UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster en Seguridad Informática

Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Trabajo Fin de Máster

Presentado por: Arnedo Blanco, Pedro

Director: García Rosado, David

Ciudad: Valledupar

Fecha: Marzo 11 de 2014

RESUMEN

El aumento progresivo de la tecnología, en lo referente a equipos informáticos y de telecomunicaciones con acceso a internet, ha traído como consecuencia que se incremente de manera significativa los incidentes de seguridad informática.

Aquí es donde entra a jugar un papel importante la informática forense, la cual se enfoca en la búsqueda de posibles autores de delitos informáticos.

La informática forense aplica una serie de técnicas y métodos de investigación que permiten reconstruir, lo más fielmente posible, la secuencia de eventos que tuvieron lugar en uno o en varios equipos informáticos, o en toda una plataforma tecnológica, para la ejecución exitosa de un incidente de seguridad informático.

Este trabajo de fin de máster se centraliza en demostrar la efectividad e importancia de reconocidas herramientas de software aplicadas en informática forense en lo referente a su(s) aporte(s) durante una investigación pericial.

Palabras Clave: Seguridad, Informática, Forense, Incidente, Delito.

ABSTRACT

The progressive increase of technology, in terms of computer and telecommunications equipment with internet access, which has resulted in significantly increases in the computer security incidents .

This is where comes to play an important role the computer forensics, which focuses on the search for possible perpetrators of computer crimes.

Computer forensics applies a number of techniques and research methods that allow to reconstruct, as closely as possible, the sequence of events that took place on one or more computers, or throughout a technology platform for the successful implementation of an incident computer security.

This final project work is centered on demonstrating the effectiveness and importance of recognized software tools implemented in computer forensics regarding their contribution during a forensic investigation.

Keywords: Security**,** Informatic, Forensic, Incident, Crime.

INDICE

INTRODUCCION

Es imposible dejar de reconocer la importancia que en la actualidad poseen los sistemas informáticos como motor fundamental en la gestión y procesamiento de la información sostenida en una organización, para el cumplimiento a cabalidad de su lógica de negocio. Y en forma concomitante ha crecido en importancia todo lo relacionado con la seguridad informática para las organizaciones.

Hoy es prácticamente imposible para una organización no estar sistematizada y por ende dejar de preocuparse por la seguridad de sus activos de información, los cuales se ven enfrentados a unas amenazas latentes generadas principalmente por la interconexión de su red interna con redes externas gracias al enlace proporcionado por el proveedor que le da salida a internet. Aunque existen otras amenazas importantes no derivadas por esta condición, como la ingeniería social, de la cual también hablaremos en este trabajo.

Es muy importante tener en cuenta que dependiendo la magnitud de la organización y su importancia en el mercado, así deberá manejar su proceso de gestión de la seguridad tanto de su plataforma tecnológica como de la sus activos de información. Esto se explica en el sentido de que una organización con un reconocimiento ínfimo en el mercado no tendrá el mismo interés de ser atacado en su plataforma tecnológica, que aquella organización con una imagen sólida.

Lastimosamente ningún sistema informático puede ofrecer una seguridad absoluta, siempre existen vulnerabilidades que no se pueden anular y en este caso las organizaciones deben tratar de mitigarlas al máximo. Esto se consigue mediante la implementación de un Sistema de Gestión de Seguridad de la Información.

En atención a lo anterior, los incidentes de seguridad informática en las organizaciones serán noticia permanente, ya que no existe forma de impedir que se den ataques que traten de aprovecharse de las vulnerabilidades que se pueden dar en un sistema informático en busca de un objetivo específico, como puede ser robo de información misional, robo de datos financieros (cuentas bancarias, tarjetas débito / crédito), denegación de servicio, web defacement, satisfacción personal, etc.

Aquí es donde cobra un papel primordial un área de la seguridad informática denominada análisis informático forense, como conjunto de técnicas aplicadas a la resolución de un incidente de seguridad informática.

El análisis informático forense permite, aplicando unas metodologías y unas técnicas en conjunto con una serie de herramientas tanto hardware como software, intentar descubrir inquietudes sobre el incidente tales como: ¿**desde dónde?, ¿qué se atacó?, ¿de qué forma?, ¿quién(es) atacó(aron)? y ¿en qué periodo de tiempo?** se dieron los hechos.

Motivación y Enfoque

El análisis informático forense es un área de la seguridad informática que evoluciona en forma constante con los avances tecnológicos y en paralelo con el perfeccionamiento de los ataques informáticos. Es un área que se apoya sustancialmente en el software para el cumplimiento de sus objetivos, para lo cual existe una amplia gama de aplicativos que permiten investigar un incidente desde muchas perspectivas. Estos aplicativos, al igual que la rama de la informática que soportan, siguen evolucionando al paso de la tecnología para lograr los mejores resultados.

Una de las circunstancias que hace al análisis forense informático tan atractivo, es porque le permite al investigador encontrar siempre las herramientas de software idóneas frente a lo que esté investigando. Claro que esto se debe combinar con aspectos importantes como los son la experiencia y la proactividad del investigador.

A través del presente trabajo se tratará de presentar de la forma más objetiva, clara, detallada y profesional, la efectividad y aplicabilidad de algunas de las herramientas de software más representativas del mercado encaminadas a la investigación informática forense.

Propósito

El propósito de este trabajo es servir como marco de referencia para estudiantes, docentes e investigadores de la informática forense en sus procesos de peritaje y enseñanza,

demostrando mediante pruebas simuladas y el acompañamiento de imágenes y gráficos detallados, la efectividad y aplicabilidad de herramientas de software según la función que desarrolla cada una de ellas.

Alcance

El alcance de este trabajo a nivel académico es muy amplio, ya que abarca a estudiantes, docentes e investigadores, esparcidos en todo el planeta a donde ha llegado la tecnología y las telecomunicaciones, lógicamente Internet, y por ende la amenaza real de ataques informáticos.

Estructura del trabajo

Este trabajo se estructura de la siguiente manera:

En el capítulo 1 se presenta el Estado del Arte en lo que corresponde al tema escogido. En este capítulo se hace referencia a definiciones, conceptos y literatura base existente para el entendimiento de los temas posteriores.

En el capítulo 2 se presenta en una forma clara y detallada las metodologías existentes a seguir para un análisis informático forense y cada una de las fases que las componen. Estas metodologías permiten alcanzar el objetivo principal frente a un incidente: descubrir la verdad de lo sucedido.

En el capítulo 3 se presentan simulaciones prácticas en cuanto a la aplicabilidad y al uso de herramientas de auditoría informática forense en incidentes de seguridad informática simulados, como aporte descriptivo para la asimilación de los conceptos plasmados en este documento.

En la última parte de este trabajo de fin de máster se presentan las conclusiones finales a que se dio lugar con relación a la temática tratada en el desarrollo del mismo acompañado de la bibliografía y cibergrafía consultada para ello.

OBJETIVO GENERAL

Analizar la aplicabilidad y funcionalidad de distintos programas informáticos forenses como herramientas imprescindibles para la investigación de un delito informático.

Objetivos Específicos

- Identificar herramientas informáticas de gran valor para la investigación forense.
- Demostrar la funcionalidad de algunas herramientas informáticas durante la investigación forense.
- Desglosar las etapas que se dan en una investigación de informática forense.
- Incentivar a la comunidad a aprender como mínimo lo básico en cuanto a normas, técnicas y software, que le permitan defenderse al máximo de la ciberdelincuencia actual.

1. ESTADO DEL ARTE

1.1. **Conceptualización.**

1.1.1. Informática.

El diccionario de la Real Academia de la Lengua Española (2001), presenta la siguiente definición: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”.

La palabra Informática tiene su origen en Francia, procede de la palabra francesa **informatique**, formada por la conjunción de las palabras "information" y "automatique". La historia nos dice que esta palabra fue utilizada por primera vez por el ingeniero Philippe Dreyfus en el año 1962.

Una definición más acorde con lo que esta palabra representa en la actualidad sería decir que la informática es la ciencia que estudia el tratamiento automático y racional de la información en equipos de cómputo, equipos electrónicos y sistemas de información, la cual se basa en múltiples ciencias como la física, la matemática, la electrónica, entre otras.

- Historia y Evolución: La informática nació para hacerle las cosas más fáciles al hombre, ya que gracias a ella podemos realizar procedimientos complejos con gran exactitud, minimizando la probabilidad del error y con una rapidez imposible de alcanzar de forma manual o mecánica. Desde sus inicios ha ido evolucionando en forma progresiva y sin latencia. Podemos señalar como un momento fundamental en el desarrollo de la informática el momento en que IBM mostró en sociedad el primer computador personal, con un procesador Intel 8088 y software desarrollado por Bill Gates y Paul Allen, específicamente sistema operativo D.O.S y lenguaje de desarrollo BASIC.

Luego llego ARPANET, la cual derivó en Internet y en 1990 aparecería la World Wide Web. En 1996 nace la segunda versión de Internet, más rápida, con más capacidad de carga y transporte de archivos, luego llegaría la conexión por modem, por microondas y actualmente por fibra óptica y vía satélite.

Actualmente la informática está involucrada en casi todos los procesos humanos de la vida cotidiana, llámese familiar, social, laboral, intelectual, etc., a tal punto que no se concibe la creación de un negocio o microempresa sin el acompañamiento de una plataforma informática.

En lo que tiene que ver con la vida académica podemos decir que la informática es prácticamente un aspecto inalienable a ella, desde la educación básica hasta la doctoral, donde el computador y el internet se han convertido en algo imprescindible para cualquier estudiante.

1.1.2. Delito.

La enciclopedia en línea Wikipedia, presenta la siguiente definición: “El delito es definido como una acción típica, anti jurídica, imputable, culpable, sometida a una sanción penal, y a veces a condiciones objetivas de punibilidad. Supone una conducta infraccional del derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley.

- Historia y Evolución: El delito desde sus inicios se concibe como aquel acto indebido que es realizado por una o varias personas en perjuicio de alguien, ya sea persona natural o jurídica y que está en contra de lo permitido por la ética y la moral. Antes de la llegada de los computadores a la industria y al hogar los delincuentes debían estar cerca a la víctima para cometer el acto ilegal. Hoy en día el delito va más allá, hasta el punto de involucrar actores en

puntos equidistantes al momento de cometer el delito, los cuales pueden gracias a la tecnología, actuar en conjunto para lograr el cometido.

1.1.3. Delito Informático.

La enciclopedia en línea Wikipedia, presenta la siguiente definición: “Un delito informático o ciberdelicuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.”.

También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley y utiliza medios tecnológicos para su consecución y que están encaminados a atacar la integridad, confidencialidad y disponibilidad de los activos de información en un sistema informático.

- Historia y Evolución: Podemos decir que el primer tipo de delito informático que se dio fue el de robo de información en un computador, por rompimiento de contraseña. Hoy en día los delitos han evolucionado hasta tal punto que actualmente existe toda una ramificación de tipos y subtipos.

  Entre algunos delitos informáticos encontramos:

  - Fraude informático: es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio, casi siempre económico, utilizando medios informáticos.

  - Contenido obsceno u ofensivo: Cuando se envían mensajes a través de internet con contenido que atenta contra la integridad de una o más personas u organizaciones (por medio de redes sociales, emails, etc.).

  - Hostigamiento / acoso: Delito que se concreta cuando se contacta a una persona para que realice o entregue algo bajo una situación de amenaza.

- Terrorismo Virtual: Se da cuando se ataca una organización o estado para hacer daño a su sistema de información (ataques 0-days, denegación de servicio, acceso no autorizado, etc.).

- Pornografía Infantil: Delito que se comete cuando se envían archivos de imágenes o video por la web con contenido sexual explicito con menores de edad.

- Propiedad Intelectual: Delito que se comete en el momento que se accede a información privada o confidencial sin la autorización expresa de su autor, ya sea para su difusión gratuita o comercialización.

1.1.4. Vulnerabilidad Informática.

La enciclopedia en línea Wikipedia, presenta la siguiente definición: "Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo."

Una vulnerabilidad informática se refiere a una debilidad presente en un software, la cual puede ser explotada por un atacante permitiéndole violar la confidencialidad, integridad, disponibilidad, control de acceso y fiabilidad del sistema donde se encuentra implementado y/o sus datos.

- Características: Es común descubrir vulnerabilidades constantemente en variados programas de computador y su rápida propagación por internet, inclusive mucho antes de que se descubra la solución o se publique la misma.

  Podemos mencionar como vulnerabilidades comunes:

  - Buffer overflow o desbordamiento de pila: Es un fallo de software debido a una mala programación que se ve reflejado durante la ejecución de un programa, el cual no logra controlar de forma adecuada la cantidad de datos que se deben copiar en el área de memoria reservada para el

buffer, permitiendo que este espacio se supere, sobrescribiendo espacios de memorias continuas a éste incluyendo el contenido de la misma.

- Inyección SQL: Es un método que se aprovecha de un fallo de programación, específicamente en la validación de entrada de datos en una consulta SQL. Este método se aprovecha de una vulnerabilidad en la validación de entrada durante la construcción de una Sentencia SQL que se va a ejecutar frente una Base de Datos, permitiendo alterar la consulta de tal forma que el atacante puede obtener datos valiosos de los registros almacenados en las diferentes tablas existentes en la base de datos atacada, como de su estructura e inclusive de los usuarios administradores de la misma, permitiéndole escalar privilegios en el sistema.

- Secuestro de sesiones: Primero definamos cookie, el cual es archivo generado al iniciar sesión en un sitio web y que idéntica de forma unívoca a la dualidad que se da entre la cuenta de usuario y el servicio web enlazado. Entonces un secuestro de sesión es un método de ataque informático en el cual se captura la cookie activa de un usuario en la red, lo cual permitirá al atacante acceder al servicio web enlazado a esa cookie sin pasar por las medidas de autenticación requeridas. De esta manera el atacante puede actuar de la misma forma que el usuario titular frente al servicio web enlazado con la cookie secuestrada.

- Ejecución de código remoto: Método que consiste en aprovechar una vulnerabilidad que permite tomar privilegios sobre una máquina remota y ejecutar código en ella, lo cual le daría la potestad al atacante de alterar, borrar o consultar información no autorizada e inclusive escalar privilegios en la maquina atacada.

    - XSS (Cross-Site Scripting): En español, Secuencias de Comandos en Sitios Cruzados. Vulnerabilidad común en las aplicaciones Web, que le brinda la oportunidad a un atacante inyectar en una página web código escrito en lenguajes tipo script como Javascript o VBScript, lo cual le permitiría esquivar

los controles establecidos dentro de las políticas de seguridad del sistema de información atacado.

1.1.5. Amenaza Informática.

Una amenaza informática es la probabilidad de ocurrencia de cualquier tipo de evento o acción que tenga la capacidad de ocasionar daño a los elementos de un sistema informático, tanto a nivel de software como de hardware.

1.1.6. Ataque o Incidente de Seguridad Informática.

Se puede definir como el intento de violación o la violación efectiva (penetración) a la seguridad de un sistema informático con fines delictivos.

Fases de un Ataque o Incidente de Seguridad Informática:

- Descubrimiento o Identificación: Esta fase trae consigo la adquisición de datos relacionados con una posible víctima, la cual puede ser una persona o una entidad. Esta fase se puede comparar con los conocidos test de penetración realizados por hackers éticos. También se le conoce en el idioma inglés como “Information Gathering”.

  En esta fase se utilizan herramientas que analizan el tráfico de la red de datos, conocidas como sniffers (término en idioma inglés), además se complementa con técnicas de ingeniería social y con la ayuda de buscadores como shodan, google y bing. Además los buscadores google y bing ofrecen una metodología de búsqueda y filtrado en la web por medio de comandos conocidos como “DORKS”, muy efectivos a la hora de encontrar información oculta en la web. De esta forma se estarían garantizando resultados valiosos y positivos para el ataque.

  En síntesis, el delincuente en esta fase se dedica investigar en profundidad sobre la plataforma tecnológica que va a atacar, utilizando para ello técnicas

pasivas de levantamiento de información, tratando de encontrar la mayor cantidad de información pública sobre la misma. Entre la información a encontrar podemos mencionar:

- Dirección física de la entidad.
- Direcciones IP y Rangos.
- Direcciones IP de servicios contratados.
- Correos electrónicos.
- Nombres de empleados.
- Números telefónicos
- Detección de redes WiFi.
- Análisis de vulnerabilidades al portal WEB.

- Exploración: En esta fase y con base en la información obtenida en la fase anterior, se busca profundizar en el sistema a violentar, obteniendo información como dirección o direcciones de red, rango y subrangos de red, nombres de equipos, datos de autenticación, sistemas operativos implementados, servidores web utilizados, etc.

  En esta fase se suelen utilizar herramientas informáticas tales como escáner de vulnerabilidades, escáner de red, escáner de puertos, mapeadores de red y de puertos, analizadores de protocolos, detección remota de servicios, detección remota de equipos activos y sistemas operativos, identificación de software y versiones, análisis de banners y búsqueda de aplicaciones web. Además de análisis de la configuración en las redes WiFi.

En otras palabras se usan técnicas no intrusivas que permiten descubrir todas las vulnerabilidades potenciales a explotar durante el ataque.

- Evaluación: Luego de encontrar las vulnerabilidades que nos permitirán violar el sistema, estas comienzan a explotarse mediante las técnicas directamente relacionadas con ellas, tales como ataques de denegación de servicios, ataques de desbordamiento de buffers, filtrado de contraseñas, etc. En esta fase se dan las siguientes tareas:

  - Escaneo Automatizado de Vulnerabilidades. Mediante herramientas sistematizadas que permiten:

    - Detectar vulnerabilidades en los Sistemas Operativos y en los demás servicios que se estén ejecutando.

      Generar reportes con información técnica relevante de seguridad.

    - Permitir, si es posible, explotar toda vulnerabilidad detectada.

  - Escaneo Manual de Vulnerabilidades. Este se realiza a través de sitios web con información sobre vulnerabilidades reportadas. Para ello se verifica la existencia de vulnerabilidades que afecten a las versiones del software instalado. Algunos de estos sitios web poseen bases de datos con exploits públicos, los cuales pueden ser de utilidad para el ataque.

- Intrusión: Esta fase, considerada como la más compleja en un ataque informático, se caracteriza por darle utilidad a todo lo detectado y recabado en etapas previas, tratando de encontrar las herramientas adecuadas que permitan realizar la intrusión y obtener el control del sistema mediante el escalamiento de privilegios (proceso por el cual se obtienen niveles de acceso superior en una plataforma especifica).

Casi siempre este proceso no se realiza en forma inmediata y a menudo requiere la explotación en conjunto de dos o más vulnerabilidades para hacerse efectivo.

En esta fase el atacante se asegura de implantar en el sistema atacado herramientas que permanezcan lo más indetectable posible y que le permitan volver a penetrar el sistema en un futuro desde cualquier lugar donde exista conexión a internet. Estas herramientas (o mejor, Malware) suelen ser del tipo:

- Troyanos: Es un malware que se muestra como un software autentico y luego de alojado en un equipo permite al atacante tomar el control del mismo.

- Rootkits: Malware que se compone de varios elementos que otorgan a un atacante el acceso al sistema víctima.

- Backdoors: Líneas de código dentro de un programa de forma intencional, el cual está destinado para controlar remotamente el equipo víctima.

Uno de los pasos finales de todo atacante informático es el de eliminar cualquier evidencia o rastro que lo pueda incriminar con el delito informático cometido y más aún que le permita al responsable de la seguridad informática y/o de la información de la empresa detectar su presencia en tiempo real. Para lo cual se vale de herramientas que borran esas evidencias, como pueden ser herramientas para borrado de logs y de alarmas generadas por los IDS instalados.

1.1.7. Evidencia Digital.

"Información de valor probatorio almacenada o transmitida en forma digital" (Cano, 2005, p.186). En otras palabras la podemos definir como las pruebas

digitales encontradas en una escena de un delito que pueden servir en un proceso judicial como evidencia probatoria.

La evidencia digital se puede dividir en tres categorías:

- Registros almacenados en un equipo informático: Correos electrónicos, imágenes, documentos ofimáticos, etc.

- Registros generados por un equipo informático: Logs de Eventos, logs de errores, logs de transacciones, etc.

- Registros parcialmente generados y almacenados en un equipo informático: por ejemplo aquellos archivos generados temporalmente por el navegador de internet mientras consultamos el ciberespacio o aquellos archivos generados cuando se ejecuta un procedimiento por lotes o un procedimiento almacenado en una base de datos.

Se tiene que anotar que una evidencia digital es anónima, duplicable, alterable y eliminable.

1.1.8. Auditoria.

Naranjo, Alice (2009) afirma: “La palabra auditoría viene del latín auditorius y de esta proviene la palabra auditor, que en español significa aquel que tiene la virtud de oír y revisar cuentas. La auditoría debe estar encaminada a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando el área analizada, para que por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien, mejorar la forma de actuación.” (p. 3)

También se puede definir al término auditoria como la evaluación desarrollada por un grupo de profesionales a una entidad, del orden público o privado, con el fin de detectar fallas y hacer las respectivas sugerencias para subsanarlas.

- Historia: La auditoría es tan antigua como lo es la aparición del hombre sobre la tierra. En sus inicios esta se desarrollaba de manera empírica. En la época de la conquista estaban los “oidores” de la corona, que en el fondo eran auditores, ya que vigilaban el pago de tributos a la corona española.

  En la era moderna la auditoria se implementa en cualquier empresa o entidad para encontrar falencias misionales y posteriormente proseguir con implementar el correctivo necesario.

- Aplicabilidad: La aplicabilidad de un proceso de Auditoria abarca un rango amplio de entidades, de procesos, de procedimientos y de ejecuciones. Se aplica a cualquier entidad o empresa que desee detectar falencias en su lógica de negocio para su posterior corrección o como mínimo alcanzar su mayor mitigación.

1.1.9. Seguridad.

En la enciclopedia en línea Wikipedia se encuentra la siguiente definición: El término seguridad proviene del latín “securitas”. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien.

1.1.10. Seguridad de la Información.

Según Álvarez Gonzalo (2004), “La seguridad de la información es una disciplina que se ocupa de gestionar el riesgo dentro de los sistemas informáticos” (p. 3).

En síntesis se puede decir que al hablar de seguridad de la información nos referimos a todas las metodologías implementadas como medidas de seguridad en un sistema informático, que permitan contrarrestar las amenazas a las que están expuestos sus activos de información o a mitigar el impacto de las mismas.

1.1.11. Seguridad Informática

En la enciclopedia en línea Wikipedia está definida como: “La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.”

También en Wikipedia se define como: “La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable”.

Se puede decir que se empieza a hablar de Seguridad Informática a partir del momento en que nace el primer computador, conocido como ENIAC, equipo que se manejaba con tarjetas perforadas, las que debían mantenerse seguras, alejadas de personal no autorizado. Allí ya se aplicaba la seguridad informática.

1.1.12. Auditoria Informática.

Rivas Gonzalo Alonso (1989) la define así: “…es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que serán auditados.” (p. 39-40).

1.1.13. Análisis Forense

Se puede definir como la metodología científica que se aplica al estudiar un delito para recabar pistas que permitan encontrar o descifrar quien lo cometió, que utilizó para su cometido y como se llevó a cabo.

1.1.14. Informática Forense

En la enciclopedia en línea Wikipedia está definida como: "…es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal."

- Historia La historia nos dice que la informática forense tiene su origen en los Estados Unidos en los años 90, en atención de las necesidades por parte del FBI de peritos en delitos informáticos. Esta necesidad se generaba de las actuaciones procesales en actividades probatorias donde estaban involucradas evidencias tecnológicas o en la recolección de estas evidencias en una escena del crimen, en donde las pruebas o evidencias digitales en un proceso legal tenían el potencial de convertirse en un elemento probatorio tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN.

  A finales de los años 90 se creó la IOCE (International Organization of Computer Evidence) cuya finalidad principal es compartir información sobre las prácticas de informática forense alrededor del mundo.

  A raíz de esto nace como tal la labor del perito informático o informático forense, cuyo objetivo principal es encontrar pruebas en un delito informático que le permita identificar de forma tácita y real el origen y la forma como se llegó a la consecución del mismo.
  .

- Objetivos: La informática forense persigue tres objetivos puntuales, basados en la recolección de evidencias:

  - Búsqueda y llevada a juicio de los ciberdelincuentes.

  - El resarcimiento de todos los delitos cometidos

- Identificación de la vulnerabilidad y establecimiento de los controles pertinentes para su mitigación.

- Importancia: La Informática Forense es una disciplina criminalística que se enfoca en investigar hechos delictivos en los que están involucrados sistemas informáticos y con base en esa investigación hallar pruebas o evidencias que tengan la suficiencia jurídica necesaria para poder ser presentada como prueba válida ante un ente judicial.

  Para esto la Informática Forense desarrolla y perfecciona técnicas que permiten encontrar, analizar, salvaguardar y documentar hallazgos o evidencias tecnológicas frente a instancias legales.

- Aplicabilidad: La Informática Forense es una disciplina criminalística que se puede aplicar en las siguientes áreas:

  - Investigación Científica: En la actualidad entidades de educación superior se valen de la informática forense para el estudio y análisis de amenazas y vulnerabilidades informáticas y su posible solución o mitigación al máximo grado posible.

  - Investigación Criminal: La informática forense es aplicada como ayuda para solucionar delitos con variadas tipificaciones: Financieros, Narcotráfico, Pornografía Infantil, Trata de Blancas, Grupos Extremistas, Homicidios, etc.

  - Proceso Judicial: La informática forense es aplicada como ayuda para solucionar procesos judiciales relacionados con Estafas, Fraudes, Acosos, Espionaje, Robo de Información, etc.

  - Hogar: Existen múltiples aplicativos con tecnología forense que un usuario normal puede utilizar con finalidad particular, como recuperar archivos borrados accidentalmente, entre otros.

1.1.15. Tipos de Análisis Informático Forense.

- Análisis Forense de Redes: Mediante el cual se analiza en investiga un delito informático en el cual se ve involucrada una red de computadores.

- Análisis Forense en Sistemas Embebidos: Mediante el cual se analizan dispositivos electrónicos como tablets, smartphones, etc., que estén involucrados en un delito informático.

- Análisis Forense de Sistemas: Mediante el cual se analizan computadores tipo servidores o de escritorio, los cuales hayan sido protagonistas para un delito informático, ya sea como medio para lograrlo o como objetivo final del mismo.

1.1.16. Herramientas Informáticas como medio delictivo.

El avance desenfrenado de los equipos informáticos y las telecomunicaciones ha traído como consecuencia el aumento exponencial de la delincuencia informática, esto por ende se ha visto reflejado en el desarrollo de nuevas herramientas tanto a nivel de software como de hardware para la protección de los activos de información de una organización. Me centraré en este trabajo en lo concerniente a herramientas de software como apoyo en el proceso de análisis forense informático.

1.1.17. Principios de la Informática Forense.

- Organización y documentación detallada: El investigador forense debe ser una persona plenamente organizada en su trabajo investigativo, debe dejar trazabilidad de cada uno de los pasos que desarrolló durante el mismo, de las herramientas informáticas que utilizó durante la investigación. Además debe brindar un reporte del análisis de las evidencias encontradas bien detallado y soportado con toda la documentación pertinente para la misma,

para que al momento de ser consultado por cualquier persona, ésta entienda y valide lo que está leyendo sin problema alguno. Esto permite al investigador tener tranquilidad sobre la veracidad e integridad de su trabajo, y en el eventual caso de que se realicé por otras personas una investigación adicional sobre la misma evidencia, que los resultados sean iguales y se pueda salir avante frente a una comparación de los mismos.

- Integridad de la evidencia: El investigador forense debe garantizar que las evidencias digitales obtenidas y las copias de éstas no se puedan alterar o modificar en ninguno de las fases de la investigación forense hasta su entrega a la instancia judicial competente y la emisión de los informes respectivos. Para lo cual se debe implementar la cadena de custodia tal cual como lo dictan las normas estandarizadas y las buenas prácticas reconocidas para este proceso.

- Validar el proceso de custodia. Todo proceso de custodia debe cumplir con ciertos lineamientos preestablecidos en lo concerniente al diligenciamiento de información mediante el cual se le da soporte y trazabilidad a todos los procesos que se dieron durante ese proceso de custodia. Esto con todo el rigor y la importancia que el tema merece.

1.1.18. Pruebas básicas a identificar según el tipo de delito informático

A continuación se enumeran una serie de pruebas basadas en buenas prácticas, en lo que corresponde al análisis informático forense, dependiendo del tipo de delito informático investigado.

- Investigaciones de Fraude Financiero: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con las cuentas utilizadas en portales dedicados a subastas online, software contable u hojas de cálculo con información contable, agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), información de tarjetas bancarias (débito o crédito), información financiera de bienes, datos de clientes y software de edición de imágenes.

- Investigaciones relacionadas con la pedofilia, pornografía y abuso Infantil: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con: agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.

- Investigaciones relacionadas con la penetración ilegal a una red de cómputo y fraudes en telecomunicaciones. En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones y nombres de usuarios, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.

- Investigación de Homicidios: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con las cuentas utilizadas en portales dedicados a subastas online, software contable u hojas de cálculo con información contable, agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), información de tarjetas bancarias (débito o crédito), información financiera de bienes, documentos legales de propiedad de bienes (escrituras, testamentos, etc.),datos de clientes y software de edición de imágenes, historia médica, imágenes y violencia intrafamiliar.

- Investigaciones relacionados con el narcotráfico: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.

- Investigaciones relacionadas con los derechos de autor: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones y nombres de usuarios,

conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.

1.1.19. Tipos de Herramientas de Software Aplicadas en el Análisis Informático Forense.

Existen múltiples herramientas de software que tienen como marco de acción el análisis forense informático, las cuales permiten encontrar pistas, descubrir detalles, que sirven como medio de prueba para el descubrimiento de los objetivos a cubrir por un análisis informático forense:

- Herramientas de red: Existen múltiples variedades de herramientas de red, entre los más comunes tenemos a los capturadores de tráfico, que permiten la captura de los paquetes de datos que se transmiten y reciben por equipos informáticos en una red local; están los sistemas de detección de intrusos (o IDS abreviatura de sus definición en inglés Intrusion Detection System) que son aplicativos que permiten detectar cualquier acceso no autorizado a un solo computador o a una red de computadores.

  Se conocen dos tipos de Sistemas de Detección de Intrusos:

  - HIDS (HostIDS): Un IDS para Hosts. Este permite detectar en el equipo donde se encuentra instalado rastros de las actividades de los intrusos.

  - NIDS (NetworkIDS): un IDS basado en red. Este permite detectar en todo el segmento de la red donde se encuentre instalado, el rastro dejado por los intrusos, para lo cual la interfaz debe funcionar en modo promiscuo, lo cual le permitirá capturar la totalidad del tráfico de la red.

    Este tipo de software está basado en un análisis exhaustivo de la información que circula en la red donde se encuentran instalados.

Información que es confrontada frente a firmas de ataques reconocidos almacenados en una base de datos propia del IDS.

- Herramientas de encriptación: Mediante este tipo de software se cifran archivos o documentos utilizando un algoritmo específico. Este tipo de software se usa para proporcionar un nivel de seguridad fuerte en lo concerniente a la accesibilidad de archivos privados o confidenciales.

- Editores Hexadecimales: Un editor hexadecimal, también llamado editor de archivos binarios, es un tipo de software que permite leer y modificar el contenido de archivos binarios. También se les conoce como “editores de sectores” porque pueden leer datos almacenados en sectores específicos en una unidad de almacenamiento magnético y modificarlos de igual forma que si estuvieran modificando un archivo binario.

  Por medio de este tipo de software se puede editar el contenido de cualquier archivo binario, lo cual permite entre otras cosas analizar si existe algún tipo de malware embebido en un archivo binario o alguna función maliciosa.

- Herramientas de virtualización: Son programas que permiten transportar una infraestructura física de un equipo informático (incluyendo su software) a una plataforma de software que simula la totalidad de los componentes de su arquitectura.

  Mediante este tipo de software se puede instalar en un sistema real, un sistema virtualizado que simula el funcionamiento de un equipo informático sin afectar la configuración de su huésped pero si aprovechando sus recursos físicos (disco duro, memoria RAM, etc.), permitiendo en este sistema virtualizado instalar y verificar cualquier software sin comprometer nuestro sistema real..

- Emuladores: Tipo de software que permite ejecutar software (programas o videojuegos) en una plataforma diferente para el que fue desarrollado, tanto a nivel de hardware como de sistema operativo.

Mediante un emulador se imita de la forma más fiel posible un dispositivo y su plataforma de tal manera que funcione como si se tratara del dispositivo original.

- Herramientas de borrado de archivos: Son programas que permiten borrar archivos en un dispositivo de almacenamiento de manera segura, de tal forma que no se pueda recuperar el archivo borrado mediante un programa especializado en recuperación de archivos. Para ello utiliza una serie de algoritmos de borrado que permiten que el archivo sobre el que se aplique su funcionalidad quede irrecuperable.

  Este tipo de software se suele utilizar en la medida que necesitamos eliminar documentación confidencial de un dispositivo de almacenamiento, al cual puede tener acceso personal sin la autorización pertinente para su lectura.

- Herramientas de recuperación de Contraseñas: Herramientas que permiten recuperar contraseñas usadas en el sistema operativo investigado.

- Herramientas de recuperación de datos o archivos: Son programas que permiten recuperar archivos borrados previamente. Utilizan varios formas de recuperación como recuperación en bruto (cuando ha sido formateado el dispositivo de almacenamiento), recuperación rápida (cuando ha sido borrado el archivo recientemente), entre otros.

  Este tipo de software se suele utilizar en la medida que necesitamos recuperar documentación borrada de un dispositivo de almacenamiento, ya sea de forma intencional o no.

- Herramientas de investigación y análisis: Son aplicativos orientados a la investigación y análisis forense. Entre otras funcionalidades ofrecen recolección de evidencia digital, realización de análisis de la evidencia digital recolectada e informe detallado del mismo.

Son aplicativos que tienen una gran importancia en la investigación informática forense, por la cantidad de funcionalidades que ofrece en la consecución y análisis de evidencias digitales.

- Herramientas de análisis de discos (Montaje y Recuperación): Software que permite montar imágenes de discos, producto de copias a la evidencia original, para su análisis especializado y determinar si la imagen está afectada en su integridad.

- Clonación: Software especializado en copiar bit a bit la información contenida en una unidad de almacenamiento lógico (disco duro, pendrive, etc.) y volcar esta información en otro dispositivo de igual o mayor capacidad; también permite volcar esta información en un archivo digital que se puede tratar mediante software especializado como si fuese la unidad de almacenamiento lógica original.

  Este tipo de software es de gran importancia al momento de tratar una o más unidades de almacenamiento lógicas como evidencia en un delito informático, ya que permite clonarlos para realizar los análisis sobre las copias y de esta forma preservar la evidencia original.

- Herramientas de adquisición y análisis de memoria: Herramientas de software que permite tener acceso a la memoria RAM de un equipo, adquirirla y exportarla a un archivo para su análisis posterior.

- Distribución LiveCD de Linux: Es un tipo de distribución Linux que no requiere instalarse en el computador, ya que se puede ejecutar directamente desde un pendrive o un dvd.

1.1.20. Herramientas de Informática Forense.

- Herramientas de red:

- TCPDump: Es un software analizador de trafico de paquetes de red, funciona a nivel de línea de comandos. Esta herramienta permite analizar el funcionamiento de aplicaciones, detectar problemas en la red o capturar datos que se transmiten por la red y se encuentre sin encriptación alguna (Figura 1). Hay una versión similar para entorno Windows llamada Windump (Figura 2).

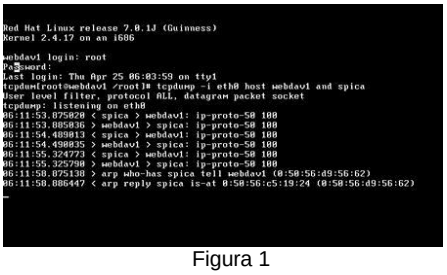


Figura 1

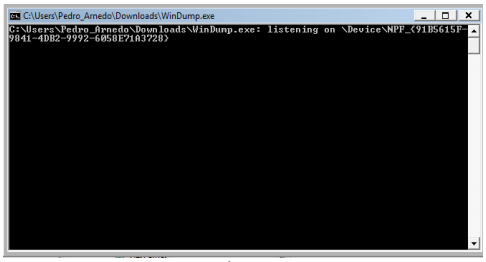
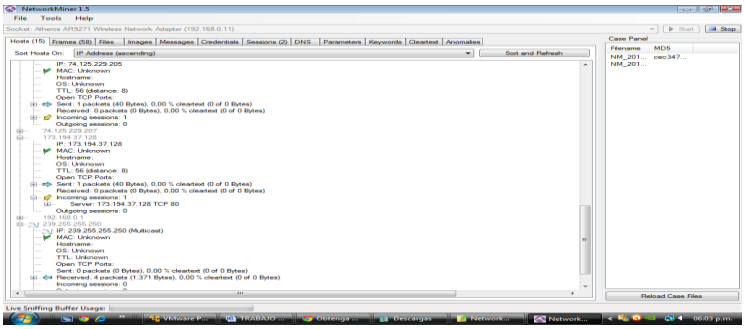


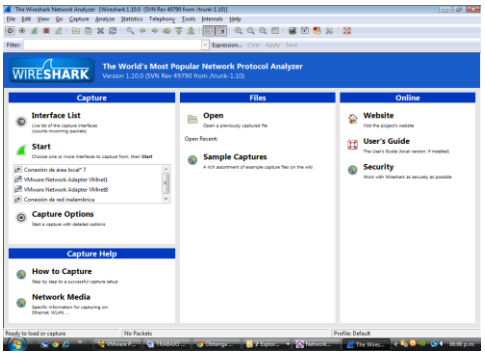
Figura 2

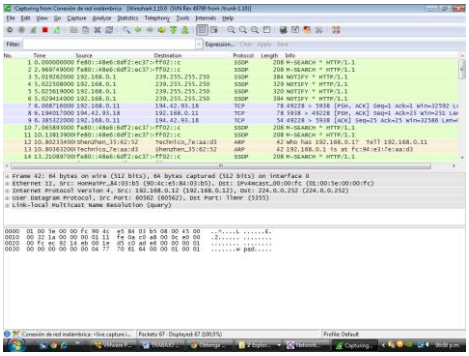
- NetworkMiner: Herramienta que permite capturar información de red. Permite analizarla aplicando filtros de búsqueda de datos.



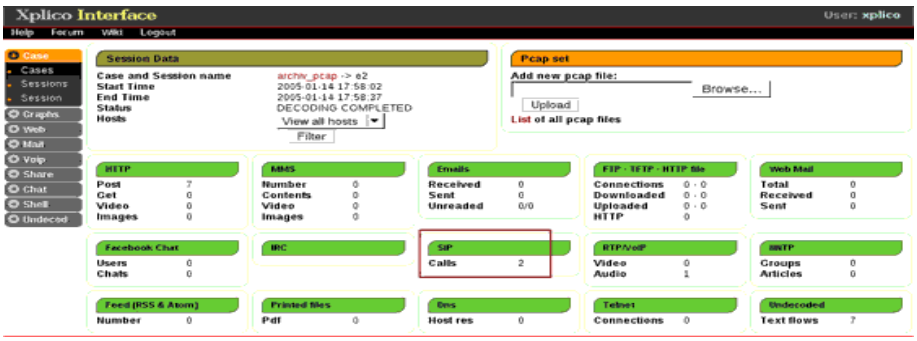
- Network Appliance Forensic Toolkit: Paquete de herramientas forenses desarrolladas en lenguaje Python, que se especializan en la captura de tráfico en la red y análisis del mismo.

- WireShark: Es un software que permite capturar tramas y paquetes que circulan a través de una interfaz de red. Este aplicativo posee todas las características mínimas requeridas por un analizador de protocolos.





- Xplico: Software que permite capturar el tráfico de la red, con la particularidad que permite extraer los datos transmitidos mediante el protocolo HTTP y los mensajes de correos electrónicos que tienen implementado los protocolos POP y SMTP.



- Splunk: Software que funciona en los sistemas operacionales más importantes del mercado, permite monitorear y analizar el tráfico de la red, detectando entre otros aspectos transacciones, registros de llamadas y lugares de navegación de los usuarios. Cuenta con un módulo de firmado de datos, que permite generar una prueba de autenticidad en cualquier proceso de análisis forense o auditor.

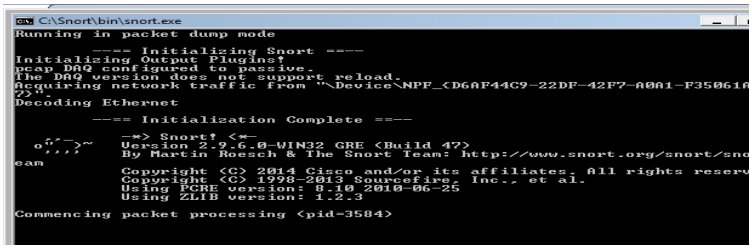
- Snort.: Es un software libre y de código abierto que funciona como un sistema de prevención de intrusiones de red (NIPS) y sistema de detección de intrusiones de red (NIDS). Este software tiene la capacidad de realizar un análisis de tráfico en tiempo real y registro de paquetes generados por el protocolo IP, lo cual deja plasmado en una bitácora o archivo tipo log, para su análisis posterior.

  Snort puede ser configurado en tres modos principales:

  - Rastreador: se comporta como un registrador de paquetes y de detección de intrusiones en la red;

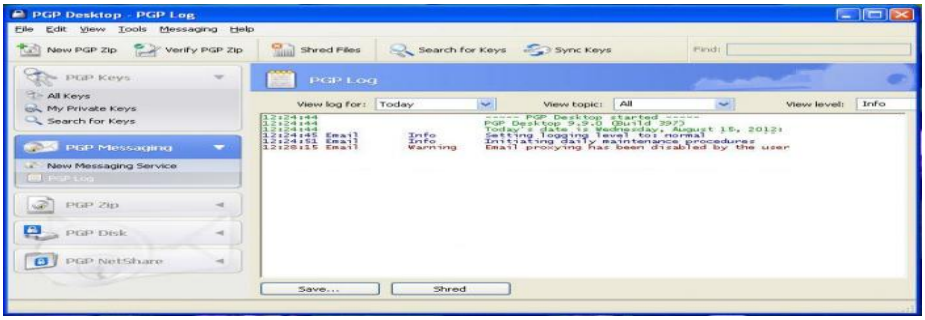
  - Sniffer, en este modo el software lee los paquetes de red, los muestra en la consola y los registra en el disco

  - Detección de intrusos: en este modo el software rastrea el tráfico de red y lo analiza frente a un conjunto de reglas definidas por el usuario, de acuerdo a lo obtenido de este análisis ejecutará la acción adecuada para su mitigación o corrección.

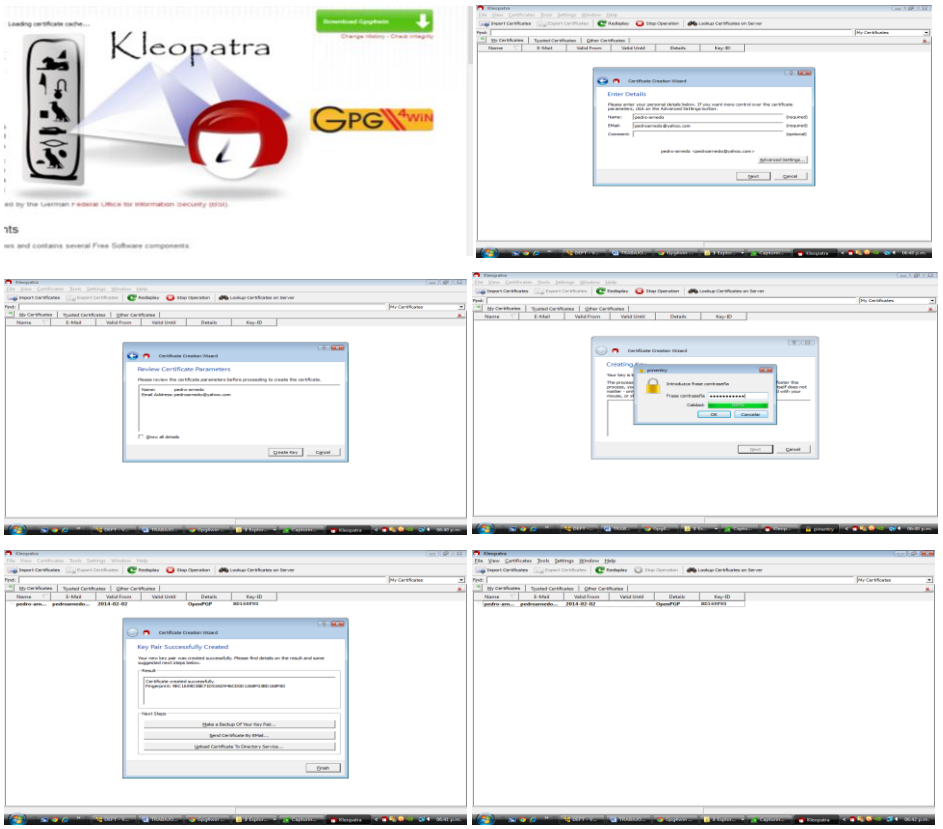


- Cifrado.

  - PGP: Aplicativo desarrollado por Phil Zimmermann, el cual tiene como funcionalidad principal la de proteger archivos de datos mediante el uso de criptografía de clave pública y además ofrece la facilidad de autenticación de documentos a través de firmas digitales.



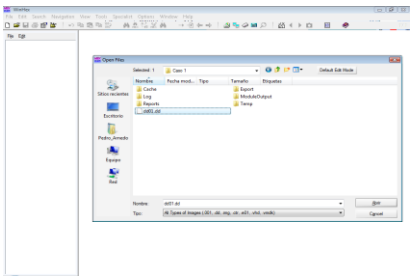
- GNG4Win: Aplicativo que sirve para encriptar datos mediante un sistema de clave pública bajo Windows.

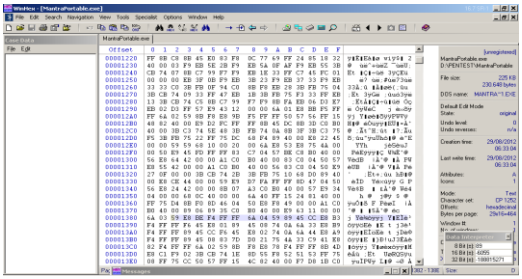


- Editores.

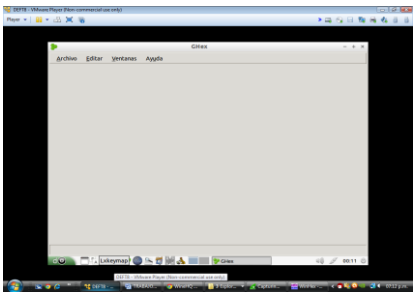
- WinHEX: Es un editor hexadecimal que permite editar todos los tipos de archivos, dispositivos de almacenamiento y memorias RAM. Además

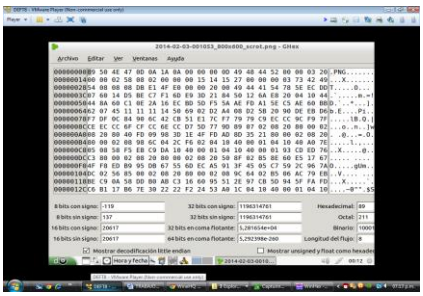
permite recuperar archivos borrados en dispositivos de almacenamiento con sistemas de archivos corruptos.





- GHEX. Es un editor hexadecimal que permite editar todos los tipos de archivos, dispositivos de almacenamiento y memorias RAM. Software para ambiente Linux.

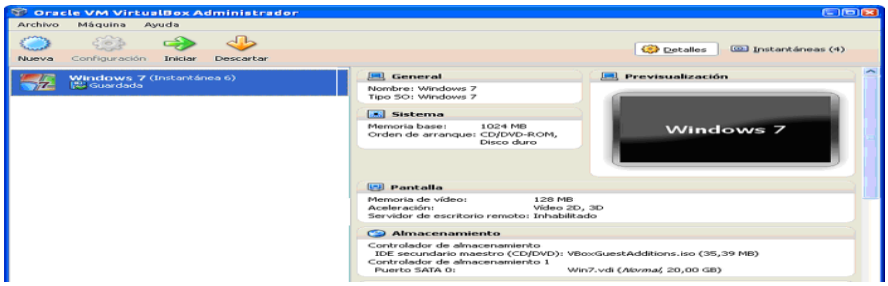




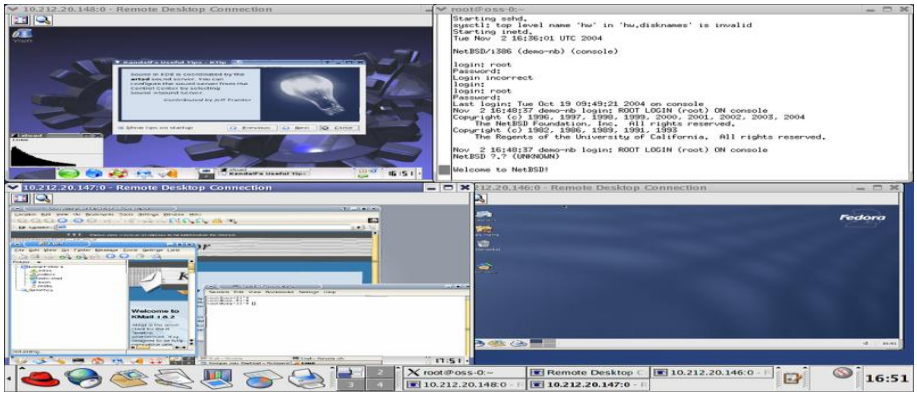
- Virtualización.

- VMWare: Software de virtualización para arquitecturas x86 y x86-64. Mediante este software se pueden crear virtualmente múltiples computadoras x86 y x86-64 en un sistema operativo huésped, cada una con su propio sistema operativo (Unix, Linux, Windows, etc.).

- VirtualBox: Software de virtualización para arquitecturas x86/amd64. Mediante este software se pueden crear virtualmente múltiples computadoras, cada una con su propio sistema operativo (Unix, Linux, Windows, etc.)



- XEN: La enciclopedia online Wikipedia define esta herramienta como: “Es un monitor de máquina virtual de código abierto desarrollado por la Universidad de Cambridge. La meta del diseño es poder ejecutar instancias de sistemas operativos con todas sus características, de forma completamente funcional en un equipo sencillo. Xen proporciona aislamiento seguro, control de recursos, garantías de calidad de servicio y migración de máquinas virtuales en caliente”.

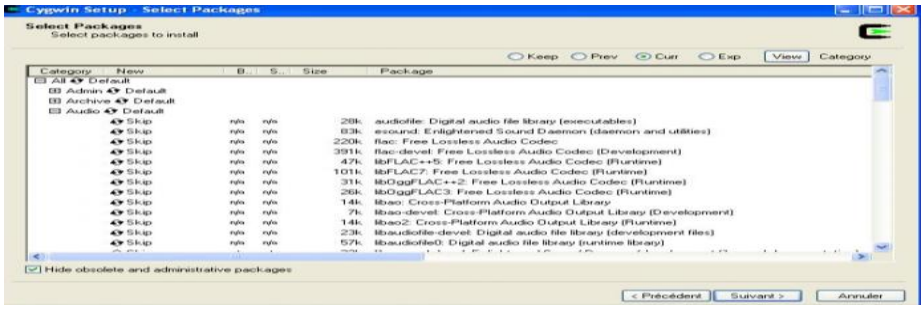


- Emuladores

- Wine: Es una reimplementación de la interfaz de programación de aplicaciones de Win16 y Win32 para sistemas operativos basados en

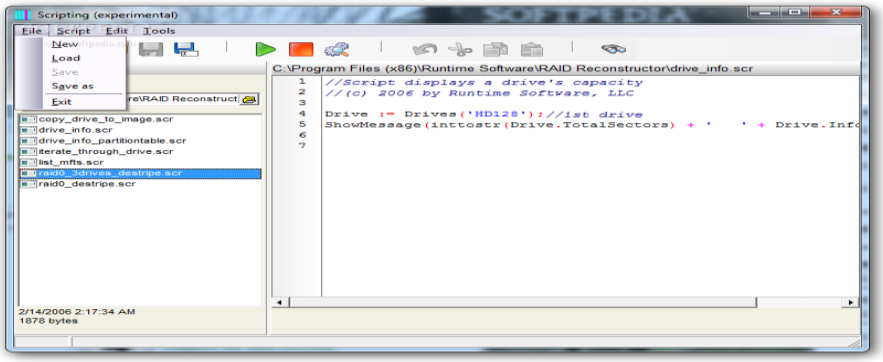
Unix. Permite la ejecución de programas diseñados para MS-DOS, y las versiones de Microsoft Windows.

- Cygwin: Software que permite tener un entorno de Linux dentro de un sistema Windows.



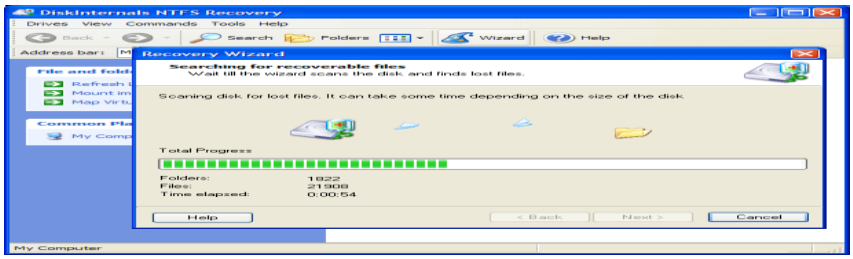
- Recuperación de archivos. En esta parte es importante definir un proceso conocido como “Carving”, que en si es el proceso de extracción de un conjunto de datos utilizando una técnica de análisis de información que no se basa en la estructura del sistema de archivos. También se podría definir como la extracción de un conjunto de datos que se encuentran inmersos en otro conjunto de datos.

  - Raid Reconstructor: Herramienta que permite recuperar datos de un sistema RAID 0 o RAID 5 dañado.



  - Raid Recovery: Herramienta que permite recuperar datos de un sistema RAID 0 o RAID 5 dañado. Desarrollado por la reconocida empresa DiskInternals.

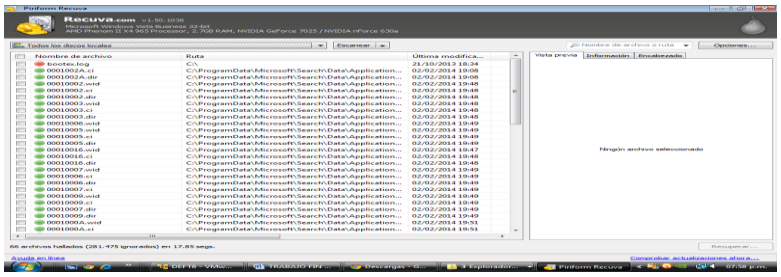
- NTFS Recovery: Software que permite la recuperación de archivos eliminados en sistemas NTFS. Desarrollado por DiskInternals.



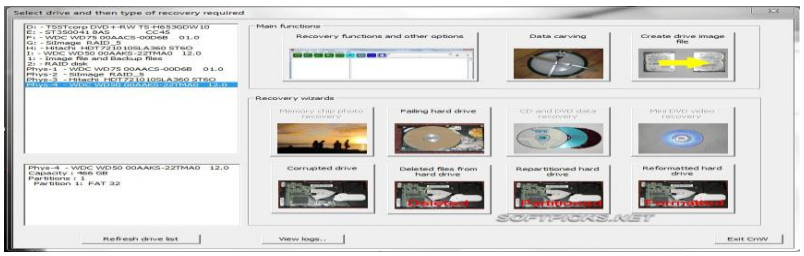
- Fat Recovery: Software que permite la recuperación de archivos eliminados en sistemas FAT. Desarrollado por Diskinternals.

- Linux Recovery: Software que permite la recuperación de archivos eliminados en sistemas Ext2/Ext3 desde Windows. Desarrollado por Diskinternals.

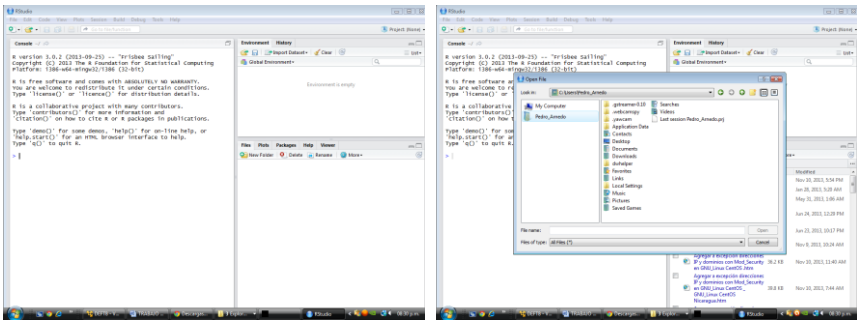
- Recuva: Software especializado en la recuperación de archivos eliminados.



- CNW Recovery: Herramienta que permite recuperar sectores dañados. Permite extraer datos de mediante Carving.

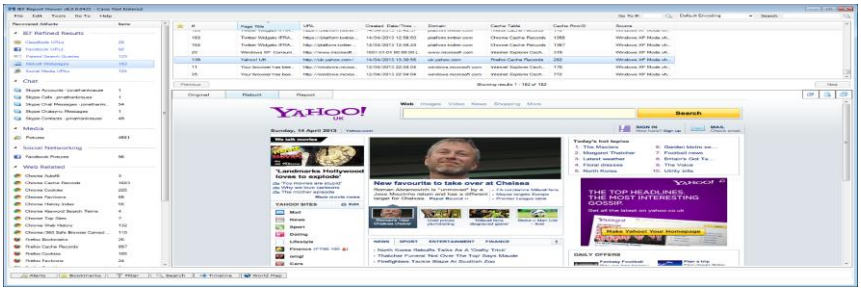


- Rstudio: Software que permite recuperar archivos de múltiples sistemas de archivos, entre otros: NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS, UFS1/UFS2 y particiones Ext2/Ext3/Ext4.

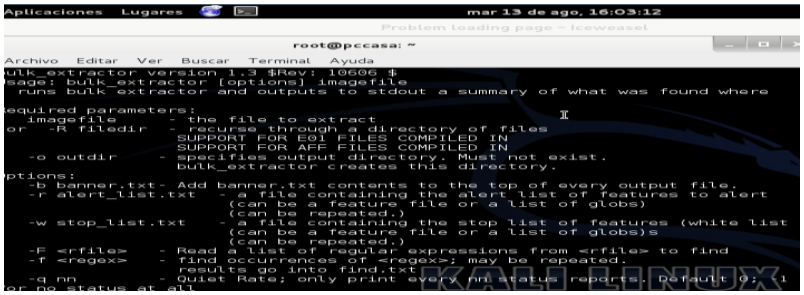


- FreeRecover: Herramienta que permite recuperar archivos borrados en discos duros o unidades de almacenamiento con partición NTFS.

- IEF (Internet Evidence Finder): Software que permite buscar evidencias en las imágenes de discos (o en discos directamente) extrayendo mediante el proceso de Carving, datos sobre archivos abiertos desde portales que ofrecen almacenamiento en la nube, tales como dropbox, google drive, skydrive, entre otros. Entre los datos que trata de encontrar están: tamaño y nombres de archivos, fechas y horas de acceso, nombres de usuario y tamaño de los archivos.

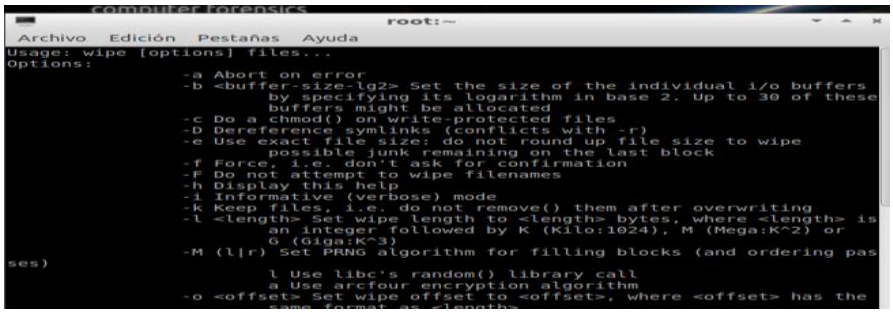


- Bulk_extractor: Software que permite extraer datos desde un archivo o imagen e inclusive desde carpetas.



- Borrado de archivos

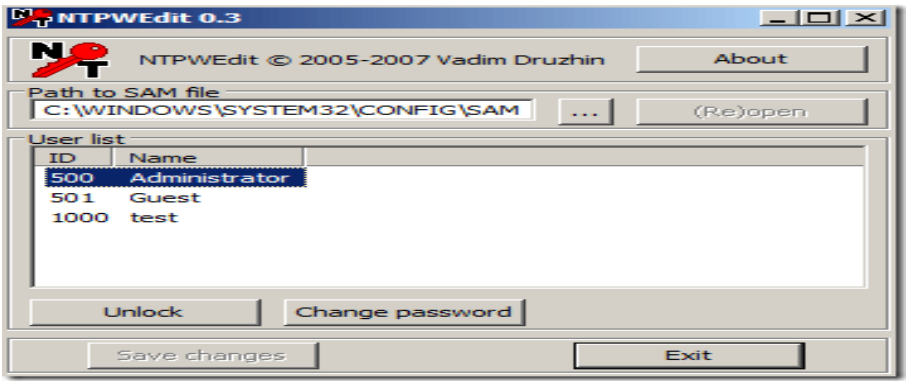
  - Wipe: Software que tiene como finalidad borrar archivos de cualquier medio de almacenamiento de forma segura y recuperar el espacio libre existente en el mismo. Además permite eliminar cualquier registro relacionado con la actividad personal en el equipo informático.



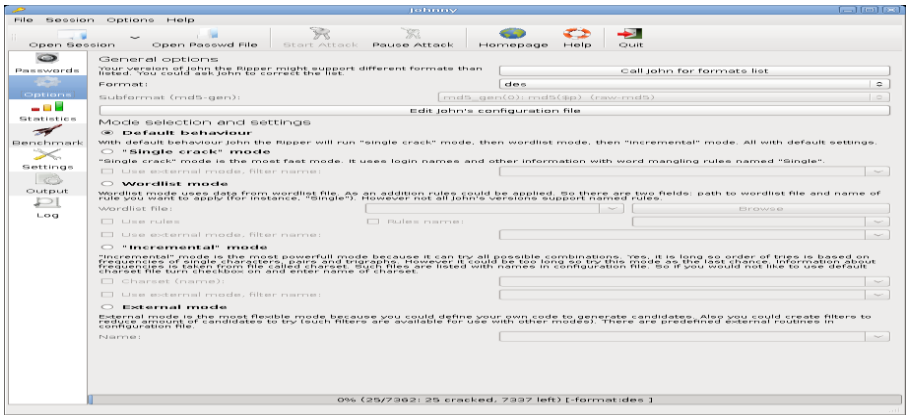
  - HardWipe: Software que tiene como finalidad borrar archivos de cualquier medio de almacenamiento de forma segura y recuperar el espacio libre existente en el mismo. Cuenta con varios algoritmos de borrado seguro como GOST R, DOD 5220, Schneier y Gutmann.

- Recuperación de Contraseñas:

  - Ntpwedit: Software que permite cambiar o eliminar contraseñas en sistemas Windows versiones 2000, XP, Vista, 7 y 8, pero no aplica para sistemas Windows que implementen Active Directory (Windows Server).

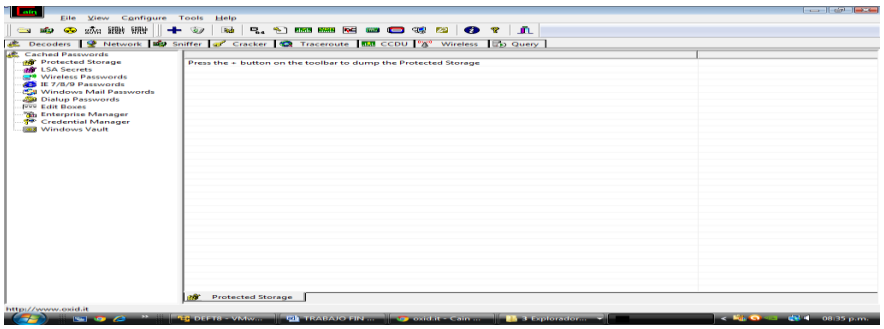


- John The Ripper: Programa que permite descubrir contraseñas a base de fuerza bruta. La interfaz gráfica se denomina Johnny.



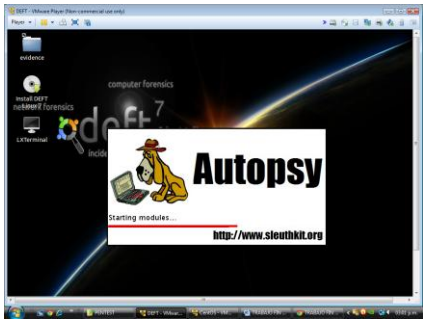
- Ntpasswd: Software parecido a Ntpwedit, con la particularidad que permite arrancar el sistema desde un CDLive y ejecutarse desde allí para su proceso de recuperación.

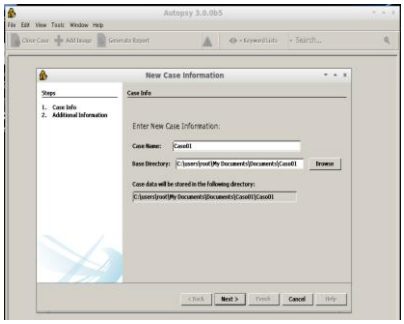
- Cain & Abel. Aplicativo para analizar tráfico y permite también recuperar contraseñas bajo entorno Windows.

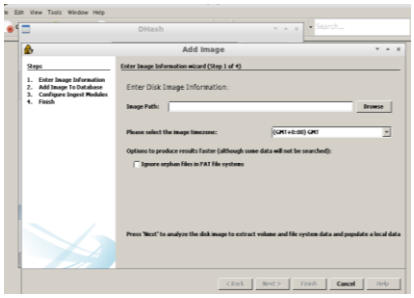


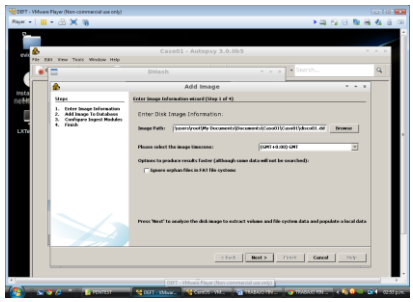
- Frameworks (Suite de herramientas estandarizadas para el análisis forense):

  - Sleuth Kit y Autopsy: Sleuth Kit es una colección de herramientas robustas para el análisis forense de volumen de sistema y archivos. Autopsy es la interfaz gráfica que permite utilizar de una forma más fácil y amigable todo el potencial de este aplicativo.

- 







  - Encase Forensic: Software líder mundial para el análisis forense informático, desarrollada por la empresa Guidance Software Inc., mediante la cual se recolectan datos digitales, se realizan análisis y se realizan informes sobre descubrimientos en la escena del crimen.

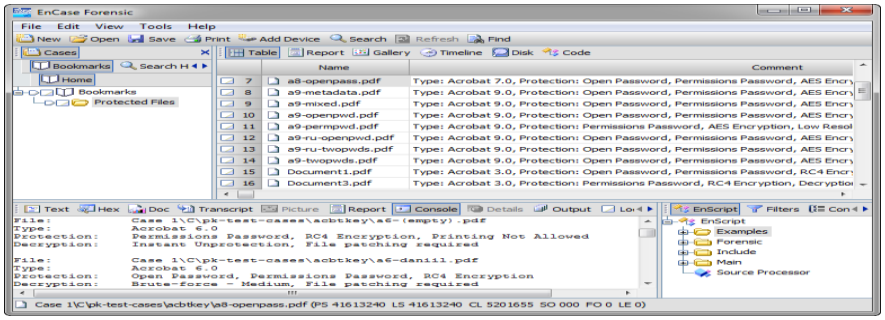
    Entre muchas características relevantes de ENCASE que la convierte en un marco referencia en el mundo del software informático forense se puede destacar:

    - Copiado de Discos Fuente en formato Comprimido. Encase permite crear copias comprimidas sin perdidas de datos durante el proceso de compresión. Además las copias comprimidas se

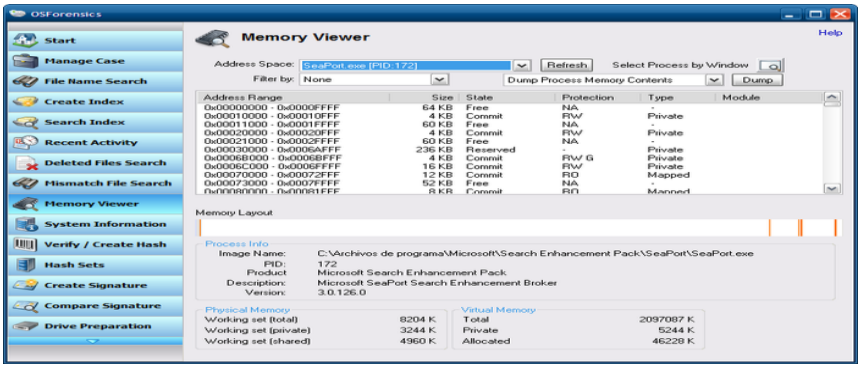
pueden tratar en todo el proceso de análisis forense de igual forma que se manejaría el dispositivo original. Esto genera ventajas como el ahorro de espacio en el disco del equipo donde se hace el trabajo forense.

- Encase permite al equipo investigador hacer comparativos en paralelo con otras copias sin complicaciones. La evidencia puede ser analizada en forma local o en red por el investigador y Encase permite además que pueda ser colocada en dispositivos de diferentes características como puede ser de tecnología IDE, SCSI, ZIP, etc.

- Encase permite analizar las cabeceras de los archivos en un dispositivo o copia digital permitiendo descubrir tipos de archivos ocultos o modificados intencionalmente para su no detección.



- OSForensics: Conjunto de herramientas forenses, que permiten entre muchas opciones realizar análisis sobre copias de discos montados en el sistema, búsqueda de archivos y generación de Hash.



- Forensic Toolkit: Desarrollado por AccessData, es un aplicativo forense muy completo. Entre sus características más sobresalientes se pueden destacar:

  - Permite analizar cientos de ficheros en búsqueda de características predefinidas, lo cual favorece al investigador forense a descubrir evidencias más rápidamente.

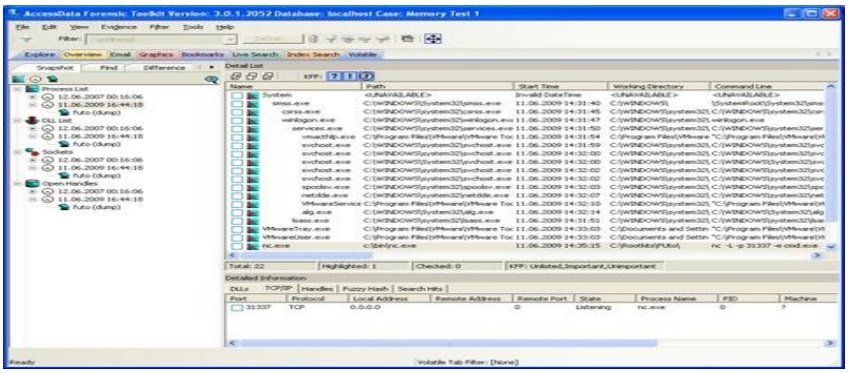
  - Maneja 270 tipos de formato de ficheros diferentes.

  - Permite recuperar particiones borradas.

  - Permite recuperar correos electrónicos borrados parcial o totalmente.

  - Ubica archivos por tipo analizando la cabecera de los mismos, detectando extensiones y archivos modificados intencionalmente.

  - Permite extraer datos de ficheros comprimidos con los algoritmos comunes de compresión (Zip, Rar, Gzip, Tar. Permite generar informes detallados.



- Digital Forensic Framework (DFF): Framework para análisis forense, con licenciamiento libre y código abierto. Cuenta con su propio entorno gráfico lo que permite ser usado más fácilmente por personal no experto.

Entre las funcionalidades que ofrece están:

- Preservación de la evidencia digital (cadena de custodia). Ofrece funcionalidad en cuanto a bloqueo de escritura de software y cálculo de hash criptográfica.

- Acceso a dispositivos locales y remotos. Unidades de disco, dispositivos extraíbles, sistemas de archivos remotos

- Lee formatos de archivos forenses digitales. Ewf, AFF 3, formatos de archivo RAW

- Reconstrucción de disco de máquina virtual. Reconstruye discos virtuales corruptos compatibles con VMware.

- Análisis de archivos en Windows y Linux. Registro, buzones, NTFS, los sistemas de archivos FAT 16/12/32

- Búsqueda de (meta) datos. Las expresiones regulares, diccionarios, búsqueda de contenidos, etiquetas, etc.

- Recupera objetos ocultos y eliminados.

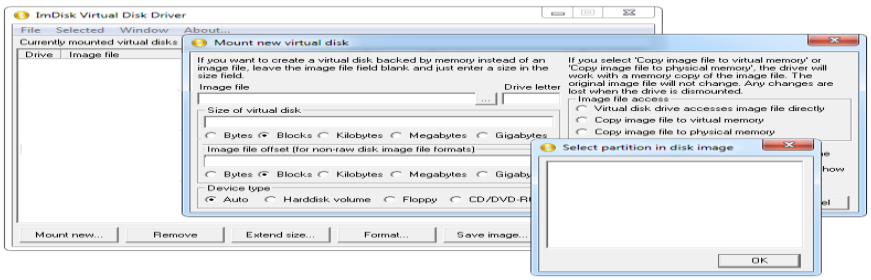
- Análisis de la memoria RAM. Procesos, archivos locales, extracción binaria, conexiones de red.

- Análisis de discos (Montaje, Virtualización y /o Recuperación).

  - Smart: Desarrollado por ASR Data, software cuya finalidad es el apoyo al análisis forense. Este permite detectar todos los dispositivos de almacenamiento conectados a un computador, su estructura lógica (particionamiento) y demás características, entre las que se destacan marca, modelo, capacidad y serial

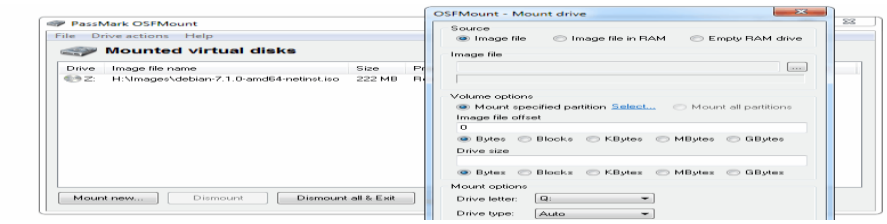
  - ILook: Software muy completo para el análisis forense informático, entre sus principales características podemos detallar que permite extraer y analizar imágenes digitales de medios de almacenamiento, analizar cabeceras de archivos para validación real de tipo de archivos, editor hexadecimal integrado, entre otras.

  - ImDisk: Software que permite crear virtualmente unidades de discos y de CD/DVD usando imágenes de discos o la memoria del sistema.



  - Daemon Tools: Software que permite montar imágenes de disco. Es comercial pero presenta una versión lite con mucha funcionalidad.

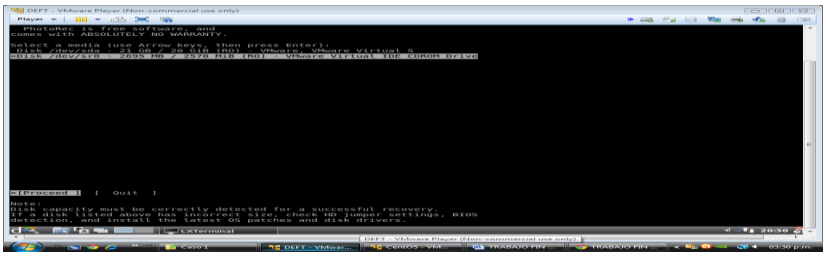
- PassMark OSFMount: Software que permite montar imágenes de discos en unidades virtuales.



- LiveView: Herramienta que toma una imagen de disco y genera con ésta una máquina virtual que se puede utilizar con la herramienta VMware.

- MountImagePro: Software que permite montar imágenes de discos en unidades virtuales.

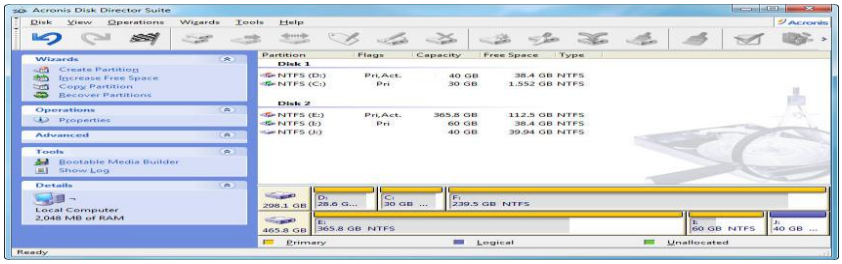
- PhotoRec: Herramienta que tiene entre muchas otras funcionalidades la del tratamiento de imágenes de discos.



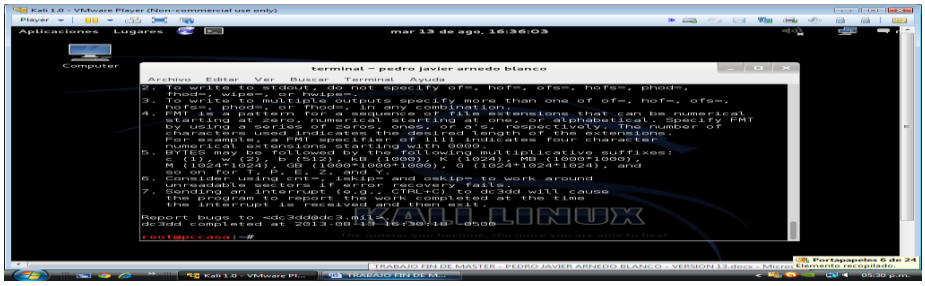
- Clonación

- Ghosts: Software que permite clonar o crear imágenes de un medio de almacenamiento permitiendo copiar el contenido completo o una partición específica. Este clonado se puede realizar a otro disco de igual o superior tamaño o como un archivo que se puede restaurar posteriormente.

- Acronis: Este software de clonado permite crear una imagen exacta del disco o de los discos de un servidor Windows o Linux, incluyendo el sistema operativo, las bases de datos y las aplicaciones instaladas en el mismo. Esta clonación posteriormente se puede migrar a servidores virtuales o físicos.



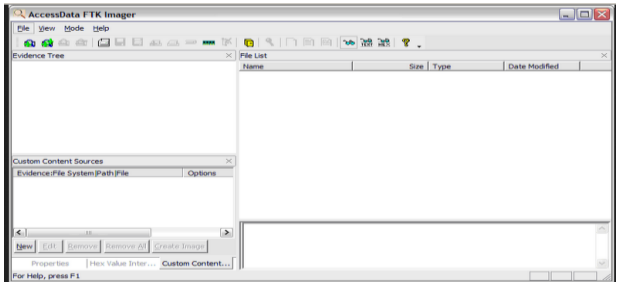
- Dc3dd: Software que permite crear imágenes o copias de unidades de almacenamiento.



- Adquisición y Análisis de Memoria.

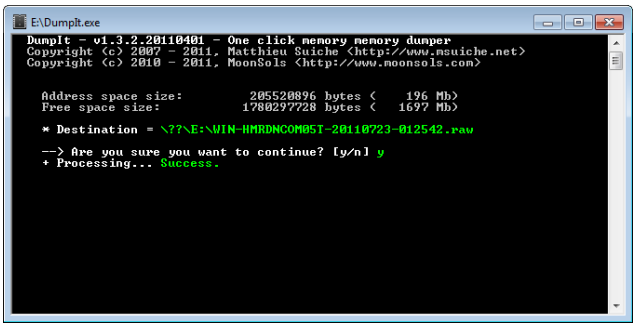
- RedLine: Software, con interfaz gráfica, que permite adquirir la memoria RAM y analizarla.

- FTK Imager: Software que se especializa principalmente en la adquisición de memoria RAM.

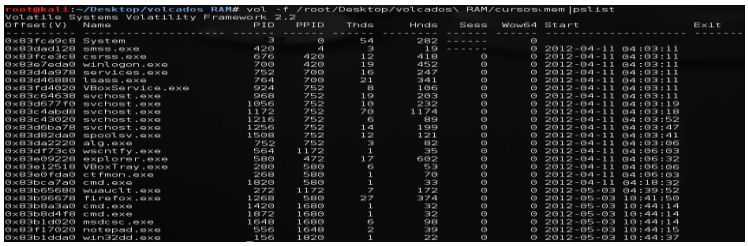


- Proccess Dumper (PD): Herramienta que permite exportar un proceso de la memoria RAM a un archivo.

- DumpIt: Aplicativo que permite realizar volcados de la memoria RAM a un archivo.



- Volatility: Herramienta que permite analizar los procesos que se están ejecutando en la memoria RAM y extrae de ellos información relevante.



- Sistema de Archivos: Tipo de software para el tratamiento de archivos.

  En este ítem es pertinente conocer la definición de “Tabla Maestra de Archivos” (MFT: Master File Table), la cual podemos enunciar como una base de datos que contiene entradas que relacionan en su totalidad los archivos de sistema, archivos del usuario y directorios que componen un volumen de disco.

  También es importante conocer la definición de “Directorio Prefetch”, el cual es un directorio presente en el sistema de archivos de Windows que almacena información en una serie de archivos pequeños correspondiente a los programas que se abren regularmente en un equipo, para que al momento de iniciar un computador el reconozca estas preferencias y permita ejecutar estos programas más rápidamente. Si el directorio prefech se vacía, los programas comunes tardaran más en ejecutarse la próxima vez después del vaciado.

  Las siguientes herramientas permiten el tratamiento directo sobre la Tabla Maestra de Archivos:

  - AnalyzeMFT, MFT Extractor, MFT Tools, MFT_Parser.

  Las siguientes herramientas permiten el tratamiento directo sobre el directorio prefetch:

  - Prefetch Parser, Winprefectchview

- Análisis Registro de Windows.

  En este ítem es importante anotar el concepto de shellbags, que se refiere a los espacios donde el sistema operativo Windows guarda la información correspondiente a las preferencias de los usuarios en lo concerniente a las propiedades de visualización de sus interfaces graficas. Entre otras

propiedades podemos mencionar: posición de las ventanas en la pantalla, tamaño de las ventanas, etc.

- RegRipper: Es una aplicación para la extracción, la correlación, y mostrar la información del registro.

- WRR: Software que permite obtener de forma gráfica importantes datos del sistema, usuarios y aplicaciones, tomando como base para extraer esta información el registro de windows.

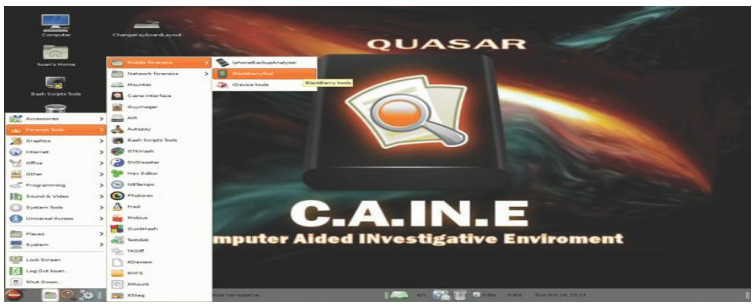
- Shellbag Forensics: Software que permite analizar los shellbags de Windows.

- Linux Distribución LiveCD

  - Backtrack: Distribución de Linux especializada Seguridad Informática. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador

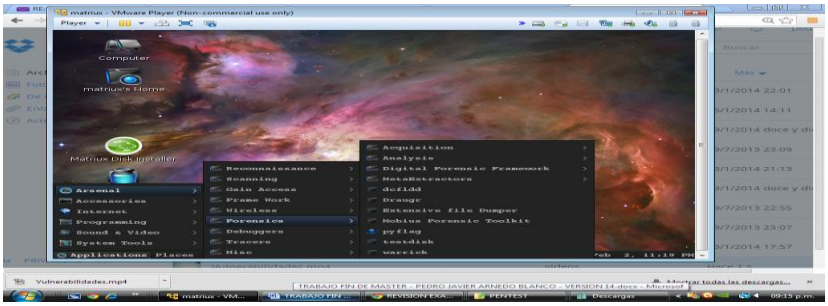
  - KALI: Distribución de Linux especializada Seguridad Informática. Basada en Debian, viene como LIVECD pero permite instalar la distribución en nuestro computador. Distribución dirigida a realizar auditorías de seguridad orientadas al sector profesional.

- CAINE: Distribución de Linux de origen italiano, especializada en el análisis forense. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador.



- DEFT: Distribución de Linux especializada en el análisis forense, no solo de discos duros, también se pueden realizar análisis forenses de redes y de dispositivos móviles. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador.

- MATRIUX. Distribución de Linux dedicada a la seguridad con buenas herramientas de Informática Forense.



- BUGTRAQ: Distribución de Linux que ofrece una gran cantidad de aplicativos para realizar pruebas de penetración y análisis forense. Esta distribución permite instalarse en un computador o utilizarse como un LiveCD desde un DVD o USB.

2. METODOLOGÍAS O MODELOS DE ANALISIS INFORMÁTICO FORENSE

Una metodología o modelo de análisis informático forense consiste en una serie de etapas que involucran procedimientos, técnicas, herramientas software y hardware y aspectos legales, las cuales tienen como misión principal servir de guía al investigador informático forense en su trabajo de peritazgo. En otras palabras tienen como objetivo principal documentar, educar y normalizar el análisis informático forense.

En este capítulo se enumeran algunas de las metodologías más importantes y reconocidas en el ámbito informático forense.

2.1. **Modelos de Análisis Informático Forense**

No existe un modelo estándar para el análisis informático forense, pero si unos modelos muy importantes y reconocidos internacionalmente, los cuales trataremos en este documento,

A continuación un resumen de los más representativos:

2.1.1. Modelo DFRWS (Digital Forensic Research Workshop).

Modelo desarrollado entre los años 2001 y 2003 en el Digital Forensic Research Workshop. El modelo aporta el concepto conocido como “Clases de Acción en la Investigación Digital”. Estas “Clases de Acción” son técnicas que permiten clasificar por grupos las actividades en un proceso investigativo. El modelo establece que cada investigación se debe establecer de forma independiente y detallada en una matriz, indicando las actividades a realizar y la técnica que se implementará en la misma.

Las actividades que se deben realizar son:

- Identificación
- Preservación
- Colección
- Examen
- Análisis
- Informe
- Decisión

2.1.2. Modelo de Casey (Versión Año 2000).

Desarrollado por Eoghan Casey, quien en el año 2000 da a conocer su modelo de análisis forense informático (Casey, 2011). Este modelo ha tenido versiones posteriores como muestra de un proceso evolutivo.

Las actividades que se deben realizar son:

- Identificación de evidencias
- Conservación, adquisición y documentación de evidencias.
- Clasificación, comparación e individualización de evidencias.
- Reconstrucción de los hechos.

En estas dos últimas actividades, se puede producir un ciclo repetitivo, ya que se pueden presentar nuevas evidencias que requieran un nuevo

procesamiento. Por este motivo estas dos últimas actividades son denominadas por Casey como *Ciclo de Procesamiento de las Pruebas*.

2.1.3. Modelo de Casey (Versión Año 2004).

Nueva versión mejorada del modelo de Casey Versión Año 2000, el cual se compone de las siguientes actividades o fases:

- Autorización y preparación de evidencias: Esta fase comprende las actividades del recabado de evidencias, previo a las autorizaciones legales a que se diera lugar.

- Identificación de las evidencias: Esta fase comprende la identificación detallada de toda evidencia encontrada.

- Documentación de las evidencias: En realidad esta fase es repetitiva, ya que se da durante todo el proceso investigativo y consiste en documentar por escrito todo lo que se realizó para encontrar las respuestas que permitieron esclarecer los acontecimientos que se dieron durante la ejecución del incidente de seguridad informático.

- Adquisición de las evidencias: En esta fase se debe generar una imagen del contenido digital (datos) de todo dispositivo de almacenamiento encontrado, ya que esto puede servir de prueba en un juicio. Es importante hacer varias copias de cada elemento, para mayor seguridad de preservar la integridad del original, la cual nunca se deberá tocar.

- Conservación de las evidencias: En esta fase se debe asegurar todas las evidencias en un lugar seguro que permita garantizar plenamente la integridad de los datos originales.

- Examen y análisis de las evidencias: Utilizando herramientas de software idóneas se analizan las copias de las evidencias, se elabora una hipótesis y

se empieza el proceso investigativo que arroje información relevante que permita validar la hipótesis y con ello el esclarecimiento de los hechos.

- Reconstrucción de lo sucedido: En esta fase se debe haber llegado al punto de tener las respuestas a los siguientes interrogantes: **¿**desde dónde?, ¿qué se atacó?, ¿de qué forma?, ¿quién(es) atacó(aron)? y ¿en qué periodo de tiempo?

- Informe final o conclusiones: En esta fase se elabora un informe detallado de todos lo desarrollado y lógicamente de los resultados obtenidos.

2.1.4. Modelo Forense del Departamento de Justicia de los Estados Unidos.

El Departamento de Justicia de los Estados Unidos tiene una división especial denominada “Sección de Crimen Computacional y Propiedad Intelectual”.

Esta división desarrolló un modelo de análisis forense informático basándose en aportes intelectuales de una gran cantidad de funcionarios que laboraban en ese momento en agencias federales y que estaban especializadas y dedicadas a la informática forense (Ashcroft John, Daniels Deborah y Hart Sara, 2004). Esta investigación dio como aporte principal las tres fases que este organismo establece como la base principal del análisis forense, haciendo acápite en que estas fases dan como realizado, en forma previa, las copias de seguridad o clonación de los dispositivos de almacenamiento encontrados como evidencias digitales en un caso investigado. Estas fases son:

- Preparación y Extracción

- Identificación

- Análisis

Además este modelo estableció las especificaciones básicas en la investigación forense, las cuales son:

- Emplear métodos científicos
- Recolectar y Preservar
- Validar
- Identificar
- Analizar e Interpretar
- Registrar, Documentar y Presentar.

En lo referente a las fases se detallan más a fondo a continuación:.

- Preparación y Extracción. En esta fase los investigadores se dan a la tarea de estudiar si las pruebas o evidencias encontradas en un delito investigado, tienen el valor probatorio suficiente para ser presentado antes una autoridad judicial. Si durante este estudio se detecta alguna falencia se comunican con el o los investigadores involucrados en la recolección de evidencias y le exponen la situación para ver si se puede subsanar o si por el contrario se desecha la prueba.

  Una de las primeras actividades a realizar por los analistas forenses es verificar que las herramientas, tanto software como hardware, funcionen sin complicaciones. Esto debe hacerse siempre que se adquiera una nueva herramienta o después de aplicada alguna actualización o modificación a la misma.

  Después de esta revisión, el paso a seguir es realizar la clonación de las evidencias digitales. El listado de evidencias que quedan inmersas dentro de la investigación y se deben clonar debe ser allegado a los analistas forenses por escrito por una instancia superior, con base en los resultados de la etapa

previa de recolección de evidencias. En ese mismo documento se debe indicar como proceder con cada evidencia a tratar.

Siguiendo el proceso y verificado el listado correspondiente, los analistas deben realizar la copia o clonación de cada una de las evidencias y deben verificar igualmente la integridad de las mismas después de la clonación. Hay que anotar que lo que el analista recibe está basado en un proceso previo, en el cual se debió haber obtenido los datos originales de estas evidencias, se ha debido hacer una copia de las mismas y comprobado igualmente la integridad de cada una. De no ser así, el analista deberá antes de sacar una copia o clonación de cada evidencia, establecer la integridad de ella, aplicando una función resumen a las mismas y luego proceder a clonar. Luego de esto realizar un nuevo hash o función resumen a lo original y a lo clonado y entregar todo lo original a la instancia que le corresponde efectuar la cadena de custodia.

Lógicamente antes de empezar, el analista forense hace una comprobación del resumen o hash para validar la integridad de lo que va a empezar a analizar.

El paso siguiente es extraer la información, organizarla y responder inquietudes mismas del delito, en atención a lo analizado. Todo esta información se registra en un documento denominado “Información Extraída”. Esas mismas respuestas servirán para que en un acto judicial se formulen las preguntas que se requieren para llevar por buen término el proceso.

A medida que se van analizando las evidencias se van marcando como evaluada y todo el material probatorio se incluye en listado base de información extraída y válida como prueba.

- Identificación. En esta fase los analistas informáticos forenses validan nuevamente la identificación de cada evidencia registrada en el documento “Información Extraída”. Durante esta validación se identifica su tipo y se establece si la misma es vital para la investigación, para el esclarecimiento

de los hechos y si se puede presentar como elemento probatorio frente a una instancia judicial. Si el analista considera que la evidencia, legalmente hablando, no la puede procesar él como perito, debe buscar la instancia competente para ello y trasladarle la evidencia. Si se determina que si es válida, se identifica como “Evidencia Probatoria o Relevante”. Si al contrario, la evidencia no es relevante, se le establece la condición de “procesada” y se aparta definitivamente del lote previamente seleccionado.

Cada evidencia puede arrojar nuevas evidencias, a las cuales se le tratarán en condiciones iguales a las ya estipuladas.

Ya para finalizar, el analista realiza un informe técnico con las conclusiones pertinentes, los cuales la entidad que está al frente de la investigación determinará si es suficiente con lo conseguido hasta ese momento o si es necesario ahondar más en la investigación.

- Luego de analizadas todas las evidencias y encontrados muchos datos importantes para resolver el caso, se detallan en un documento que se le entrega a la entidad que lleva el caso. Estos datos deben responder los interrogantes básicos en cualquier investigación: ¿qué se atacó?, ¿de qué forma?, ¿quién(es) atacó(aron)? y ¿en qué periodo de tiempo?; además de justificar cada dato encontrado, cada evidencia analizada y el aporte probatorio frente a una instancia judicial. Si es posible detallar situaciones relevantes especificas por cada evidencia mucho mejor. Y al final todos estos hallazgos se detallan en un documento denominado “Análisis de Resultados”.

- Reporte final. En esta fase los analistas forenses entregan un documento completo y detallado con todos sus resultados, para que sean presentados ante una instancia judicial con toda la validez probatoria necesaria.

3. SIMULACIÓN PRÁCTICA APLICADA AL USO DE HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE

Para el desarrollo de este capítulo se van a enumerar algunos incidentes de seguridad informática, los cuales servirán como marco de referencia para llevar a cabo en ellos un proceso de análisis informático forense, lo que permitirá determinar con claridad y certeza la aplicabilidad de diversas herramientas de software en la investigación de delitos informáticos, lo cual es el objetivo principal de este trabajo de fin de máster.

Para el análisis de los incidentes de seguridad informática enunciados a continuación, se ha optado por utilizar el modelo Forense del Departamento de Justicia de los Estados Unidos.

Cabe anotar que se asumen como realizados los pasos relacionados con el aseguramiento y cadena de custodia de las evidencias digitales identificadas en los casos que a continuación se tratarán, ya que este trabajo se centra en la ejecución de herramientas de software, su funcionalidad y su aplicabilidad de acuerdo al objetivo de investigación planteado.

3.1. Delito Informático – Incidente DELINF0951.

Un cracker aprovechándose de sus conocimientos y experiencia y aprovechándose de tener acceso a recursos computacionales adecuados viola el sistema de seguridad informático de una clínica, accediendo a un servidor con sistema operativo Linux CentOS y robando información confidencial de los pacientes atendidos en los últimos diez años, alimentada en una hoja de cálculo con tablas dinámicas, la cual publico en internet en un blog anónimo.

Se requiere investigar el origen del incidente, posibles delincuentes, herramientas informáticas utilizadas, daños ocasionados, fallas que permitieron el ilícito y correcciones a corto plazo.

3.1.1. Investigación Forense.

El día 14 de octubre de 2013 un funcionario informa a sus superiores de la clínica Medical Center Valledupar (Colombia) que el equipo HP destinado a alojar la base de datos de los pacientes tratados en los últimos años, soportada en una hoja de cálculo con tablas dinámicas, presenta registros borrados. El administrador descubre esta incidencia porque al consultar el archivo la información estaba incompleta.

Equipo afectado:

Fabricante	HP
Modelo	Deskpro
Número de serie	978978978
Procesador	Intel® Pentium® i7 (4 núcleos, 2,9 GHz, 3 MB, 55 W)
Memoria	8 GB DDR3
Disco Duro	Marca: HP Capacidad: 750 GB Tecnología: SATA Serial: XYZ7890
Sistema Operativo	CentOS 6.5
Nombre del equipo	ServidorCM1
IP	192.168.1.1

Luego de pasadas las fases de análisis del problema, recolección de evidencias digitales y preservación de las mismas, continuamos con la fase de evaluación de estas evidencias.

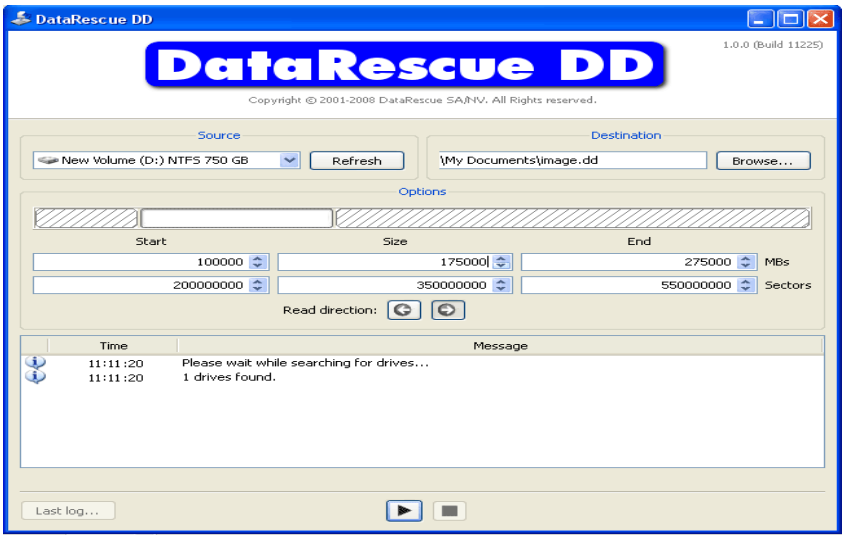
Novedades encontradas en la consecución de este delito:

- Computador de escritorio simple sirviendo como Servidor de aplicaciones, con sistema operativo CentOS v6.5, sin implementación de Herramientas de Seguridad a nivel de hardware o software (Tipo Firewall, IDS, etc.)

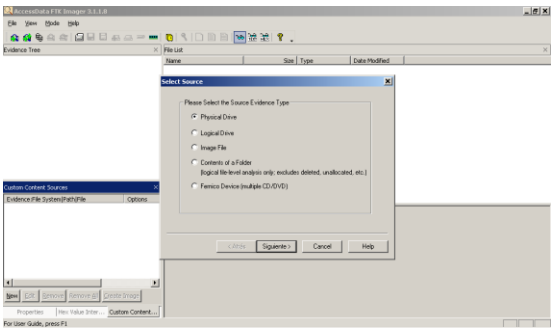
Evidencias digitales adquiridas en la consecución de este delito

- Adquisición de la memoria RAM a través del aplicativo DumpIT

- Clonación del Disco Duro mediante el aplicativo DD, previa generación del hash del disco original.



- Creación de dos imágenes del disco duro mediante el software FTK Imager. Se hace validación hash, resultado verificado.



Procedimiento Realizado:

Seleccionamos uno de los equipos de la entidad, los cuales tienen las mismas características que el servidor y clonamos una de las copias al disco duro de éste, luego hacemos una validación hash para comprobar la integridad del clonado. Se verifica y valida. Arrancamos el sistema.

Nos logueamos con el usuario root, credenciales facilitados por el usuario del equipo atacado en la entidad, que inexplicablemente su password es admin01, lo que da a entender la poca gestión de seguridad aplicada por él.

Validamos que software se ha instalado recientemente con el comando rpm -qa --last

Lo que nos arroja el siguiente resultado:

xchat-2.8.8-0 lun 09 sep 2013 22:10:15 COT
sudo-1.6.3p6-1 mar 01 ene 2013 17:00:59 COT
stunnel-3.13-3 mar 01 ene 2013 17:00:59 COT
strace-4.2.20010119-3 mar 01 ene 2013 17:00:59 COT
anonftp-4.0-4 mar 01 ene 2013 16:57:29 COT
xinetd-2.1.8.9pre14-6 mar 01 ene 2013 16:57:28 COT
zlib-devel-1.1.3-22 mar 01 ene 2013 17:00:59 COT
texinfo-4.0-20 mar 01 ene 2013 17:00:59 COT
wu-ftpd-2.6.1-16 mar 01 ene 2013 16:57:28 COT
kudzu-devel-0.98.10-1 mar 01 ene 2013 16:56:07 COT
urw-fonts-2.0-12 mar 01 ene 2013 16:57:28 COT
telnet-server-0.17-10 mar 01 ene 2013 16:57:28 COT
glibc-common-2.2.2-10 mar 01 ene 2013 16:56:07 COT
man-pages-es-0.6a-7 mar 01 ene 2013 16:56:09 COT
man-pages-1.35-5 mar 01 ene 2013 16:56:08 COT
mailcap-2.1.4-2 mar 01 ene 2013 16:56:07 COT
indexhtml-7.1-2 mar 01 ene 2013 16:56:07 COT

Se puede apreciar la instalación el día 09 de septiembre de 2013 de un software de mensajería instantánea IRC denominado xchat. Lo que trae consigo graves problemas, ya que si no existe otro usuario en el servidor además del root, significa que la persona que ha instalado el software de IRC lo ha hecho con este usuario y lo más seguro se ha conectado a canales de Chat desde ese perfil. Luego de esta conectado es muy fácil encontrar su dirección ip para otro usuario que este en el mismo canal mediante el comando /whois, el cual se puede ejecutar desde el mismo software XCHAT, sin necesidad de instalar nada adicional.

Miramos los logs fallidos en /var/log/faillog, o con el comando *faillog –u root* y se observa que el día del incidente se dieron innumerables conexiones infructuosas al servidor con el usuario root antes de ser accesado.

Username	*Failures*	*Maximum*	*Latest*
root	*17*	*99*	

Y con el comando last observamos los últimos logins correctos:

last -20

root	*tty7*	*Sat Oct 10 06:57*	*still logged in*
root	*tty8*	*Sat Oct 10 08:26*	*still logged in*
root	*tty7*	*Sat Oct 10 17:37*	*still logged in*
root	*tty8*	*Sat Oct 10 22:56*	*still logged in*
root	*tty7*	*Sat Oct 11 06:57*	*still logged in*
root	*tty8*	*Sat Oct 11 09:46*	*still logged in*
root	*tty7*	*Sat Oct 11 12:57*	*still logged in*
root	*tty8*	*Sat Oct 11 23:02*	*still logged in*
root	*tty7*	*Sat Oct 12 06:47*	*still logged in*
root	*tty8*	*Sat Oct 12 17:56*	*still logged in*
root	*tty7*	*Sat Oct 12 23:07*	*still logged in*
root	*tty8*	*Sat Oct 13 06:48*	*still logged in*
root	*tty7*	*Sat Oct 13 23:02*	*still logged in*
root	*tty8*	*Sat Oct 14 07:46*	*still logged in*

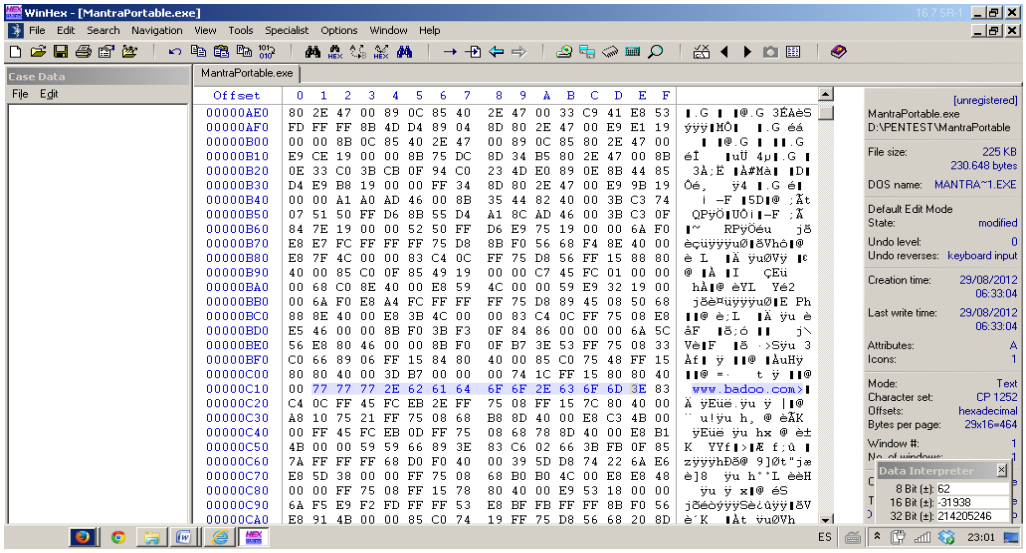
root tty7 Sat Oct 14 09.27 still logged in
root tty8 Sat Oct 14 12:36 still logged in
root tty7 Sat Oct 14 14:37 still logged in
root tty8 Sat Oct 14 17:22 still logged in
root tty7 Sat Oct 14 20:04 still logged in
root tty8 Sat Oct 14 22:51 still logged in

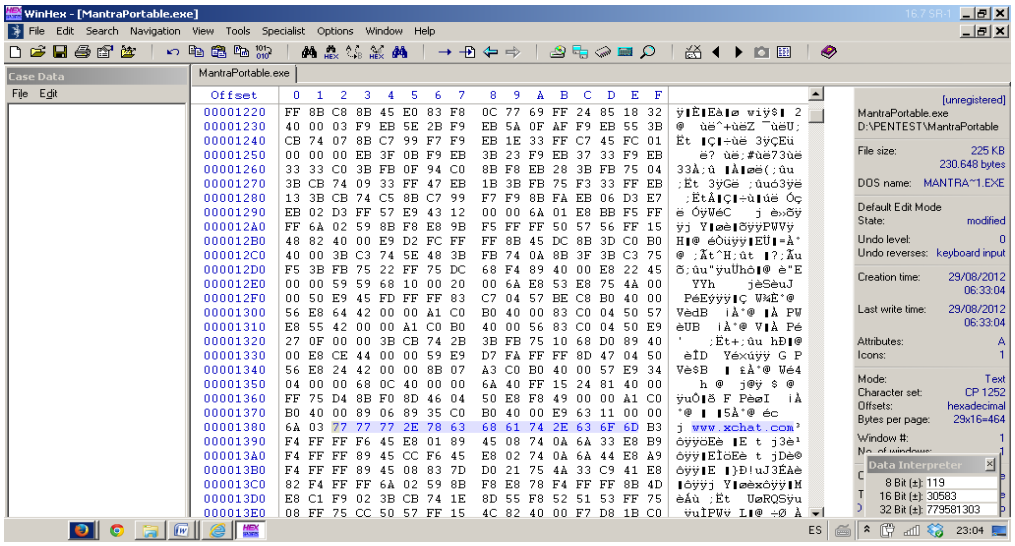
Se observa que existe unas horas comunes de logins correctos, entre las 06:46 y las 06:57 y entre las 22:56 y 23:07. Se entiende el acceso en horas de la mañana porque la política de seguridad implementada en la empresa estipula copias de seguridad todos los días antes de las 8:00 am que empiezan labores, pero no se tiene claro los accesos nocturnos, más aun cuando el usuario de la base de datos trabaja hasta las 06:00pm y las conexiones se dan localmente.

Se mira el historial de comandos que se guardan en el archivo *~/.bash_history* y se observa que el programa de chat se ejecuta todos los días en ese periodo de tiempo.

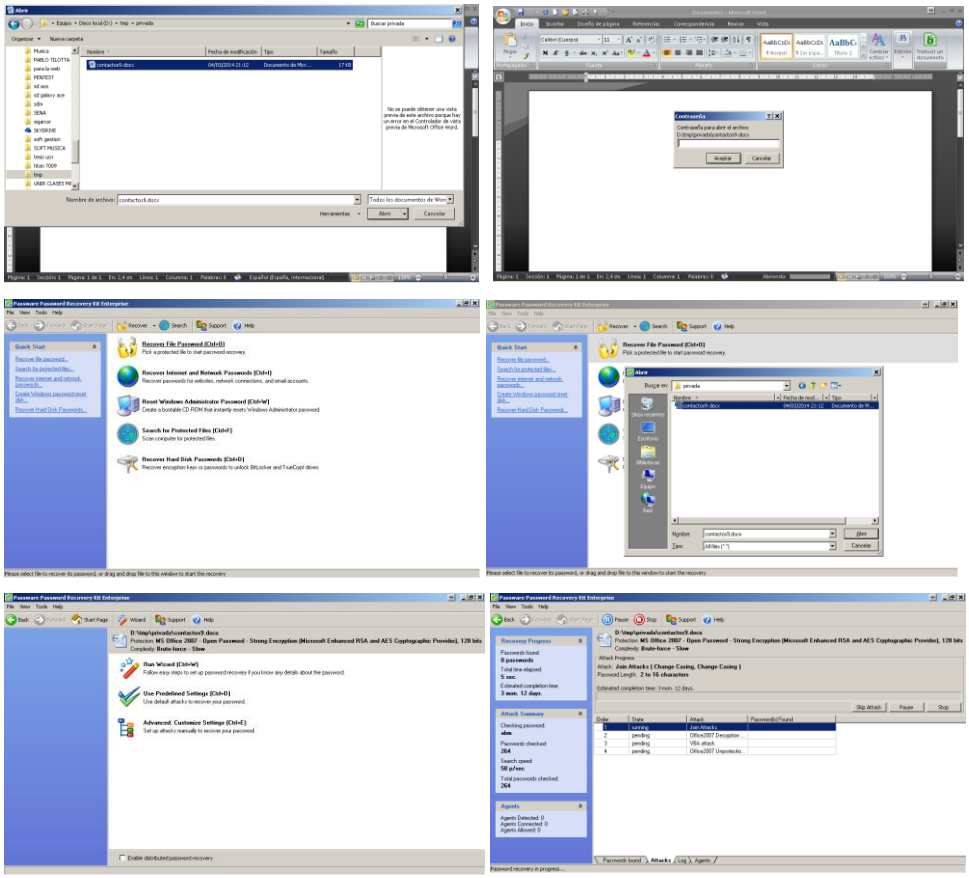
3433 su
3435 xchat
…..
4041 su
4042 xchat

Examinamos el archivo volcado de la memoria RAM del archivo atacado, la analizamos con el software WINHEX, y encontramos que en horas de la noche existe navegación a páginas para adultos y de chat.

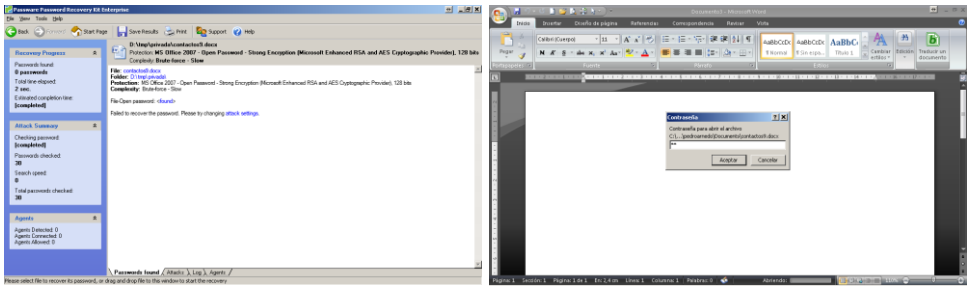




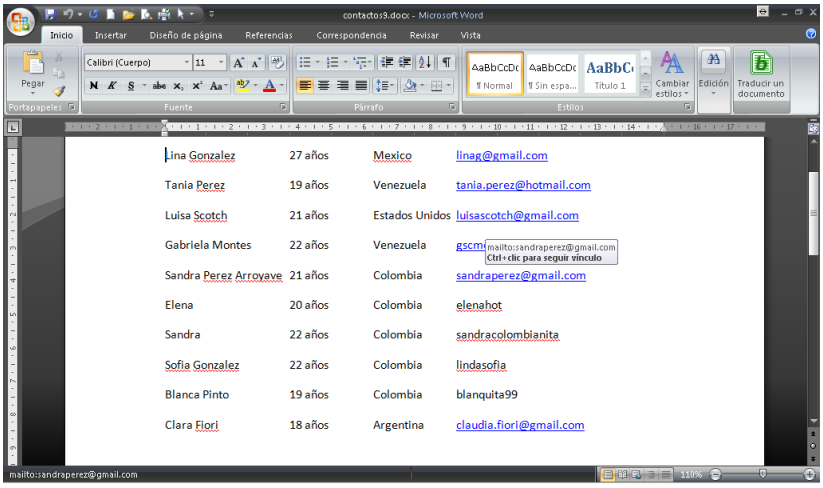
Encontramos un pendrive usb conectado al servidor, se analiza y entre otras cosas se ubica un archivo con el nombre amigoschat.doc, lo llevamos a un equipo con sistema Windows, se trata de abrir con el aplicativo ofimático Microsoft Word y no es posible porque está protegido con contraseña. Se ejecuta el software Passware, que se encarga entre otras cosas de descubrir las contraseñas en archivos ofimáticos protegidos.



Se ubica el documento protegido con contraseña, el software Passware descubre la contraseña, el cual es el número 14, solo dos caracteres, lo que facilito su fácil consecución.



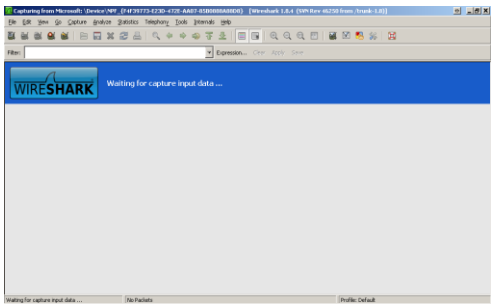
Abrimos el archivo y encontramos un documento con nombres, correos electrónicos y alias de personas. Se supone que son personas habituales a los foros de los canales activos en el programa *xchat*.



Investigamos con el jefe de personal y nos dice que en la noche solo se queda el vigilante. Que no hay más nadie dentro de las instalaciones de la entidad a esa hora.

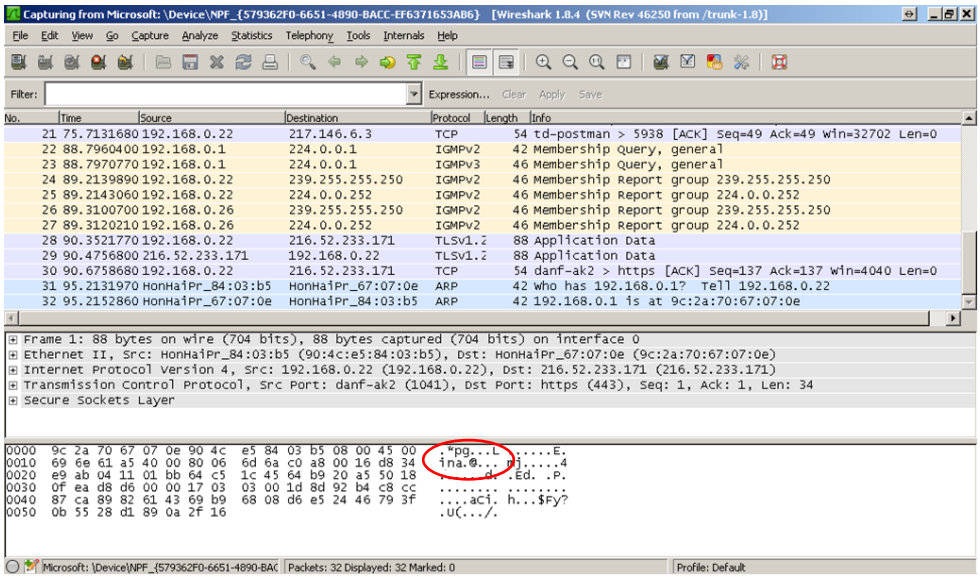
Le preguntamos al usuario afectado si existe la posibilidad de que el vigilante supiera la clave del usuario root del equipo afectado y reconoce que sí, que él se la dio un día para que consultara algo en internet ya que los demás computadores estaban ocupados.

Se ejecuta el software Wireshark y se deja activo toda la noche, para que capture el tráfico que se en la red en esas horas.



Al día siguiente se analiza el tráfico y se encuentran trazas con los nombres de los contactos registrados en el archivo de Word, desprotegido anteriormente. Se concluye que esa noche el vigilante volvió a ingresar a la plataforma de Chat XCHAT, confirmando que es él la persona que por su actuación indebida, ingresando desde el servidor a

portales web peligrosas, ha propiciado el incidente de seguridad al servidor, aunado a la falta de gestión en la seguridad del servidor por parte de la persona responsable de ello.



Se concluye que a través del programa de chat, alguien logro detectar la dirección ip y penetrar el sistema por tener un usuario root con una contraseña trivial. Se deduce que debieron utilizar un software de ataque por fuerza bruta, ya que el día del incidente se dieron más de dieciséis intentos de conexión fallidos, antes de la conexión satisfactoria utilizando el protocolo ssh.

3.2. Delito Informático – Incidente DELINF0957.

Una empresa internacional de refrescos se ve afectada en la confidencialidad de su información, al llegar a los correos corporativos del nivel directivo amenazas de hacer circular información secreta y confidencial relacionada con su lógica de negocio. Se trata de una extorsión que consiste en pedir, por parte del o de los extorsionistas, una suma considerable de dinero a esta empresa o de lo contrario se dará a conocer a la competencia su formula líder del mercado en cuanto a refrescos se refiere, producida en exclusiva por ella.

Se requiere investigar el origen del incidente, posibles delincuentes, herramientas informáticas utilizadas, fallas que permitieron el robo de información y correcciones a corto plazo.

3.2.1. Investigación Forense.

El día 22 de noviembre de 2013 los directivos de la empresa “Gaseosas del Caribe” de Valledupar (Colombia) encuentran cada uno a primera hora de la mañana en sus correos electrónicos corporativos, una serie de mensajes provenientes de un emisor con nombre “Señor Formula” y correo electrónico señorformula@hotmail.com, solicitando una fuerte suma de dinero a cambio de no divulgar la formula líder del mercado, en lo referente a un refresco gaseoso producido por la empresa. En este mensaje se adjunta un documento en formato Microsoft Excel donde se relaciona la formula exacta del producto afectado, la cual consiste en un listado de componentes, cantidades exactas de cada uno, diferentes tiempos de procesamiento y procesos exactos aplicados en la fabricación del producto, validando con total certeza la tenencia de esta fórmula secreta por parte de personal externo a la entidad y por ende no autorizado para ello.

Luego de pasadas las fases de análisis del problema, recolección de evidencias digitales y preservación de las mismas, continuamos con la fase de evaluación de estas evidencias.

Novedades encontradas en la consecución de este delito:

- La empresa no cuenta con servidor de correo propio. Utilizan el servicio de correo gratuito de Yahoo para sus correos institucionales. Todos los empleados sin excepción cuentan con su correo en Yahoo. Por políticas de la empresa es de carácter obligatorio contar con un correo electrónico y es obligatorio que el mismo sea del proveedor de correos gratuitos Yahoo.

Evidencias digitales adquiridas en la consecución de este delito

- Mensajes de correo electrónico de cada empleado del nivel directivo donde llegaron las extorsiones.

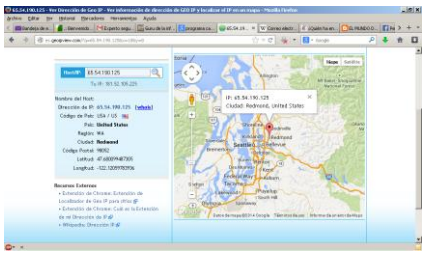
- Archivo adjunto en formato Microsoft Excel, donde se relaciona la formula violentada.

Procedimiento Realizado:

Se revisa el correo electrónico de cada empleado del nivel directivo donde llegaron los correos en investigación. Se analiza su cabecera y se determina que provienen de ls siguiente ip:

X-Originating- [65.54.190.125]
Authentication-Results:mta1419.mail.gq1.yahoo.com from=hotmail.com; domainkeys=neutral (no sig); from=hotmail.com; dkim=neutral (no sig)
from BAY169-W11 ([65.54.190.125]) by bay0-omc2-s15.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675); Fri, 22 Nov 2013 08:22:19 -0800
X-Originating-Email: [señorformula@hotmail.com]

Se rastrea la dirección ip para ver su procedencia a través del portal es.geoipview.com



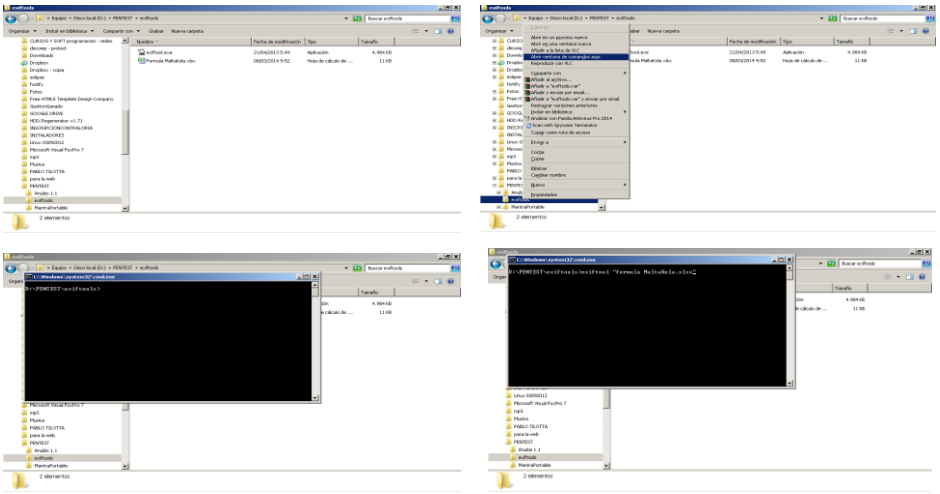
Lo que arroja una dirección de algún servidor del proveedor gratuito Hotmail en los Estados Unidos. Se concluye que el estafador no utilizó un servicio corporativo rastreable.

Se descarga el archivo adjunto que llegó en el correo electrónico extorsivo y se sacan dos copias al mismo.

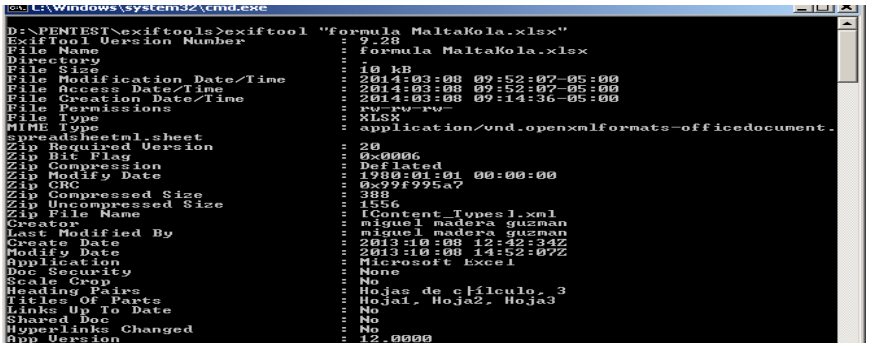
Examinamos el archivo descargado, al cual previamente se le hizo un resumen hash y luego se sacaron dos copias de seguridad, de nuevo se validan por hash, Todo el proceso correcto.

Se ejecutará el software **exiftools**, el cual será utilizado para el análisis de metadatos en el documento descargado.

Para ello se mueve a la carpeta donde se encuentra el software exiftools el archivo en Excel. Este software se ejecuta en modo consola.



Luego de analizado el archivo con el software exiftool, este arroja los siguientes metadatos:



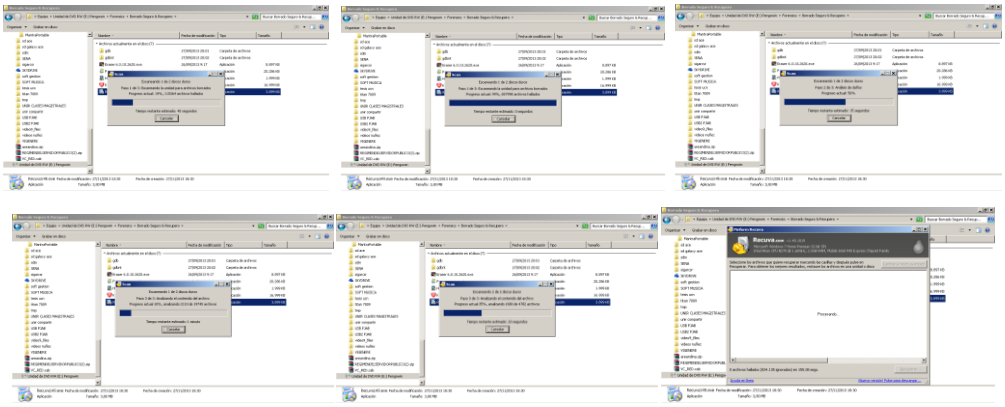
- Autor: miguel madera guzmán.

- Fecha de elaboración: Octubre 8 de 2013.

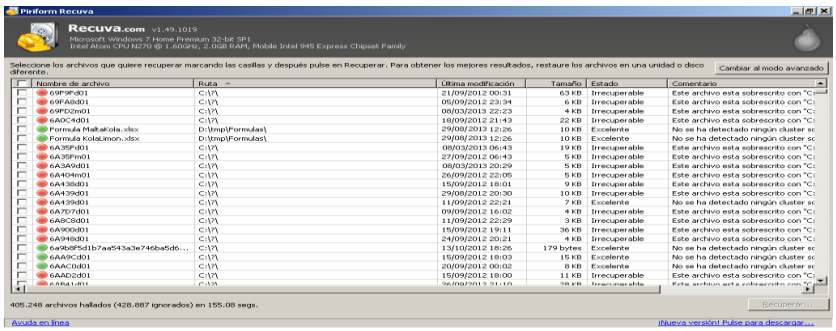
Se solicita información en el área de recursos humanos de la empresa “Gaseosas del Caribe” acerca del nombre arrojado en los metadatos y se obtiene información relevante. El señor Miguel Madera Guzmán es un ex empleado de la empresa, el cual fue despedido en el mes de septiembre del año 2013. El documento elaborado en Excel y utilizado para la extorsión vía correo electrónico fue elaborado en un equipo con el software ofimático registrado a su nombre, lo que lo ubica como principal sospechoso del delito.

Ubicamos el computador asignado a este señor cuando laboraba para la entidad, tiene Windows 7 como sistema operativo instalado, tratamos de entrar a su sesión con su cuenta de usuario aun existente en este computador “mmaderag “ y nos pide contraseña. Le solicitamos al jefe de sistemas que entre como usuario administrador y trate de cambiar la contraseña del usuario “mmaderag”. El jefe de sistema nos colabora y establece una nueva contraseña, la cual queda **abc123**. Con esta contraseña logramos entrar al usuario, se observa con el explorador de Windows que solo tiene una partición (unidad C), revisamos todas las carpetas en el directorio raíz y las propias de su biblioteca de carpetas asociada a su usuario, como son mis documentos, mis imágenes, escritorio, etc. Todas se encuentran vacías.

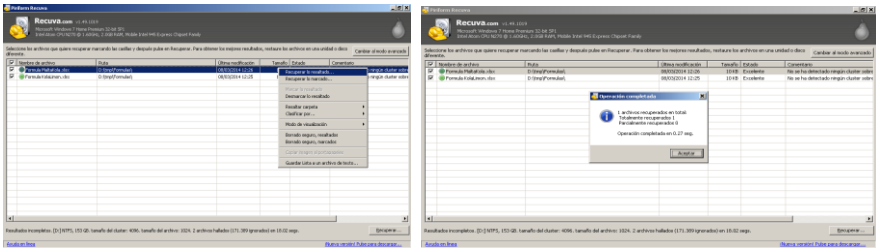
Utilizaremos el programa RECUVA para tratar de recuperar archivos eliminados en este equipo.



Luego de analizar los resultados de todos los archivos detectados por el aplicativo RECUVA nos encontramos con la siguiente evidencia:

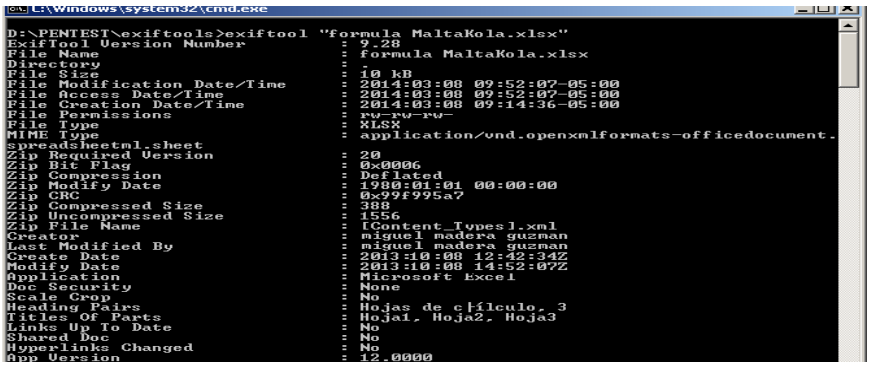


Dos archivos borrados con fecha 29 de agosto de 2013, unos días antes de ser despedido el señor Madera Guzmán, en la ubicación d:\tmp\Formulas, con los siguientes nombres: “Formula MaltaKola” y “Formula KolaLimon”, siendo la primera la utilizada en la extorsión que es investigada.



Se procede a recuperar los archivos. Luego de esto se analiza el archivo objeto de investigación denominado “Formula MaltaKola.xlsx” con el programa extractor de metadatos Exiftools, arrojando los mismos resultados

que los brindados con el archivo enviado adjunto para coadyudar a la extorsión.



Cabe anotar que el señor Madera Guzmán es de profesión Químico y tenía acceso al laboratorio de la empresa y a los equipos de cómputo de esta área donde se alojaban esta fórmulas, pero no tenía autorización de manejar esta documentación en computadores fuera de este laboratorio.

Con esto se concluye que el señor Miguel Madera Guzmán tenía en su poder información confidencial de la empresa con la que trabajaba. Que el documento que se recuperó después de su borrado en su computador es el mismo que enviaron por correo electrónico para extorsionar a los directivos de la empresa. Se concluye que él es autor material e intelectual del delito extorsivo.

3.3. Delito Informático – Incidente DELINF0998.

Una empresa nacional dedicada a la venta al por mayor de ropa femenina, se ve afectada en la integridad y confidencialidad de su información y posiblemente en la solidez de sus finanzas, ya que el 8 de noviembre de 2013 le intentan hacer un fraude por la suma de doscientos cincuenta millones de pesos en mercancía a través de internet.

Se requiere investigar el origen del incidente, posibles delincuentes, herramientas informáticas utilizadas, daños ocasionados, fallas que permitieron el ilícito y correcciones a corto plazo.

3.3.1. Investigación Forense.

La empresa “RopaFina” dedicada a la venta al por mayor de ropa femenina, se ve afectada en la integridad y confidencialidad de su información y en la solidez de sus finanzas, ya que el 8 de noviembre de 2013 recibe un correo de uno de sus clientes minoritarios, el señor Pedro Amira, representante legal de la empresa “Area-Femme”, donde solicita doscientos cincuenta millones de pesos en mercancía y adjunta como soporte el recibo de consignación bancaria correspondiente al pago del negocio. Este procedimiento se viene realizando de esta forma con este cliente desde hace cinco años sin inconveniente alguno.

El comprador solicita se envíe la mercancía a una dirección física la cual se notó no estaba entre las que usaran normalmente, pero se justificó con la ampliación de sedes por parte de la misma. Esto genero sospecha, ya que los directivos de “Area-Femme” acostumbran a socializar con sus proveedores cualquier cambio que afecte su lógica de negocio y hasta ese momento no había llegado información de nueva sede o traslado alguno de su parte.

Se llama a la empresa que realizó la compra, “Area-Femme”, procedimiento que se hace para validar la negociación. Al realizar esta llamada se descubre que esta empresa no ha solicitado mercancía alguna y por ende no ha hecho consignación alguna. Inmediatamente se verifican las transacciones bancarias y efectivamente no existe ingreso por esa cantidad. Se desvirtúa la legalidad del recibo de consignación que llego adjunto al correo electrónico Se verifica la dirección donde se debería enviar la mercancía, por parte de personal de la empresa “Area_Femme” en la ciudad donde se ubican, específicamente la ciudad de Montería, y se descubre que el sitio corresponde a un local alquilado, el cual se encuentra desocupado.

Novedades encontradas en la consecución de este delito:

- La empresa “RopaFina” no cuenta con servidor de correo propio. Utilizan el servicio de correo gratuito de Yahoo para sus negocios. Tienen un solo correo electrónico donde manejan sus negocios, denominado “ropafinavalledupar@yahoo.com”.

Evidencias digitales adquiridas en la consecución de este delito

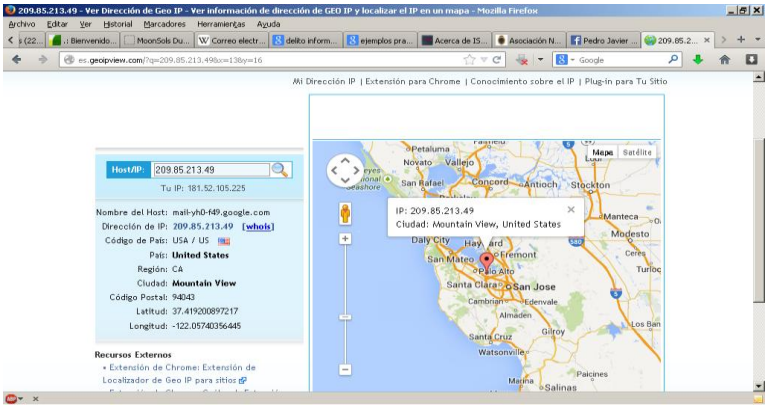
- Mensaje de correo electrónico donde llego el mensaje fraudulento.
- Archivo adjunto en formato PDF, donde se soporta la transacción bancaria fraudulenta.

Procedimiento Realizado:

Se revisa el correo electrónico donde llegó el correo fraudulento. Se verifica su autenticidad y se observa que tiene un nombre similar al original, con un cambio casi imperceptible. El correo de la empresa minorista es “area_femme@hotmail.com” y el utilizado para el fraude es “area_femme.@hotmail.com”. Se analiza su cabecera y se determina que provienen de la siguiente ip:

X-Originating- [209.85.213.49]
Authentication-Results:mta1419.mail.gq1.yahoo.com
from=hotmail.com; domainkeys=neutral (no sig); from=hotmail.com; dkim=neutral (no sig)
from BAY169-W11 ([209.85.213.49]) by bay0-omc2-s15.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675) Fri, 8 Nov 2013 15:20:17 -0800
X-Originating-Email: [area_femme@hotmail.com]

Se rastrea la dirección ip para ver su procedencia a través del portal es.geoipview.com



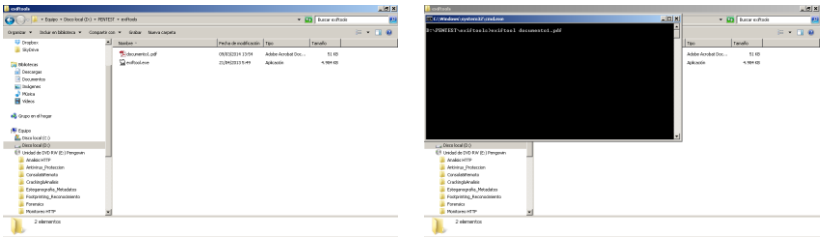
Lo que arroja una dirección de algún servidor del proveedor gratuito Hotmail en los Estados Unidos. Se concluye que el estafador no utilizó un servicio corporativo rastreable.

Se procede con descargar el archivo adjunto que llegó en el correo electrónico fraudulenta y se sacan dos copias. Este archivo tiene formato PDF.

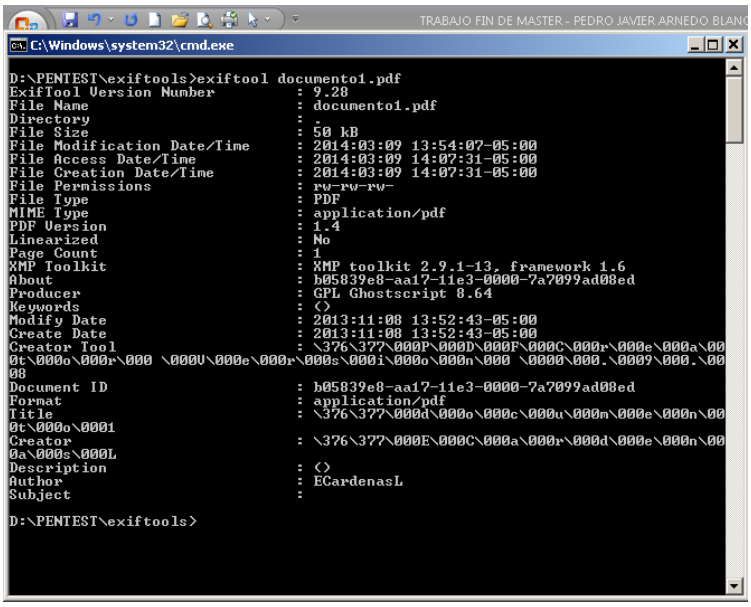
Examinaremos el archivo descargado, a la que previamente se le hizo un resumen hash y luego se sacaron dos copias de seguridad, de nuevo se validan por hash cada copia, Todo el proceso resulta correcto.

Se ejecutará el software **exiftool**, el cual será utilizado para el análisis de metadatos en el documento descargado.

Para ello se mueve a la carpeta donde se encuentra el software exiftools el archivo en Excel. Este software se ejecuta en modo consola.



Luego de analizado el archivo con el software exiftool, este arroja los siguientes metadatos:



- Autor: ECardenasL.

- Fecha de elaboración: Noviembre 8 de 2013.

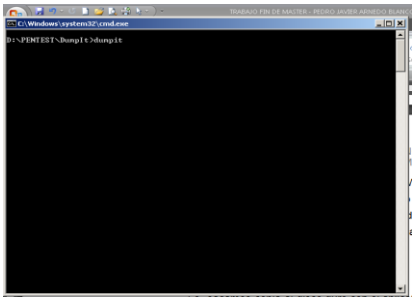
Se solicita información a la compañía “Area-Femme” con relación al seudónimo o usuario extraído de los metadatos del archivo pdf y se nos informa que ese usuario corresponde al empleado Ernesto Cárdenas Lozada, quien es un empleado activo de la empresa.

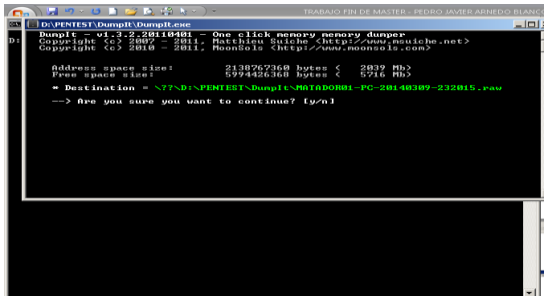
Los directivos de la empresa “Area-Femme” se reúnen con el empleado Ernesto Cárdenas y le solicitan explicación de los hechos. Dice que no tiene conocimiento de nada de lo que le exponen.

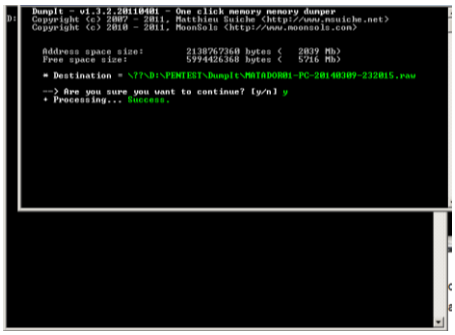
Nos trasladamos a la ciudad de Montería donde tiene la sede la empresa “Area-Femme” y ya en la compañía ubicamos el computador asignado a este empleado.

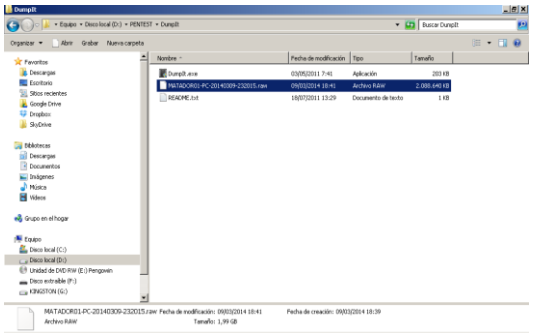
El computador tiene el sistema operativo Windows 7 instalado, este se encuentra encendido. Hacemos un volcado de memoria con el software DumpIT. Lo hacemos con este software porque consume solamente 97Kb de recursos, lo que permite que se altere de forma mínima la memoria del equipo investigado.

Luego de realizado el volcado se hace el respectivo hash al archivo, se sacan dos copias y se hace un hash a cada una. Se validan los resultados y las copias quedaron perfectas.

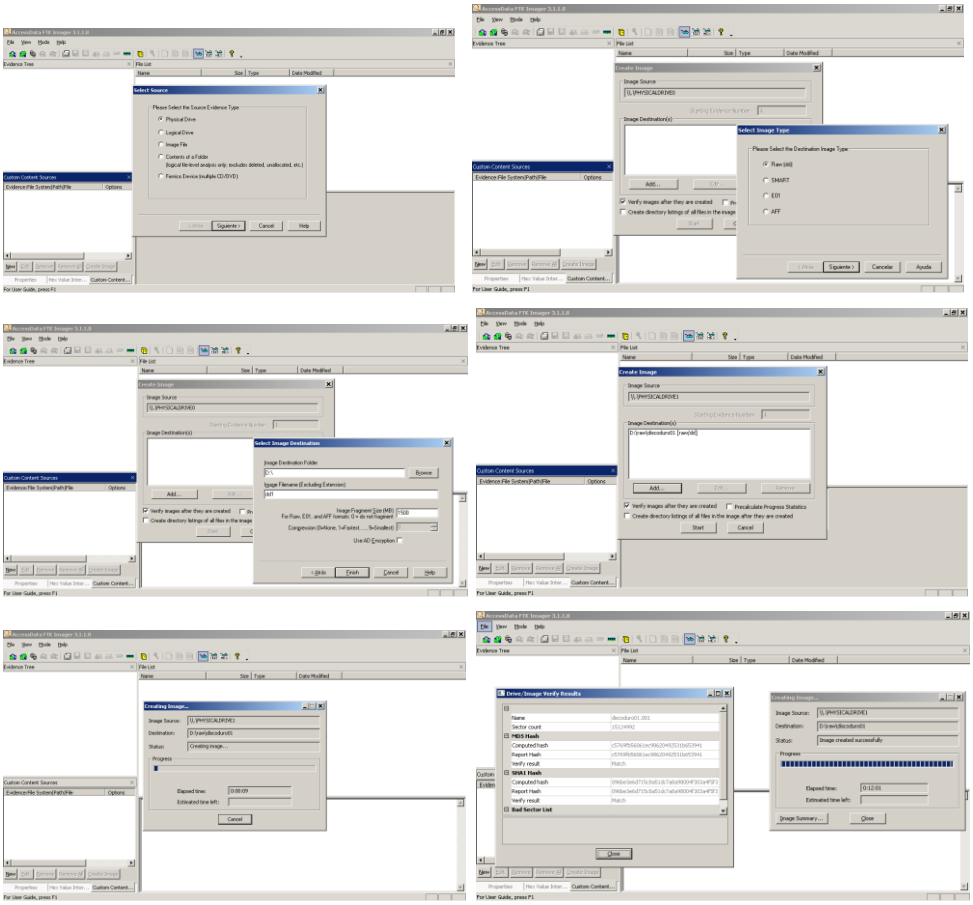




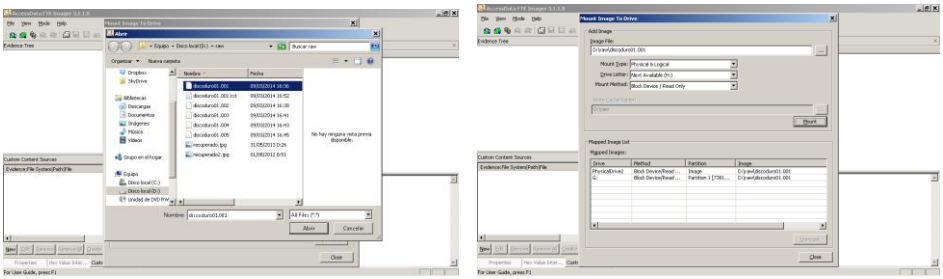




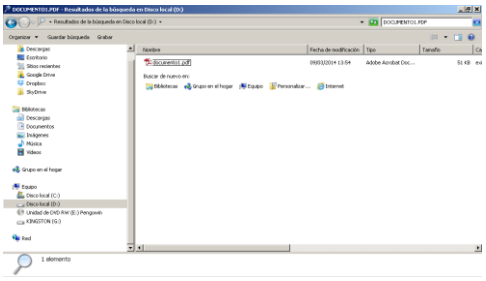
Le sacamos copia al disco duro con el aplicativo FTK Imager, se sacan dos copias y se hace un hash a cada uno. Se validan los resultados y las copias quedan correctas.

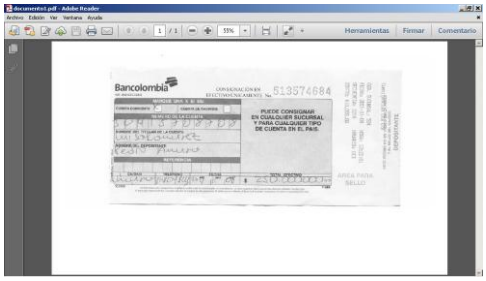


Nos trasladamos al computador donde revisaremos la imagen del disco, hacemos el montaje respectivo de una de las imágenes y procedemos a hacer una búsqueda por nombre, tratando primero que todo de localizar un documento de nombre documento1.pdf.



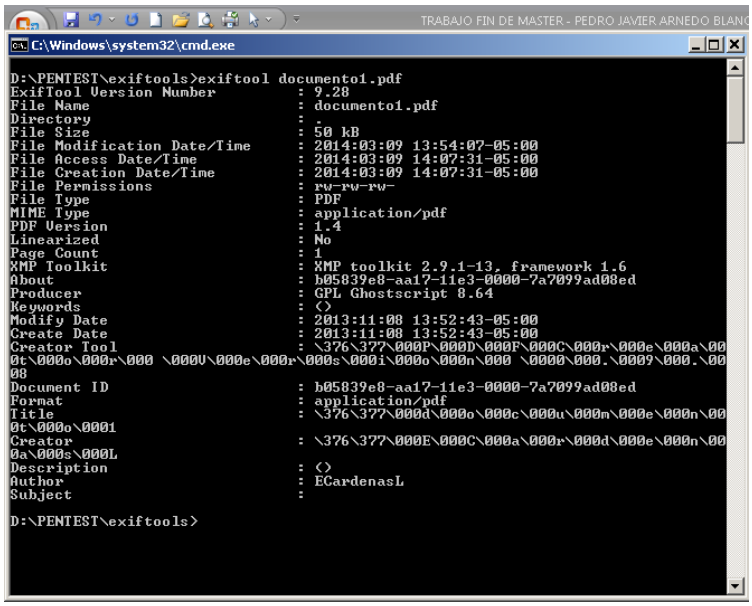
Se ubica en el disco montado con la imagen del disco duro del empleado sospechoso y efectivamente arroja un único archivo con ese nombre. Seguido procedemos a abrirlo.



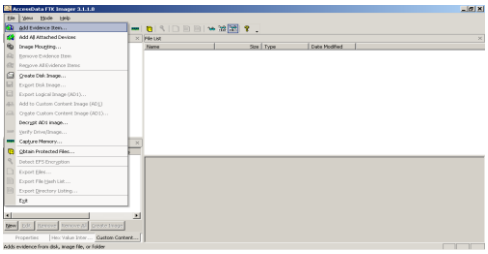


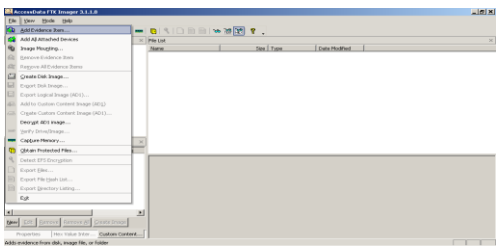
Efectivamente concuerda con el archivo utilizado como prueba para efectuar el fraude.

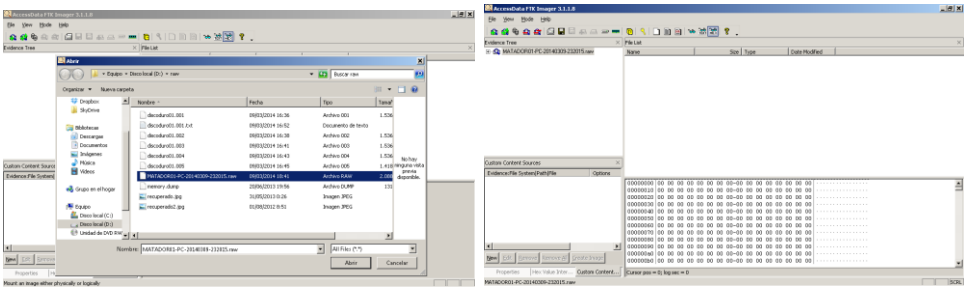
Se comprueba nuevamente con el software Exiftool arrojando los mismos resultados.



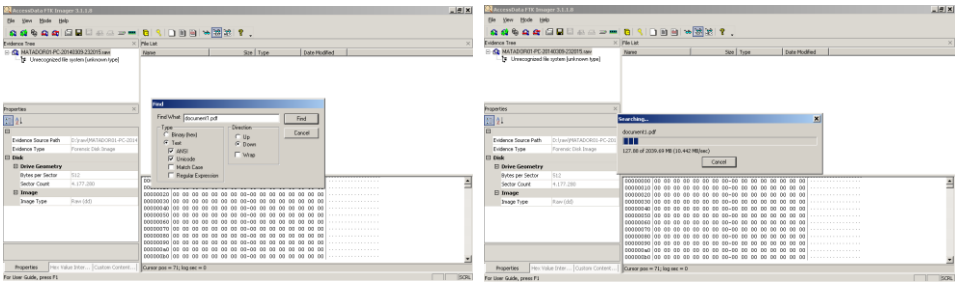
Ahora montamos el archivo con el volcado de memoria realizado al computador del señor Cárdenas Lozada. Esto lo hacemos en el equipo que utilizaremos en la investigación forense, con el software FTK Imager.



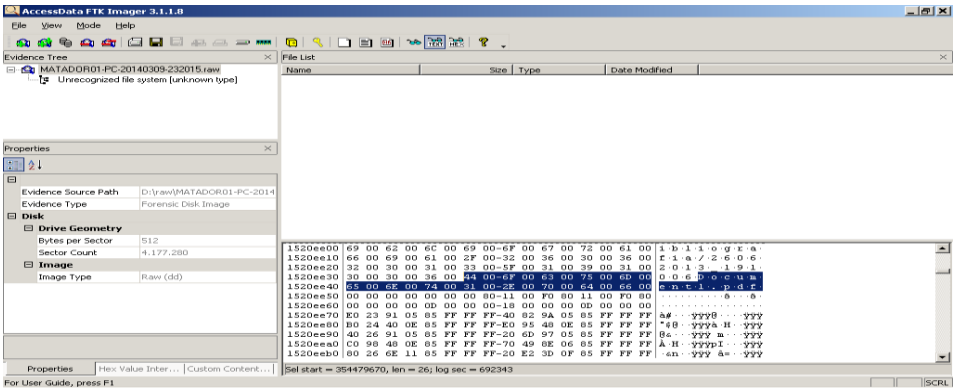




El software FTK Imager nos abre una interfaz tipo editor binario (hexadecimal), lo cual nos permite proceder a buscar en memoria el nombre documento1.pdf, para ver si el señor Cárdenas Lozada estaba trabajando en ese documento al momento de llegar a su oficina.



Efectivamente se encuentran indicios de haber trabajado con el documento document1.pdf.



Se concluye que el empleado Ernesto Cárdenas Lozada pretendía estafar a la empresa “Ropa Fina” tratando de obtener de ella una suma considerable en mercancías, aprovechándose de datos obtenidos en la empresa “Area_Femme” donde labora.

3.4. Aportes Herramientas de Software Aplicadas en Incidentes de Seguridad Informática.

Se puede observar con el análisis de los incidentes anteriormente expuestos la invaluable importancia de las herramientas de software enfocadas a la investigación informática forense. El aporte para la consecución de pruebas con base a evidencias digitales es relevante.

En el caso **Incidente DELINF0951** se utilizaron las siguientes herramientas de software:

Software	Tipo	Interfaz	Facilidad de uso	Funcionalidad	Recomendado
DumpIT	Volcado Memoria	Consola	Fácil	Objetivo exitoso	Si
DD	Clonación	GUI	Fácil	Objetivo exitoso	Si
Ftk Imager	Suite (Copias a imagen, Volcado Memoria, Editor Hexadecimal, entre otras)	GUI	Algo difícil	Objetivo exitoso	Si
WinHex	Editor Hexadecimal, Volcado de memoria	GUI	Fácil	Objetivo exitoso	Si
Passware	Recuperador de contraseñas, Desbloqueador de protección	GUI	Algo difícil	Objetivo exitoso	Si
Wireshark	Analizador de protocolos, Sniffer	GUI	Difícil	Objetivo exitoso	Si

En el caso **Incidente DELINF0957** se utilizaron las siguientes herramientas de software:

Software	**Tipo**	**Interfaz**	**Facilidad de uso**	**Funcionalidad**	**Recomendado**
Geolocalizador ONLINE: es.geoipview.com	GPS, Localización	WEB	Fácil	Objetivo exitoso	Si
Exiftool	Extracción Metadatos	Consola	Difícil	Objetivo exitoso	Si
Recuva	Recuperación de Archivos	GUI	Fácil	Objetivo exitoso	Si

En el caso **Incidente DELINF0998** se utilizaron las siguientes herramientas de software:

Software	**Tipo**	**Interfaz**	**Facilidad de uso**	**Funcionalidad**	**Recomendado**
Geolocalizador ONLINE: es.geoipview.com	GPS, Localización	WEB	Fácil	Objetivo exitoso	Si
Exiftool	Extracción Metadatos	Consola	Difícil	Objetivo exitoso	Si
DumpIT	Volcado Memoria	Consola	Fácil	Objetivo exitoso	Si
Ftk Imager	Suite (Copias a imagen, Volcado Memoria, Editor Hexadecimal, entre otras)	GUI	Algo difícil	Objetivo exitoso	Si

En los incidentes anteriores solo se ha aplicado una mínima parte de una innumerable cantidad de aplicativos existentes tanto del orden comercial como no comercial (open source, GPL, Freeware, etc.). Por lo que cualquier investigador forense informático tiene un buen material disponible en internet para su descarga y puesta en uso.

Saber escoger el software indicado, según el caso de estudio, es fundamental para cualquier perito informático. Es por esto que, agrupando los aplicativos por categoría, se puede concluir que para algunas investigaciones será más apropiado usar un software en particular, pero en otras ocasiones tal vez ese software no sea el adecuado y se opte por otro con algunas prestaciones específicas, que estén acordes con el incidente que este siendo objeto de investigación.

Las herramientas de software informático forense ofrecen un servicio invaluable, ya que permiten al perito hacer sus procesos investigativos con mayor rapidez y fiabilidad.

Es impensable hoy en día no tener en cuenta la gran cantidad de herramientas disponibles en el mercado. Se invita a los peritos informáticos a esta constantemente descargando y probando las nuevas herramientas que se dan a conocer continuamente, para no dejar pasar un aplicativo que puede significar el lograr llevar con cabalidad una investigación forense.

CONCLUSIONES

La informática forense se ha venido fortaleciendo continuamente, en aras de contrarrestar el incremento progresivo del índice de incidentes de seguridad informática a nivel global y a la cada vez más sutil y avanzada forma de ataques informáticos.

En este documento, se ha dejado plasmado con total profesionalismo y un alto nivel de investigación, todo lo referente a la utilización práctica de herramientas de análisis forense y su efectividad real al momento de obtener resultados probatorios válidos en una investigación, en conjunción con la aplicación de diversas metodologías forenses estudiadas en este mismo documento.

Como aporte relevante, se concluye que existen varias metodologías completamente válidas para la investigación informática forense y cualquiera que se seleccione para una investigación, después que se le dé la aplicabilidad correcta, permitirá alcanzar los objetivos planteados.

Es importante decir que tanto el aporte académico como el aporte técnico / operativo de este trabajo es de gran valor, no solo para la comunidad involucrada en el área de la informática forense, sino también para la comunidad en general, quien puede documentarse con todo lo aquí expuesto y asimilar fácilmente lo que se está comunicando, gracias a la forma detallada y grafica del texto escrito, aunado a un lenguaje técnico y sencillo.

De igual forma se concluye que en el mercado existe una nutrida cantidad de herramientas de software, de gran calidad y aporte técnico, que se pueden utilizar para estas investigaciones. Además de que con el día a día siguen apareciendo nuevas herramientas, resaltando que tanto las comerciales como las no-comerciales (open source GPL, freeware, etc.) ofrecen una excelente calidad en sus prestaciones.

REFERENCIAS BIBLIOGRAFICAS

Álvarez Marañón, Gonzalo & Pérez García, Pedro Pablo. (2004). *Seguridad informática para empresas y particulares*. España: McGraw-Hill.

Ashcroft, John & Daniels, Deborah & Hart, Sara. (2004). *Forensic examination of digital evidence. A guide for law enforcement*. Washington: US Department of Justice.

Berdinelli, Maximilianot. (2012). *Evidencia digital: la informática forense crece como aliada de los procesos judiciales*. Recuperado Diciembre 07 de 2013 de http://www.iprofesional.com/notas/139289-Evidencia-digital-la-informtica-forense-crece-como-aliada-de-los-procesos-judiciales

Cano José, Jeimy. (2005). *Evidencia Digital: Conceptos y Retos*. Bogotá: Legis.

Casey, Eoghan. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Miami: Academic Press.

Cyber and information Security Research. *Models of Models: Digital Forensics and Domain-Specific Languages*. Recuperado el 06 de diciembre de 2013 de http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf

Domínguez, Antonio. (2012). *IEF (buscador de evidencias) de JADsoftware compatible con los servicios en la Nube*. Recuperado el 17 de diciembre de 2013 de http://adfinformaticaf.wordpress.com/2012/05/25/ief-buscador-de-evidencias-de-jadsoftware-compatible-con-los-servicios-en-la-nube/

Guirado, Rodrigo. (2009). *Penetration Testing: Conceptos Generales y Situación Actual*. Uruguay: PriceWaterHouseCoopers - ISACA Chapter.

Martínez, Roberto. (2012). *La importancia de la evidencia y el análisis forense digital*. http://www.bsecure.com.mx/opinion/la-importancia-de-la-evidencia-y-el-analisis-forense-digital/

Microsoft. (2013). *Qué es la carpeta Prefetch*. Recuperado el 15 de diciembre de 2013 de http://windows.microsoft.com/es-co/windows-vista/what-is-the-prefetch-folder

Moura, William. (2012). *Evidencia Digital en Colombia: Una reflexión en la práctica*. Recuperado el 7 de diciembre de 2013 de http://www.egov.ufsc.br/portal/conteudo/evidencia-digital-en-colombia-una-reflexi%C3%B3n-en-la-pr%C3%A1ctica

Naranjo, Alice. (2009). *Conceptos de la auditoria de sistemas*. Argentina: El Cid Editor.

Real Academia Española. (2001). *Informática*. En Diccionario de la lengua española (22.a ed.). Recuperado de http://lema.rae.es/drae/?val=inform%C3%A1tica

Rivas, Gonzalo Alonso. (1988). *Auditoría Informática*. España: Ediciones Díaz de Santos S.A.

Sánchez, Antonio. (2010). File Carving. Recuperado el 09 de diciembre 2013 de http://blog.elhacker.net/2010/04/file-carving.html

Sergio, Hernando. (2014). *Análisis forense con Digital Forensics Framework (DFF).* Recuperado el 15 de diciembre de 2013 de www.sahw.com/wp/archivos/2011/01/11/analisis-forense-con-digital-forensics-framework-dff/

Wikipedia. (2013). *Delito*. Recuperado el 05 de diciembre de 2013 de http://es.wikipedia.org/wiki/Delito

Wikipedia. (2013). *Delito Informático*. Recuperado el 05 de diciembre de 2013 de http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Wikipedia. (2013). *Vulnerabilidad Informática*. Recuperado el 05 de diciembre de 2013 de http://es.wikipedia.org/wiki/Vulnerabilidad#En_inform.C3.A1tica

Wikipedia. (2013). *Seguridad*. Recuperado el 05 de diciembre de 2013 de http://es.wikipedia.org/wiki/Seguridad

Wikipedia. (2013). *Informática Forense*. Recuperado el 05 de diciembre de 2013 de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense

Wikipedia.. (2013). *Seguridad informática*. Recuperado el 09 de diciembre de 2013 de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Wikipedia.. (2013). *Xen*. Recuperado el 09 de diciembre de 2013 de http://es.wikipedia.org/wiki/Xen