluyendo expresiones regulares
- acceso ssh para los teléfonos con jailbreak (beta)
- Informes
- Restaurar archivos
- recuperar copias de seguridad
- Ver todas las fotos del iPhone
- examinar la libreta de direcciones, SMS y las cargas de los demás
- encontrar y recuperar las contraseñas
- archivos de sistema de archivos local de exportación a
- mapas en línea y fuera de línea
- Geo pista que un dispositivo ha sido
- IOS5 y versiones anteriores apoyado
- IOS6 sólo se admite parcialmente (varios conocidos problemas)

✓ **IPhone Backup Extractor.** Nuestro software iPhone Backup Extractor puede recuperar contactos, imágenes, historiales de llamadas, MMS, SMS y mensajes de texto, video, mensajes de voz, entradas de calendario, notas, archivos de aplicaciones, juegos guardados, información de depuración y datos que de otro modo serían de fácil acceso.

También podemos mencionar que dicho software funciona en iPhone SE, 6 y 6S, iPhone 6 Plus y 6S Plus, iPhone 5s, el iPhone 5, iPhone 5c, el iPhone 4s, iPhone 3GS, iPhone 3G, iPod, lo

cual genera una copia de seguridad para proteger todas las versiones de iTunes, iCloud y iOS, incluyendo iOS 10.

El software iPhone Backup Extractor, es una aplicación que es ideal para la recuperación de información para el equipo que cumpla con estos tres ítems:

- Ha dañado los datos o perdido su iPhone, iPad o iPod
- Ha eliminado algo importante
- Falla en la actualización de iOS

También podemos mencionar que el software tiene unas características y funcionalidades que se caracterizan por ser muy importantes al momento de realizar el análisis forense las cuales son:

- Convierte automáticamente las bases de datos de copias de seguridad extraídas en formatos CSV, VCard o ICAL, para poder importarlas fácilmente a Excel, Outlook o Webmail.
- Recupere datos desde copias de seguridad cifradas de iTunes.
- Recupere datos desde copias de seguridad de iCloud.
- Fácil de utilizar, no se requieren conocimientos técnicos.
- Sin spyware ni publicidad.
- Potente versión gratuita.
- Visor de PList integrado.

✓ **IPhone-data protection.** Herramienta para iPhone en donde su funcionalidad es tener la información en iOS 3/4/5/6/7 en donde se caracteriza por la protección de datos. También podemos mencionar que dentro de la herramienta principalmente se crea un disco RAM forense, el cual es importante en el ataque ante las contraseñas simples que son de 4 dígitos y el descifrado que son copias de seguridad de iTunes.

Tenemos que mencionar que hay una versión modificada que se llama HFS- Explorer y es utilizada en la salida de las herramientas del Disco RAM el cual procesa imágenes de partición de datos de iOS, esto quiere decir que son los códigos de fuente. Para tener en cuenta las imágenes

que están dentro del Disco se podrán descifrar de forma permanente con la función *fem* descifrador teniendo los siguientes parámetros:

- iOS 5 actualizaciones
- Bajo nivel de iOS forense
- Manzana - Seguridad IOS - mayo 2012
- SEC-T 2012 - recuperación iPhone prima NAND y forense - Torbjörn Lofterud.

b) Programas para Black Berry.

✓ **Phoneminer.** Fue desarrollado como una solución a este mismo problema, lo que permite a los usuarios recuperar datos de archivos de copia de seguridad del teléfono y luego ver y exportar datos.

Puede restaurar fotos, restauración de vídeo, recuperar una libreta de direcciones eliminado, recuperar correos electrónicos, registros de llamadas de salvamento y lo más importante que es con gran facilidad. Algunos ejemplos son:

- Contactos (libreta de direcciones).
- Mensajes SMS
- Fotos
- Los correos electrónicos
- Calendario
- Registros de llamadas
- Películas
- Memos
- Tareas

Este programa también realiza la recuperación de uno o dos archivos que se encuentren perdidos, pero si el usuario borro todo lo que tenía dentro del equipo, se ejecutara una solución avanzada por medio de la herramienta PhoneMiner en la cual pueden recuperar datos de una

amplia gama de archivos de copia de seguridad y le permiten guardar los datos en un número de formatos de archivo populares dentro de los cuales tenemos:

- Contactos de Google
- Excel (XLS y XLSX)
- EML (correo electrónico)
- CSV
- PDF
- VCF (vCard)
- HTML
- XML
- ICS (Apple iCal).

Debemos tener en cuenta que la herramienta Phoneminer es compatible con una amplia gama de marcas populares de dispositivos:

- Apple iPhone, iPad y iPod
- Sony Xperia y Sony Ericsson
- BlackBerry (IPD y la acreditación de archivos) Tormenta, Bold, Curve, Pearl, el estilo, la antorcha, Touch & Tour.

c) Programas para Android

✓ **Androguard.** Se caracteriza porque puede analizar, visualizar, modificar y guardar sus aplicaciones con facilidad y de forma estática mediante la creación de su propio software (mediante el uso de la API), o mediante el uso de la herramienta (androlyze) en la línea de comandos. Esta herramienta es útil cuando se desea hacer la ingeniería inversa en una aplicación específica (por ejemplo: el malware).

La segunda parte de la herramienta es hacer nuevas herramientas para obtener las diferencias entre las dos aplicaciones de Android / Java, o para encontrar similitudes en diferentes aplicaciones (por ejemplo: para comprobar si una aplicación de una parte o la totalidad ha sido

robada). Y, ahora bien, podemos comprobar si una aplicación Android está presente en una base de datos (como un malware).

8.3 Cuáles son las herramientas más utilizadas en materia de informática forense?

Como vimos anteriormente en la informática forense son muchas las herramientas utilizadas para como base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, son muy pocas las que cumplen con los protocolos de seguridad establecidos que permiten validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza. (Cano, 2015. p.25)

Es así como estos dos elementos hacen del uso de las herramientas, una constante evaluación y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo. Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, debido que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática. Entre ellas encontramos:

– EnCase Forensic Edition: Programa usado para obtener datos del disco o memoria RAM en documentos, imágenes, correos electrónicos, correo web, artefactos de Internet, caché e historial web, reconstrucción de páginas HTML, sesiones de chat, archivos comprimidos, archivos de copia de seguridad, archivos cifrados, generando un conjunto reiterado de discos independientes llamado (RAID), o estaciones de trabajo, que se maneja en los servidores con la versión 7 y analiza también teléfonos inteligente y tabletas.

El Software Encase permite al especialista forense realizar un análisis de crimen digital en donde la herramienta aplica las siguientes características.

- Copiado Comprimido de Discos Fuente
- Búsqueda y Análisis de Múltiples partes de archivos adquiridos
- Diferente capacidad de Almacenamiento

- Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo.
- Análisis Compuesto del Documento.
- Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de
- E-Mail.
- Firmas de archivos, Identificación y Análisis
- Análisis Electrónico Del Rastro De Intervención.
- Soporte de Múltiples Sistemas de Archivo.
- Vista de archivos y otros datos en el espacio Unallocated.
- Genera el reporte del proceso de la investigación forense como un estimado.
- Visualizador Integrado de imágenes con Galería.

_ **Tool Kit (FTK):** Es una herramienta que nos permite realizar replicas y visualizar los datos que se encuentran en el ordenador, permitiendo una evaluación rápida de la evidencia electrónica, para garantizar un análisis posterior con la herramienta forense Access Data Forensic Toolkit. Por otra parte, FTK permite crear copias perfectas llamadas (Imágenes Forenses) que son datos Cambie la definición de la herramienta y características encontrados en el ordenador sin realizar ningún cambio en la evidencia original. De acuerdo a FTK todos los filtros son personalizables y permite buscar en miles de archivos rápidamente las pruebas necesarias, se dice que FTK es la herramienta más reconocida en forense por el análisis que realiza en los correos electrónicos, y sus principales funciones son:

- Fácil de usar
- Opciones de búsqueda avanzadas
- Registry viewer
- Análisis de correo electrónico y de archivos Zip
- Diseño de capa de base de datos
- Montaje seguro de dispositivos remotos

-Nuix Investigator: Herramienta que le permite a los investigadores procesar en TeraBytes, lo que permite analizar diariamente las evidencias que arroja al momento del análisis, sus

resultados están rápidamente a disposición del investigador para el pertinente análisis. Por otra parte la tecnología avanzada de Nuix se diseñó para la búsqueda y recolección de información a través de grandes cantidades de datos de forma rápida y eficiente, convirtiéndolo en una alternativa superior a otras aplicaciones o herramientas.

Por otra parte los investigadores pueden realizar la adquisición de todos los datos que se encuentran disponibles, mediante el uso de técnicas de investigación avanzada el cual podrán adquirir y entender que el contenido y el contexto son evidencias digitales. Además Nuix es capaz de identificar y relacionar automáticamente elementos claves como nombres de compañías, cantidades de dinero, direcciones de email, direcciones IP, números de la seguridad social, números de teléfono y tarjetas de crédito.

Con esta herramienta se examina todas las fuentes de una sola vez:

- Archivos y carpetas sueltos.
- Bases de datos de email de un usuario (PST, OST, NSF, mbox) o multi-usuario (EDB, Domino, Groupwise).
- Imágenes de herramientas forenses incluyendo dd, EnCase (E0x & Lox) y Access Data AD1.
- Microsoft SharePoint
- Sistemas de archivos de dispositivos móviles e imágenes de Cellebrite, Oxygen Forensic y XRY.
- Mac OS Parallels, Microsoft Virtual Server y el software de virtualización VMware.
- Servicios de correo electrónico en la nube como Hotmail y Gmail.
- Bases de datos Microsoft SQL Server.

-**Autopsy:** Es una herramienta de análisis forense digital que permite ampliar la investigación de lo ocurrido en el equipo. Por lo que es rápida y ejecuta varias tareas en un segundo plano, generando un aprovechamiento de los núcleos del procesador del equipo, y así tener resultados lo más antes posible. Estos análisis requieren de horas para analizar el disco duro, pero en minutos se sabrá si la información no se encuentra, lo que permite que la palabra clave en la carpeta sea del usuario.

- **Recent Activity:** extrae la actividad del usuario como lo último guardado por los navegadores web y el sistema operativo incluso en el registro de Windows.
- **Hash Lookup:** utiliza bases de datos hash para ignorar archivos conocidos del NIST NSRL, se puede utilizar la opción Avanzada para agregar y configurar las bases de datos de hash para usar durante este proceso.
- **Keyword Search:** La búsqueda por palabras clave utiliza listas de palabras clave para identificar archivos con palabras específicas. Puede seleccionar las listas de palabras clave para buscar de forma automática y además podremos crear nuevas listas utilizando el botón "Opciones avanzadas".
- Archive Extractor abre ZIP, RAR, y otros formatos de archivo y envía los archivos para su análisis.
- Exif Image Parser extrae la información EXIF de archivos JPEG y expone los resultados en la interfaz de usuario principal.
- Thunderbird Parser: Identifica Thunderbird MBOX y extrae los correos electrónicos de ellos.

El programa autopsy corre en diversos sistemas operativos como Linux, Unix y hasta en el sistema operativo Microsoft.

- **Xways:** En determinados casos el análisis forense digital se pretende incluir como se evidencia diferentes fotografías de la escena o sitio que sea objeto de nuestra intervención y que de alguna manera estén implicados en el caso o pueda servir como prueba real en el sitio referenciado con los dispositivos relacionados. Para obtener una mejor prueba o análisis de datos se podrá utilizar Xways como sistema de almacenamiento y enlace a dichos archivos fotográficos.

La herramienta Xways contiene un entorno muy avanzado para los investigadores y personas que trabajan como analistas forenses, el cual funciona sobre sistemas operativo o plataformas Window 2000 / XP / 2003 / Vista / Seven / 2008, teniendo en cuenta que debe tener tecnología de 32 y 64 Bits.

Algunas de las características de la Herramienta Xways Son:

- Posibilidad de crear imágenes o copiados seguros de evidencias digitales.
- Recuperación de información eliminada.
- Visualizar estructuras de directorios sobre imágenes del tipo .dd.
- Acceder a discos, RAIDs, e imágenes de gran tamaño (2Tb).
- Soporte nativo para FAT12, FAT16, FAT32, TFAT, NTFS, Ext2, Ext3, Ext4, CDFS/ISO9660/Jolite, UDF.
- Visualización y volcado de memoria RAM y memoria virtual de procesos en ejecución.
- Creación de medios forenses estériles.
- Generación y cálculo de firmas criptográficas (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD.
- Capacidades de búsquedas en la evidencia recolectada.
- Bookmarks.
- Anotaciones y un largo etc.

Las herramientas mencionadas en el último párrafo son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas a su vez vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta en un futuro próximo que éstas estén compitiendo mano a mano con las licenciadas mencionadas anteriormente.

Así mismo se compararon las herramientas utilizadas actualmente para determinar si efectivamente se relacionan con las fases expuestas en el capítulo anterior, esto con el fin de identificar si cumplen o no con uno de los requisitos exigidos para llevar a cabo un análisis forense informático eficiente, veraz y confiable.

De acuerdo con esto, se ha elaborado un cuadro donde se detalla la fase con la que se relaciona la herramienta:

Fase / Herramientas	Identificación de un incidente.	Recopilación de evidencias.	Preservación de la evidencia.	Análisis de la evidencia.	Documentación y Presentación de los Resultados
Encase Forensics Edition	✓	✓	✓	✓	✓
Tool Kit (FTK)	✓	✓	✓	✓	
Nuix Investigator	✓	✓	✓	✓	
Autopsy	✓	✓	✓	✓	✓
Xways	✓	✓		✓	

Figura 13: Relación de las herramientas con las fases de AFI.

Con estas herramientas se expusieron aquellas características y particularidades propias de esta disciplina de la seguridad informática. Nos hemos enfocado desde el punto de vista de una herramienta o programa que es indispensable tenerla en la organización donde se contempla en la política de seguridad y aplicada dentro del proceso de respuesta a incidentes en los sistemas informáticos.

VIII. CONCLUSIONES

En el desarrollo de este trabajo se puede evidenciar la implicación de la identificación, la administración, el análisis, la presentación y el reporte de las evidencias digitales extraídas de los medio tecnológicos intervenidos, así como los retos que deben asumir cada uno de los profesionales dedicados a esta disciplina para combatir la criminalidad en casos que atenten contra a seguridad informática.

Dentro del estudio de la informática forense se busca filtrar datos e información que no sirva para levar a cabo una información veraz y confiable, a cambio se busca recopilar aquella información que aporte lo suficiente para llevar un proceso legal exitoso. Cabe resaltar que la informática forense comprende las acciones, los procedimientos y los conceptos aplicados a situaciones reales que ayudaran a cada uno de los niveles gerenciales de una organización a concientizarse sobre la importancia de llevar un adecuado control y atención a los incidentes informáticos presentados al interior o fuera de ella.

La informática forense es un reto que lleva a que todos los miembros administrativos de una organización se actualicen permanentemente en temas jurídicos, tecnológicos, humanos y organizacionales para contribuir a la seguridad informática y colaborar con la justicia a capturar a quienes ejecuten estas prácticas delictivas.

En cuanto a la utilización de herramientas tecnológicas que sirven de apoyo en el desarrollo del Análisis Forense Informático se puede decir que desde el punto de vista de la situación actual dicha disciplina, se enfatiza una falta de diversidad de criterios tanto a la hora de definir estándares para las herramientas a emplear, como para el proceso de certificación y acreditación de los profesionales del sector. Aunque si se ha encontrado una importante comunidad de desarrollo, tanto por parte de organizaciones como por parte de grupos de software de libre distribución, que están continuamente aportando nuevas herramientas y procedimientos.

Estamos en un mundo que evoluciona constantemente debido a la interconexión a nivel global, lo que permite a los delincuentes sacar provecho de ellos para cometer sus ataques e identificar cualquier vulnerabilidad existente en el sistema y de esta manera sacar provecho de ella. En este sentido es importante revisar los protocolos de seguridad en las organizaciones y contribuir de esta manera a proteger la información relevante para evitar ser vulnerada.

De esta misma manera se hace necesario que los jueces sean capacitados en todos los aspectos técnicos que conllevan al desarrollo del análisis forense informático, para que de esta manera se comprenda un poco más la investigación realizada y puedan dar un fallo a favor de los que han sido afectados por estos ataques. Así mismo los instrumentos utilizados en la extracción y análisis de las evidencias digitales, deben cumplir con todos los protocolos establecidos para su uso, teniendo en cuenta que dichas evidencias pueden ser contaminadas y pueden llegar a afectar los resultados de un caso procesal.

Como estudiantes de Administración de la Seguridad y Salud Ocupacional, debemos conocer todos los aspectos que implica la seguridad informática, debido que es una de las ramas de seguridad que se deben tener en cuenta en cualquier campo y somos nosotros quienes debemos encargarnos de manejar y coordinar las acciones que se deben llevar a cabo en caso de detectar un posible ataque en los sistemas informáticos de la organización, contando con procesos y procedimientos que permitan una actuación proactiva frente a las fallas de continuidad y rechazo del servicio que el sistema pueda presentar en el desarrollo normal de sus funciones.

IX. BIBLIOGRAFÍA

Alejandro Ramos. (2011). Historia de la informática forense. 09 de agosto de 2016, de Security by default Sitio web: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

Ana María Restrepo. (2008). Computación forense, análisis de "cadáveres" virtuales. 29 de agosto de 2016, de DragonJar.com Sitio web: http://www.dragonjar.org/computacion-forense-analisis-de-cadaveres-virtuales.xhtml

Antonio Salmerón. (2015). Concepto de informática forense. 29 de agosto de 2016, de Informática forense y pericial Sitio web: http://forense.info/articulos/conceptosdeinformaticaforense.html

Apoyo para el análisis forense de computadoras, José Arquillo Cruz, Escuela Politécnica Superior de Jaén, Septiembre, 2007

Congreso de Colombia. (2009). Ley 1273 "de la protección de la información y de los datos"

Conpes 3854 (2016). Política Nacional de seguridad Digital. Sitio Web: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Coruniamericana.edu.co, (2016). (Página web) disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/98/93 (Acceso 19 Feb. 2016).

Edgar Calderón Toledo. (2008). Metodología para la forensia informática. 09 de agosto de 2016, de Universidad Autónoma del Estado de Hidalgo Sitio web: http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/319/Metodologia%20para%20la%20forensia%20informatica.pdf?sequence=1

Easey, Eoghan. Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet. Academic Press. p. 840. ISBN 978-0123742681.

Experiencias de análisis forense en México. Departamento de Seguridad en Cómputo / UNAM-CERT en Jornadas de Análisis Forense. Madrid, Septiembre 2005.

Fiscalía General de la Nación de Santander. Estadísticas de la Unidad de Delitos Informáticos del Cuerpo Técnico de Investigaciones de la Fiscalía General de la Nación de Santander. Bucaramanga: CTI. 2014

GITS, C. (2016). Ciberseguridad GITS Informática: Análisis Forense y Peritaje Informático, Privacidad y Delitos Informáticos. (Página web) Gitsinformatica.com. disponible en: http://www.gitsinformatica.com/forense.html (Acceso 14 Feb. 2016).

Gonzalo Piñeros. (2008). los detectives de la era digital. 10 de agosto de 2016, de revista enter.co Sitio web: http://www.enter.co/archivo/los-detectives-de-la-era-digital/

Gutiérrez, Roberto. PÁRRIZAS, Ángel Alonso. Curso de Análisis Forense - TISSAT- 24, 12 Enero 2005.

Harold Emilio Cabrera. (2014). Informática Forense. 28 de agosto de 2016, de Universidad Nacional Abierta y a Distancia Sitio web: http://seginformaticacarolinavillamil.blogspot.com.co/p/delitos-comunes.html

Inteco. (Diciembre de 2013). Identificación y reporte de incidentes de seguridad para operadores. 115, 2, 15.

Interpol Colombia (2008). Informe forense de INTERPOL sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia.

Jeimy J. Cano M.. (2009). Computación forense. México D.F.: Alfaomega.

Jeimy J. Cano M.. (2015). Computación forense 2 edición. México D.F.: Alfaomega.

Julián Correa López. (2011). manual de políticas y estándares en seguridad informática. 17 de junio 2016, de Itenalco Educación Superior Sitio web: http://www.intenalco.edu.co/MP_V01.pdf

José Luis Rivas López. (2009). Que es el análisis forense. En Análisis forense de sistemas informáticos (60). Barcelona: Eureca Media, SL.

Paula Rochina. (2016). Análisis forense informático. Tras la pista del delito. 28 de agosto de 2016, de INESEM Sitio web: http://revistadigital.inesem.es/nuevas-tecnologias/analisis-forense-informatico/

Rivas, L. (2009). (Página web) disponible en: http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf (Acceso 14 de febrero de 2016).

Roberto Hernández Sampieri, Carlos Fernández y Pilar Baptista. (2006). Metodología de la Investigación. México D.F.: Mc Graw Hill.

Seguridad en la red y análisis forense, Hades. Universidad de Murcia – Facultad de Informática. Murcia, España: Administración y seguridad en redes.

Vargas D., José (2010). Proceso de análisis informático forense sobre plataforma linux. Proyecto de Grado Ingeniería de Sistemas, Universidad de Pamplona.

Whos. (05 mayo 2014). Análisis Forense de Memoria RAM (II). 23 de junio 2016, de White Hat and Other Stuff Sitio web: http://wh0s.org/2014/05/05/analisis-forense-de-memoria-ram-ii/