RESUMEN – TRABAJO DE GRADO

AUTOR	**GINA ALEJANDRA ARENIZ AREVALO**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**INGENIERIA DE SISTEMAS**
DIRECTOR	**LEONARDO DAVID LOBO PARRA**
TÍTULO DE LA TESIS	**DEFINICIÓN DE UNA METODOLOGÍA PRÁCTICA PARA LA ADQUISICIÓN Y ANÁLISIS DE EVIDENCIA DIGITAL EN EL CONTEXTO DE UN ANÁLISIS FORENSE ON LINE**

RESUMEN
(70 palabras aproximadamente)

LA PRESENTE INVESTIGACIÓN REALIZADA BUSCARÁ REVISAR LAS DIFERENTES FUENTES BIBLIOGRÁFICAS CON EL FIN DE OBTENER UNA METODOLOGÍA TEÓRICA O ESTÁNDAR QUE SIRVA COMO BASE PARA INICIAR CON EL ESTUDIO, POSTERIORMENTE SE REALIZARA UN ANÁLISIS DE LAS HERRAMIENTAS DISPONIBLES Y COMPATIBLES PARA EL ESTUDIO, PARA A PARTIR DE LAS HERRAMIENTAS Y SIGUIENDO LOS PASOS DE LA METODOLOGÍA TEÓRICA, ESTABLECER LAS ACTIVIDADES RECURRENTES EN CADA LABORATORIO PARA HACER CRUCE CON LOS ESTÁNDARES Y METODOLOGÍAS SELECCIONADAS INICIALMENTE PARA ASÍ DEFINIR LA METODOLOGÍA PROPIA.

CARACTERÍSTICAS

PÁGINAS: 119	PLANOS:	ILUSTRACIONES: 27	CD-ROM: 1

DEFINICIÓN DE UNA METODOLOGÍA PRÁCTICA PARA LA ADQUISICIÓN Y ANÁLISIS DE EVIDENCIA DIGITAL EN EL CONTEXTO DE UN ANÁLISIS FORENSE DIGITAL ON LINE

GINA ALEJANDRA ARENIZ ARÉVALO

Trabajo de grado presentado para optar el título de Ingeniero de Sistemas

Director

LEONARDO DAVID LOBO PARRA

Especialista en Auditoria de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERIAS

INGENIERIA DE SISTEMAS

Ocaña, Colombia **Mayo de 2016**

Índice

Resumen

La presente investigación realizara buscara revisar las diferentes fuentes bibliográficas con el fin de obtener una metodología teórica o estándar que sirva como base para iniciar con el estudio, posteriormente se realizara un análisis de las herramientas disponibles y compatibles para el estudio, para a partir de las herramientas y siguiendo los pasos de la metodología teórica, establecer las actividades recurrentes en cada laboratorio para hacer cruce con los estándares y metodologías seleccionadas inicialmente para así definir la metodología propia.

Introducción

La presente investigación pretende ilustrar el trabajo a realizar con respecto a la investigación “DEFINICIÓN DE UNA METODOLOGÍA PRÁCTICA PARA LA ADQUISICIÓN Y ANÁLISIS DE EVIDENCIA DIGITAL EN EL CONTEXTO DE UN ANÁLISIS FORENSE DIGITAL ON LINE”. El entorno de estudio es el laboratorio del semillero de investigación SIGLAS (Gnu Linux And Security) de la universidad Francisco de Paula Santander Ocaña; y fundamentalmente se busca diseñar una metodología con enfoque práctico para la realización del análisis digital forense en caliente, puesto que existen dos maneras para realizar dicha investigación. En primera instancia encontramos la metodología en caliente o en vivo, donde el equipo o terminal a analizar se encuentra encendida, y por consiguiente los programas en ejecución son visibles y la totalidad de la funcionalidad de la máquina, no obstante, también están latentes las trampas del atacante que pudieran dejar fuera de servicio el equipo u ocultar el ataque en sí mismo.

Capítulo 1. Definición de una Metodología Práctica para la Adquisición y Análisis de Evidencia Digital en el Contexto de un Análisis FORENSE ON LINE

1.1 Planteamiento del Problema

En los últimos años se ha hecho evidente el aumento de incidentes informáticos que van desde ataques a usuarios comunes conectados a la red hasta usuarios que poseen grandes sistemas de información generalmente a entidades importantes como las gubernamentales, así lo expreso la Cámara Colombiana de Informática y Telecomunicaciones, en entrevista realizada al Gerente de Operaciones de la Empresa Digiware (Digiware, http://www.digiware.net/), precisa que Colombia se encuentra en el noveno país en el mundo frente a delitos informáticos y el quinto a nivel Latinoamérica con crecientes problemas de seguridad informática, realiza su afirmación dado el crecimiento de la tecnología, el avance en la cobertura de internet y en la multiplicación de equipos tecnológicos. (CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES. DELITOS INFORMÁTICOS. 2014]

Adicionalmente, en su documento Avances y retos de la defensa digital en Colombia, (CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES. Avances y retos de la defensa digital en Colombia, Ed. noviembre de 2014) este mismo organismo indica que: Según un estudio realizado por la compañía MacAffe y la Organización de Estados Americanos (OEA), Colombia se posicionó como el sexto país en generar una mayor actividad maliciosa en línea para el año 2013. Por otro lado, en lo que respecta al costo, esta misma compañía estimó que el ciber- delito causó un daño económico al consumidor cercano a los 500 millones de dólares durante lo corrido de 2013,

acercándose así cada vez más a los país que reciben mayores ataques cibernéticos en el mundo; Hecho que deja en claro las falencias existentes en sistemas operativos y de seguridad implementados hoy en día, comprobando que ningún sistema de información es 100% seguro lo que conlleva a una pérdida importante de información que representa muchas veces derroches económicos, problemas sociales o políticos. Así entonces se hace necesario desarrollar métodos y aplicaciones que ayuden a contrarrestar el daño causado tras un ataque informático, todos estos elementos que enmarca el análisis forense (Lázaro, 2013. Introducción a la informática forense. España: RA-MA, 340 pp.) pueden volverse en muchas ocasiones una ardua labor, y bajo ciertas circunstancias como: condiciones internas de la organización, falta de conocimiento o inexistencia de estándares o buenas prácticas; y condiciones como: el desconocimiento o falta de leyes, hacen que el estudio se pueda volver incluso imposible. Esta imposibilidad no siempre viene determinada por la capacidad técnica sino por los requisitos legales exigibles a las evidencias (Acurio, 2009). Por ejemplo una de las condiciones clave en la recolección de evidencias es la asepsia, práctica que asegura que las pruebas recogidas no estén contaminadas, y que por tanto sean válidas para ser utilizadas en procesos judiciales, siguiendo una rígida cadena de custodia en todos sus pasos y completamente documentada.

En Colombia, la recolección de los elementos materiales probatorios permitidos tanto por el ente investigador como la defensa técnica del acusado, es definida como la igualdad de armas en un proceso penal. El descubrimiento de pruebas, el legislador colombiano lo definió en la etapa de juicio como aquella que tiene un carácter adversarial, pudiéndose realizar una confrontación entre las partes: el acusador y el acusado, de allí que la defensa, apoyándose en la

parte técnica, adicionalmente de controvertir las pruebas mismas, han descubierto que es más eficiente para su ejercicio, debatir la técnica y metodología. (CORTE CONSTITUCIONAL. 2014).

Basados en el principio de igualdad de armas, como la define la Corte Constitucional en sus diferentes pronunciamientos de la controversia de las pruebas, y en los desafíos que conlleva el combatir la delincuencia en Colombia, es que se generar la pregunta: ¿Cómo realizar auditoría al análisis forense que se práctica en Colombia?

De este cuestionamiento no solo en el contexto nacional sino que también en las esferas internacionales, surge la computación forense pues en el año 2003, la American Society of CrimeLaboratoryDirectors–LaboratoryAccreditationBoard (ASCLD–LAB) reconoce la evidencia digital y el análisis forense digital como una disciplina aceptada, en respuesta al creciente número de incidentes que comprometían la seguridad informática. No obstante y a pesar de los múltiples avances desde la fecha en el tema, aun así, distintas organizaciones como la Internet Engineering Task Force (IETF) (The Internet Engineering Task Force (IETF). [En línea] https://www.ietf.org), o la Organización Internacional para la Estandarización (ISO) (International Organization for Standardization. [En línea] www.iso.org.) y la Comisión Electrotécnica Internacional (IEC) (3), así como Policías (4) y Departamentos de Justicia (National Criminal Justice Reference Service. [En línea] https://www.ncjrs.gov) de varios países proponen varios documentos, en los que recogen alguna pautas y consejos para llevar a cabo este tipo de investigaciones, por su parte, investigadores como Brian Carrier y Eugene Spafford proponen una metodología de análisis digital basada en las fases que se documentan en las investigaciones de crímenes “físicos”, definen las etapas de preparación, identificación, despliegue, investigación y presentación; aun así esto no ofrece

ningunas luces a un analista sobre lo que puntualmente se debe hacer en el momento de analizar un incidente de seguridad informática (Brian Carrier, Eugene Spafford. 2003)

1.2 Formulación del Problema

¿Existe una metodología que sirva como lineamiento para la implementación de un análisis forense ON LINE?

1.3 Justificación

En los últimos años se ha visto un incremento en los ataques informáticos a objetivos tan diversos como personas particulares, entidades financieras o agencias gubernamentales de tal forma que se ha aumentado la vulnerabilidad de muchos sistemas; por esta razón, se ha visto la necesidad de desarrollar e implementar diversas técnicas que permitan hacer un correcto análisis forense digital. Cuando suceden los ataques y la seguridad informática falla, es necesario evaluar los ataques, ya sea para propósitos judiciales o para analizar los motivos por los cuales se vulneró el sistema con el fin de mejorar la seguridad. Este análisis se puede realizar en las modalidades on line y post – mortem, presentando cada una ventajas y desventajas; en este proyecto, se utilizará el análisis informático forense post – mortem, con el fin de evaluar el daño o las implicaciones causados por cierto ataque informático mediante el uso de varias metodologías preestablecidas.

1.4 Objetivos de la Investigación

1.4.1 General.

- Definir de una metodología práctica para la adquisición y análisis de evidencia digital en el contexto de un análisis forense digital ON LINE

1.4.2 Específicos

- Analizar las diferentes metodologías teóricas existentes con el fin de seleccionar una de ellas para la evaluación de un ataque informático.

- Implementar el análisis forense digital ON LINE a través de las distintas herramientas y técnicas de adquisición y análisis de datos de un dispositivo de almacenamiento.

- Evaluar el potencial desempeño del análisis forense digital ON LINE en ataques informáticos estableciendo el alcance y las implicaciones de las actividades ilícitas realizadas por un intruso en un sistema.

- Proponer y documentar una metodología estructurada específica y práctica para la aplicación del análisis digital forense digital ON LINE.

Es fundamental a la hora de realizar un medición y estructuración de la consecución de los anteriores objetivos, el trazar actividades e indicadores y permitan establecer la efectividad en dicho proceso. Para tal efecto se propone el siguiente esquema:

Tabla 1.

Descripción de las actividades

OBJETIVO	ACTIVIDAD	INDICADOR	DESCRIPCION
Análisis de las diferentes metodologías teóricas existentes con el fin de seleccionar una de ellas para la evaluación de un ataque informático	Revisión en base de datos y estudio de metodologías	Listado de metodologías	Se realizará una búsqueda a través de las diferentes fuentes como libros, artículos, revistas científicas y fuentes electrónicas bibliográficas, con el fin de establecer cuales cumplen los requerimientos del presente estudio.
	Comparación, evaluación y selección de la/las metodologías	Cuadro comparativo	En este cuadro se obtendrá una visión más amplia sobre las diferencias, ventajas y desventajas de cada una de las metodologías.
	Selección de la metodología	Metodología escogida	Se obtendrá una metodología que servirá como base en la investigación.
Implementación el análisis forense ON LINE a través de las distintas herramientas y técnicas de adquisición y análisis de datos de un dispositivo de almacenamiento	Búsqueda de herramientas software	Consulta bibliográfica	Se realizará una búsqueda a través de las diferentes fuentes electrónicas para obtener software ya sea libre o propietario.
	Comparación y evaluación de software	Cuadro comparativo	En este cuadro se obtendrá una visión más amplia sobre las diferencias, ventajas y desventajas de cada una de las herramientas seleccionadas.
	Estudio de herramientas seleccionadas	Herramientas de apoyo	Selección de la o las herramientas que servirán de apoyo para el desarrollo de la investigación.
	Diseño del ataque informático controlado	Documentación, selección y montaje de los escenarios de estudio	Se plantearan escenarios que sirvan como base para la realización del análisis forense.
	Implementación del ataque informático controlado	Retos forenses y ataques controlados	Se realizará el ataque informático para obtener el análisis forense deseado
Evaluación del potencial desempeño	Documentación de los escenarios de estudio tomando como base	Informes preliminares de los escenarios de estudio	Una vez realizados los ejercicios de intrusión, ataque o retos forense, se realizara la

del análisis forense ON LINE en ataques informáticos estableciendo el alcance y las implicaciones de las actividades ilícitas realizadas por un intruso en un sistema	las metodologías teóricas seleccionadas		documentación de todos los elementos importantes dentro del incidente
	Análisis de la evidencia recolectada	Evidencia recolectada e hipótesis inferidas	Tras analizar las evidencias recolectadas se tratara de identificar el origen e implicaciones del incidente de seguridad.
	Determinación de la efectividad del análisis	Comparación de las hipótesis y evidencia recolectada con el ataque realizado	Tomando como base el ataque realizado se definirá si el análisis logro establecer el origen e implicaciones del incidente de seguridad.
Propuesta y documentación de una metodología estructurada específica y práctica para la aplicación del análisis digital forense ON LINE	Identificación de los procedimientos recurrentes en cada uno de los análisis realizados	Fases preliminares de la metodología.	Dentro de cada uno de los casos de estudio se determinaran y agruparan el conjunto de actividades comunes a cada una.
	Comparación entre la metodología teórica escogida y las fases preliminares identificadas en la actividad anterior.	Esquema comparativo	Tomando las fases preliminares como procedimientos prácticos se buscara encajarlas en los conceptos teóricos que la metodología escogida proporciona.
	Documentación de la metodología práctica.	Documento final	Exposición y sustentación de la investigación y propuesta realizada.
	Publicaciones	Entrega de documentación	Se entregan los documentos requeridos por la UFPSO

Fuente: Autor del proyecto

1.5 Delimitaciones

1.5.1 Geográfica. El proyecto se llevar a cabo en las instalaciones de la Universidad Francisco de Paula Santander de Ocaña, específicamente en el semillero de investigación SIGLAS**.**

1.5.2 Conceptuales. La presente propuesta estudiara el análisis forense digital en su modalidad ON LINE, se usara las herramientas de software libre y se empleara como

referente los estándares internacionales y conceptos de análisis forenses y ataques informáticos.

1.5.3 Temporales. El proyecto tendrá un tiempo de realización de 36 semanas, de acuerdo a las actividades a realizar.

1.5.4 Operativas. La temática a desarrollar dentro de la presente propuesta ya se ha venido trabajando en la Universidad Francisco de Paula Santander Ocaña, razón por la cual se retoma dicho trabajo en una modalidad que aún no se ha estudiado, uno de los posibles obstáculos que puede presentarse en el ejercicio investigativo del ataque informático es que no se cuenta con el suficiente conocimiento en dicha área, por tal motivo se hace indispensable la asesoría de expertos en el área.

Capítulo 2. Marco Referencial

2.1 Antecedentes Históricos

Las pruebas extraídas de las computadoras se admiten como prueba en un juicio desde los años 70, pero en su fase más temprana las computadoras no se consideraban más que un dispositivo para almacenar y reproducir registros de papel, que constituían la evidencia real. Las versiones impresas de registros de contabilidad eran aceptadas como el equivalente de expedientes de negocio conservados en mano o escritos a máquina, pero no se contaba con los datos almacenados en la computadora.

El análisis forense de computadoras (Computer Forensics) es una ciencia relativamente nueva, por lo que aún no hay estándares aceptados. Sus orígenes se remontan a los Estados unidos a mediados de los años 80. Respondiendo al crecimiento de crímenes relacionados con las computadoras, los Estados Unidos comenzaron a desarrollar programas de adiestramiento y a construir su propia infraestructura para ocuparse del problema. Estas iniciativas derivaron en centros como SEARCH, Federal Law Enforcement Center (FLETC), y el National White Collar Crime Center (NW3C).

En 1985 se crea el FBI Magnetic Media Program, que más tarde pasará a ser el Computer Analysis and Response Team (CART)

En 1990, el Laboratorio de Inspección Postal de los Estados Unidos se traslada a una nueva instalación en Dulles, Virginia, y entre 1996 y 1997 establece una unidad de Informática Forense. Trabaja junto con el FBI durante muchos años en el desarrollo de sus habilidades en informática forense.

En 1993 se celebra la primera conferencia anual sobre evidencias de computadoras (First International Conference on Computer Evidence).

En 1994, el juicio de O.J. Simpson expuso muchas de las debilidades de la investigación criminal y la ciencia forense. La investigación fue entorpecida desde el inicio con colecciones de evidencias, documentación y preservación de la escena del crimen incompletas. Como resultado de estos errores iniciales, científicos forenses especializados estaban confundidos y sus interpretaciones solo incrementaron la duda de los miembros del jurado. La controversia que rondaba este caso puso de manifiesto que investigadores y científicos forenses no eran fiables como previamente se creía, socavando no solo su credibilidad sino también su profesión. Esta crisis motivó a muchos laboratorios y agencias de investigación a revisar sus procedimientos, mejorar su entrenamiento y hacer otros cambios para evitar situaciones similares en el futuro. Por esa época hubo muchos desarrollos notables hacia la estandarización en este campo. Se fundó la Organización Internacional de Evidencias de Computadoras a mediados de los 90 que anunció “asegurar la armonización de métodos y prácticas entre naciones y garantizar el uso de evidencias digitales de un estado en las cortes de otro estado”

En España se crea en 1995 la Brigada de Investigación Tecnológica, perteneciente al Cuerpo Nacional de Policía. Comenzaron con 3 agentes de policía.

En 1997, los países del G8 declararon que "la policía debe estar adiestrada para hacer frente a delitos de alta tecnología" en el Comunicado de Moscú de diciembre. En Marzo del año siguiente, el G8 designa al IOCE para crear principios internacionales para los procedimientos relacionados con la evidencia digital.

Ese mismo año se crea el Grupo de Delincuencia Informática de la Guardia Civil, que pasó a llamarse Grupo de Investigación de Delitos de Alta Tecnología antes de tomar su nombre actual de Grupo de Delitos Telemáticos.

Los directores del Laboratorio Federal de Crimen en Washington, DC, se reunieron dos veces en 1998 para discutir asuntos de interés mutuo. Se formó lo que es ahora conocido como el Scientific Working Group Digital Evidence (SWGDE). El concepto de encontrar "evidencias latentes en una computadora" se pasó a llamar informática forense. El concepto de evidencia digital, que incluye audio y video digital se llevó ante los directores del laboratorio federal el 2 de Marzo de 1998, en un encuentro albergado por Servicio de Inspección Postal de los Estados Unidos y la División de Servicios Técnicos.

La primera discusión se centraba principalmente en la fotografía digital. El resultado de esa reunión fue que se necesitaba personal experto para abordar el tema, por lo que e12 de Mayo de ese año se reunieron de nuevo con expertos del FBI y de otros grupos especializados

en el tema. De ese encuentro surgió la formación de otro Grupo de trabajo técnico para tratar los asuntos relacionados con la evidencia digital.

El 17 de Junio de 1998, el SWGDE celebra su primer encuentro, dirigido por Mark Pollitt, agente especial del FBI y Carrie Morgan Whitcomb, del departamento forense del Servicio de Inspección Postal de los Estados Unidos. Como laboratorios forenses invitados estuvieron los del Departamento de Alcohol, Tabaco y Armas de Fuego (ATF), el Departamento de Control de Drogas (DEA), Inmigración (INS), Hacienda

(IRS), la NASA, los Servicios Secretos (USSS) y el servicio de Inspección Postal decidieron algunos procedimientos administrativos y desarrollaron documentos relevantes. Se establece que "La evidencia digital es cualquier información de valor probatorio que es almacenada o transmitida en formato binario". Más tarde "binario" cambió a "digital". La evidencia digital incluye hardware, audio, video, teléfonos móviles, impresoras, etc. Ese mismo año se celebra el primer Simposios de ciencia forense de la INTERPOL. En 1999, la carga de casos del FBI CART excede los 2000 casos, habiendo examinado 17 terabytes de datos. El IOCE presenta un borrador con estándares sobre informática forense al G8. (Análisis forense [En Línea])

En el año 2000 se establece el primero laboratorio de informática forense regional del FBI. En 2001, se realizó el primer taller de investigación forense digital –Digital Forensics Research Work Shop (www.dfrws.org)-, reuniendo a los expertos de universidades, militares y el sector privado para discutir los retos principales y buscar las necesidades de este

campo. Este taller también impulsó una idea propuesta muchos años atrás, provocando la creación de la Publicación Internacional de Evidencias Digitales -International Journal of Digital Evidence.

El rápido desarrollo de la tecnología y los crímenes relacionados con computadoras crean la necesidad de especialización:

"First Responders" (Técnicos de escena de crimen digital): expertos en recogida de datos de una escena del crimen. Deberían tener entrenamiento básico en manejo de evidencias y documentación, así como en reconstrucción básica del crimen para ayudarles a ubicar todas las fuentes posibles de evidencias.

Analistas de Evidencias Digitales: procesan la evidencia adquirida por los anteriores para extraer todos los datos posibles sobre la investigación.

Investigadores digitales: analizan todas las evidencias presentadas por los dos anteriores para construir un caso y presentarlo ante los encargados de tomar las decisiones.

Estas especializaciones no están limitadas solamente a los agentes de la ley y se han desarrollado también en el mundo empresarial. Aun cuando una sola persona sea responsable de recopilar, procesar y analizar las evidencias digitales, es útil considerar estas tareas por separado. Cada área de especialización requiere diferentes habilidades y procedimientos; tratándolos por separado hace más fácil definir el adiestramiento y los

estándares en cada área. Entendiendo la necesidad de estandarización, en 2002, el Scientific Working Group for Digital Evidence (SWGDE) publicó unas líneas generales para el adiestramiento y buenas prácticas. Como resultado de estos esfuerzos, la American Society of Crime Laboratory Directors (ASCLD) propuso requerimientos para los analistas forenses de evidencias digitales en los laboratorios. Hay además algunos intentos de establecer estándares internacionales (ISO 17025; ENFSI 2003).

A finales del año 2003 y respondiendo al creciente interés del análisis forense de intrusiones en computadoras, se propone el primer Reto de Análisis Forense por parte de Rediris, en el cual se publica la imagen de un disco duro que ha sufrido un incidente de seguridad y se reta a responder a las siguientes preguntas:

¿Quién ha realizado el ataque?, (dirección IP de los equipos implicados en el ataque)

¿Cómo se realizó el ataque? (Vulnerabilidad o fallo empleado para acceder al sistema)

¿Qué hizo el atacante? (Qué acciones realizó el atacante una vez que accedió al sistema,

¿por qué accedió al sistema?).

Al final 14 personas enviaron el informe a Rediris de los casi 500 que se presentaron, y los ganadores se llevaron licencias y manuales de software de Análisis Forense (valorados en miles de dólares).

En 2004 los Servicios de Ciencia Forense del Reino Unido planean desarrollar un registro de expertos cualificados, y muchas organizaciones Europeas, incluyendo la Red Europea de Institutos de Ciencia Forense publicaron líneas básicas para investigadores digitales. Además, El sevier comenzó la publicación de una nueva revista llamada "Digital Investigation: The International Journal of Digital Forensics and Incident Response"

A comienzos del 2005 se celebra el Reto Rediris v2.0, junto con la Universidad Autónoma de México. Se presentaron casi 1000 participantes y los premios fueron cursos de análisis forense y licencias de software. El segundo premio fue para uno de los ingenieros de la universidad de Granada.

A mediados del 2006 se celebra el III Reto Rediris, en el cual había 3 premios para los mejores de España y 3 para los mejores de Iberoamérica.

2.2 Marco Teórico

Las *RFC* por sus siglas en inglés (*Request For Comments*) son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general. La metodología que se utiliza con las *RFC* es asignarle a cada una un número único que la identifique y que es el consecutivo de la última *RFC* publicada. Una *RFC* ya publicada jamás puede modificarse,

no existen varias versiones de una RFC. Lo que se hace, en cambio, es escribir una nueva *RFC* que deje obsoleta o complemente una *RFC* anterior. (RequestForComments. [on line])

El RFC 3227 Directrices para la colección de archivos y pruebas, proporciona un interesante paso a paso de las buenas prácticas para los administradores de sistemas con directrices sobre a recopilación y archivo de las pruebas pertinentes a incidentes de seguridad.

La gestión de incidentes de seguridad de la información basada en la norma ISO 27001en su inciso A.13.1 garantizar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información están comunicados de una forma que permita tomar acciones correctivas precisas. (Norma ISO 27001)

Por otro lado la realización de informes de eventos de seguridad de información es normada por la ISO 27001 en su sección A.13.1.2 la cual busca garantizar que un enfoque consistente y efectivo es aplicado en la administración de los incidentes de seguridad de información, así mismo la norma ofrece soporte respecto a responsabilidades y procedimientos en la parte A.13.2.2 y también se habla del aprendizaje desde los incidentes de seguridad de la información en el inciso A.13.2.3 así como de Recolección de la evidencia.

El estándar ISO 20000 proporciona unos aspectos de carácter técnico para el manejo de incidentes, no obstante para comprender el estándar de dicha norma resulta casi obligatorio

hacer una referencia a otro estándar del mundo de las TI: ITIL (Information Technology Infraestructure Library). ITIL es un entorno de trabajo que engloba la "Gestión de Servicios de Tecnologías de la Información" (TI). Reúne un conjunto de las mejores prácticas recogidas por la "Oficina Gubernamental de Comercio Británica" donde se describen los procesos necesarios para administrar el área TI eficazmente, a fin de optimizar beneficios y garantizar la integración de los servicios en la cadena de valor de las unidades de negocio.

Constituye pues una biblioteca de "Buenas Prácticas de la Gestión de Servicios de TI"(ISO 20000)

ISO 20000 constituye el estándar reconocido internacionalmente para la gestión de servicios de TI. Mencionar cómo la serie ISO 20000 proviene de la adecuación de la BS 15000. El estándar ISO 20000 se divide en dos partes, al finalizar la primera nos trompamos con la sección dedicada a procesos de resolución dentro de la cual se orienta al manejo de incidentes de seguridad en los incisos 8.1 Antecedentes, 8.2 Gestión del incidente y 8.3 Gestión del problema.

El proceso DS8 de la norma administrar la mesa de servicios e incidentes de la COBIT dice "El Soporte debe responde de manera oportuna y efectiva a las consultas y problemas de los usuario TI ", en otras palabras debe hacerse cargo de la necesidad inmediata del usuario, dejando muchas veces la solución del problema técnico de fondo para otra oportunidad y otro grupo de especialistas. Es para la búsqueda de la solución del problema técnico de fondo donde entrar a tallar la Solución de Problemas y en el marco de la

metodología COBIT es el proceso DS10 Gestión de Problemas. (Administrar la mesa de servicios e incidentes de la COBIT)

2.3 Marco Conceptual

2.3.1 Análisis Forense Digital. Conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser acepta-das legalmente en un proceso judicial.

2.3.2 Análisis forense en frio (Post-mortem). El análisis en frío recoge pruebas del sistema afectado cuando éste ya ha sido apagado. El ataque ya ha terminado y, al igual que en los casos policiales, es necesario recoger pruebas para conocer los hechos ocurridos.

2.3.3 Análisis forense en caliente (On-line). El análisis en caliente recoge pruebas en el sistema afectado estando éste todavía encendido. El ataque continúa en marcha, por lo que es un momento propicio para recoger evidencias (ya que tras el apagado de la máquina, algunas de éstas se perderán).

2.3.4 Encriptación informática. La encriptación informática es simplemente la codificación de la información que se va a enviar a través de la red (Internet). Para poder

descodificarla es necesario un software o una clave que sólo conocen el emisor y el receptor de esta información.

La encriptación de la informática se hace cada vez más necesaria debido al aumento de los robos de claves, número de cuentas corrientes, y en general toda la información que viaja por la red.

2.3.5 Evidencia digital. Conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (meta-datos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

2.3.6 Seguridad Informática. Consiste en la protección conferida a un sistema de información automatizado con el fin de alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información. (WILLIAM STALLINGS. 2011.)

Confidencialidad. Este término se refiere a dos conceptos relacionados:

- **Confidencialidad de los datos:** Asegura que la información privada o confidencial no esté disponible o revelada apersonas no autorizadas.

- **Privacidad:** Asegura que el control de las personas o influir en la información que relacionados con ellos puede ser recogida y almacenada y que, por quién y para quién información puede ser revelada.

Integridad. Este término se refiere a dos conceptos relacionados:

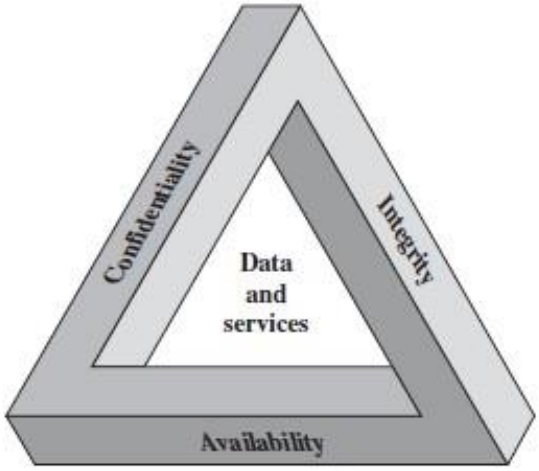
- **Integridad de los datos**: Asegura que la información y los programas sólo se cambian de una manera específica y autorizada.

- **La integridad del sistema:** Asegura que un sistema que pretende realizar una función deseada de una forma intacta, sin autorización deliberada o involuntaria no manipule el sistema.

- **Disponibilidad** Asegura que el sistemas trabaje inmediatamente y el servicio no se le niegue a los usuarios autorizados.

Estos tres conceptos forman lo que se refiere a menudo como la tríada de la CIA (**Figura 1**).Los tres conceptos abarcan los objetivos fundamentales de seguridad para ambos, datos y servicios de computación e información.

Figura 1. Requerimientos de seguridad informática.



Fuente. William Stallings, NETWORK SECURITY ESSENTIALS applications and standards. Fourth edition,

2.3.7 Incidente de Seguridad Informática. Es considerado como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

Se categorizan dichos incidentes en:

Incidentes de Denegación de Servicios (DoS): Son un tipo de incidentes cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agotamiento de sus recursos

Incidentes de código malicioso: Cualquier tipo de código ya sea, virus, gusano, “caballo de Troya”, que pueda ejecutarse en un sistema e infectarlo.

Incidentes de acceso no autorizado: Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.

Incidentes por uso inapropiado: Se dan cuando los usuarios se "saltan" la política de uso apropiado de los sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música). (Experiencias de análisis forense en México. Departamento de Seguridad en Cómputo / UNAM-CERT en Jornadas de Análisis Forense. Madrid, Septiembre 2005.)

2.4 Marco legal

2.4.1 Leyes para la regulación en las telecomunicaciones en Colombia.

Ley 1273 de **2009"De la protección de la información y de los datos"**

Congreso de la república. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

Decreta:

Artículo1o.Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos".

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

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

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

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

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

Artículo 269F. *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios

mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio o de personal confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

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

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

Por servidor público en ejercicio de sus funciones.

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro. Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional. Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

De los atentados informáticos y otras infracciones.

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

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

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

Art.236. recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.

Art 275. Elementos materiales probatorios y evidencia física.

Mensaje de datos, como el intercambio electrónico de datos, Internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de1999 o las normas que la sustituyan, adicionen o reformen.

2.4.2 Licencias para el uso del Software Libre

Licencias GPL: Una de las más utilizadas es la Licencia Pública General de GNU (GNU GPL). El autor conserva los derechos de autor (*copyright*), y permite la redistribución y modificación bajo términos diseñados para asegurarse de que todas las versiones modificadas del software permanecen bajo los términos más restrictivos de la propia GNU GPL. Esto hace que sea imposible crear un producto con partes no licenciadas GPL: el conjunto tiene que ser GPL. (Free Software Foundation, 2010)

Es decir, la licencia GNU GPL posibilita la modificación y redistribución del software, pero únicamente bajo esa misma licencia. Y añade que si se reutiliza en un mismo programa código "A" licenciado bajo licencia GNU GPL y código "B" licenciado bajo otro tipo de licencia libre, el código final "C", independientemente de la cantidad y calidad de cada uno de los códigos "A" y "B", debe estar bajo la licencia GNU GPL.

Copyleft. *Copyleft* o copia permitida comprende a un grupo de derechos de autor caracterizados por eliminar las restricciones de distribución o modificación impuestas por el copyright, con la condición de que el trabajo derivado se mantenga con el mismo régimen de derechos de autor que el original. Bajo tales licencias pueden protegerse una gran diversidad de obras, tales como programas informáticos, arte, cultura y ciencia, es decir prácticamente casi cualquier tipo de producción creativa. *Copyleft* dice que cualquiera que redistribuye el software, con o sin cambios, debe dar la libertad de copiarlo y modificarlo más. *Copyleft* garantiza que cada usuario tiene libertad. (FundaciónCopyleft. 2010)

BSD. Llamadas así porque se utilizan en gran cantidad de software distribuido junto a los sistemas operativos BSD. El autor, bajo tales licencias, mantiene la protección de copyright únicamente para la renuncia de garantía y para requerir la adecuada atribución de la autoría en trabajos derivados, pero permite la libre redistribución y modificación, incluso si dichos trabajos tienen propietario.

Creative Commons. Las licencias Creative Commons o CC están inspiradas en la licencia GPL de la *Free Software Foundation*. No son, sin embargo, un tipo de licenciamiento de software. La idea principal es posibilitar un modelo legal ayudado por herramientas informáticas, para así facilitar la distribución y el uso de contenidos.

2.4.3 Ley 842 de 2003

TITULO IV

Código de Ética para el Ejercicio de la Ingeniería en General y sus Profesiones afines y Auxiliares

CAPITULO I

Disposiciones generales

Artículo 29. *Postulados éticos del ejercicio profesional.* El ejercicio profesional de la Ingeniería en todas sus ramas, de sus profesiones afines y sus respectivas profesiones auxiliares, debe ser guiado por criterios, conceptos y elevados fines, que propendan a enaltecerlo; por lo tanto deberá estar ajustado a las disposiciones de las siguientes normas que constituyen su Código de Ética Profesional.

Parágrafo. El Código de Ética Profesional adoptado mediante la presente ley será el marco del comportamiento profesional del ingeniero en general, de sus profesionales afines y de sus profesionales auxiliares y su violación será sancionada mediante el procedimiento establecido en el presente título.

Artículo 30. Los ingenieros, sus profesionales afines y sus profesionales auxiliares, para todos los efectos del Código de Ética Profesional y su Régimen Disciplinario contemplados en esta ley, se denominarán "Los profesionales".

CAPITULO II

Artículo 33.*Deberes especiales de los profesionales para con la sociedad* Son deberes especiales de los profesionales para con la sociedad:

Interesarse por el bien público, con el objeto de contribuir con sus conocimientos, capacidad y experiencia para servir a la humanidad.

Coopera para el progreso de la sociedad, aportando su colaboración intelectual y material en obras culturales, ilustración técnica, ciencia aplicada e investigación científica.

Aplicar el máximo de su esfuerzo en el sentido de lograr una clara expresión hacia la comunidad de los aspectos técnicos y de los asuntos relacionados con sus respectivas, profesiones y su ejercicio;

Artículo 34.*Prohibiciones especiales a los profesionales respecto de la sociedad.* Son prohibiciones especiales a los profesionales respecto de la sociedad:

Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.

Imponer su firma, a título gratuito u oneroso, en planos, especificaciones, dictámenes, memorias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias de construcción y toda otra documentación relacionada con el ejercicio profesional, que no hayan sido estudiados, controlados o ejecutados personalmente.

Artículo 37. *Deberes de los profesionales para con sus colegas y demás profesionales.* Son deberes de los profesionales para con sus colegas y demás profesionales de la ingeniería:

Respetar y reconocer la propiedad intelectual de los demás profesionales sobre sus diseños y proyectos.

Artículo 38.*Prohibiciones a los profesionales respecto de sus colegas y demás profesionales.* Son prohibiciones a los profesionales, respecto de sus colegas y demás profesionales de la ingeniería:

Utilizar sin autorización de sus legítimos autores y para su aplicación en trabajos profesionales propios, los estudios, cálculos, planos, diseños y software y demás documentación perteneciente a aquellos, salvo que la tarea profesional lo requiera, caso en el cual se deberá dar aviso al autor de tal utilización.

2.4.4 Ley de Derecho de Autor.

Hace referencia sobre la protección de la información que con intención y sin derecho reproduzca, con infracción del encabezamiento del artículo 41 de esta Ley, en forma original o elaborada, íntegra o parcialmente, obras del ingenioso quien introduzca en el país, almacene, distribuya, venda o ponga de cualquier otra manera en circulación reproducciones ilícitas de las obras del ingenio o productos protegidos por esta Ley.

2.4.5 La legislación de derechos de autor en Colombia.

Mediante decisión 351 de la comisión del acuerdo de Cartagena de diciembre de 1993, que está respaldada por la ley 44 de 1993 y por la ley 23 de 1982. Estas normas otorgan amplia e importante protección a los programas de software, convirtiendo ilícita la copia de programas sin consentimiento de los titulares de los derechos de autor, con excepción de la copia de seguridad.

2.4.6 Norma Técnica Colombiana NTC 4490,1160 y 130837.

Estas normas establecen la presentación uniforme de referencias bibliográficas para publicaciones seriadas, libros, folletos y para fuentes de información electrónicas, con el fin de facilitar la identificación de los mismos o de una de sus partes.(INSTITUTO COLOMBIANO DE NORMAS TÉCNICASY CERTIFICACIÓ. Tesis y trabajos de grado. Bogotá; ICONTEC, 2002)

Capítulo 3. Diseño Metodológico

3.1 Tipo de Investigación

El proceso estará fundamentado en una investigación descriptiva, la cual consiste en llegar a conocer situaciones y actitudes predominantes de un objeto de estudio a través de la descripción exacta de las actividades, objetos, procesos a llevar a cabo la investigación. El objetivo no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

Esta investigación se define como descriptiva, ya que por medio de los laboratorios que se realicen, se analizará el comportamiento de las diferentes funcionalidades y potencial que tiene la metodología de análisis fornece post-mortem.

3.2 Población

La población está conformada por administrador del laboratorio del Grupo de Investigación en Teleinformática y Desarrollo de Software (GITYD).

3.3 Muestra

Considerando que la población es solo el administrador del laboratorio del Grupo de Investigación en Teleinformática y Desarrollo de Software (GITYD), se toma como muestra toda la población involucrada en el proceso.

3.4 Técnicas e Instrumentos de Recolección de la Información

Para la presente investigación es necesario aplicar la técnica de observación estructurada la cual se lleva a cabo cuando se pretende probar una hipótesis o cuando se quiere hacer una descripción sistemática de algún fenómeno. El instrumento mediante el cual se va a obtener la información para aplicar esta técnica es una ficha de observación para los laboratorios que se van a realizar durante el desarrollo del presente estudio. Después de un correcto y completo estudio del análisis forense informático post – mortem se realizará el análisis del ataque. La recolección de datos se hará mediante evaluación directa del ataque informático después de realizado éste. Para este propósito se utilizará la metodología de Casey.

3.4.1 Selección de la metodología.

Dentro del análisis forense podemos establecer dos fases neurálgicas dentro de su desarrollo, la primera es la que tiene que ver con el manejo y preservación de la escena y la evidencia y el segundo se refiere al análisis de estos elementos (ver figura):

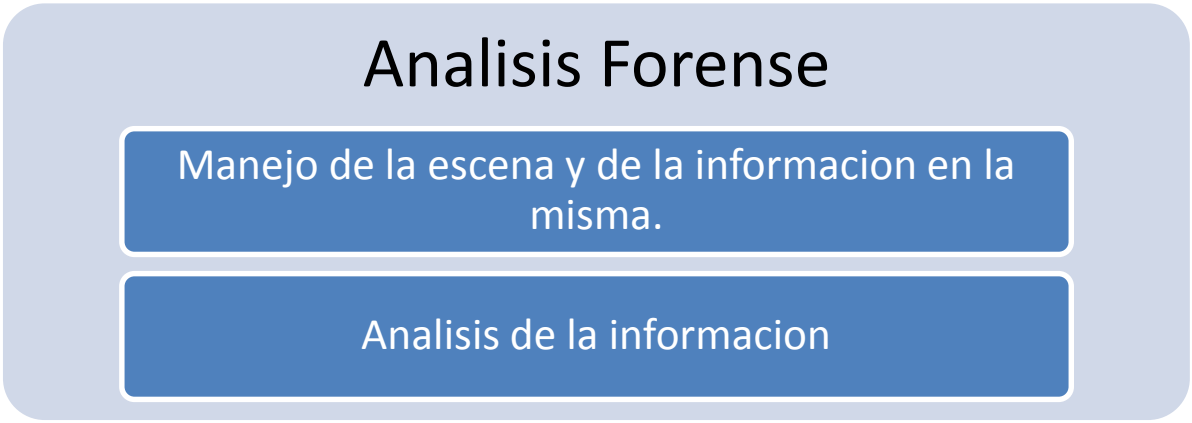


Figura 2: Etapas básicas del análisis forense

Fuente: Autor de la investigación.

Diferentes instancias como y estudiosos del tema a nivel mundial han desarrollado esfuerzos por intentar establecer unos parámetros que definan las buenas prácticas a la hora de realizar el análisis forense como la HB171-2003 Guidelines for the Management of IT Evidence (http://catalogue.nla.gov.au/Record/1032535), creada en Australia por la academia, industria, administración de justicia, gobierno y entes policiales, permite una vista homogénea frente al reto de la evidencia digital como elemento de prueba real con todos sus elementos; De igual forma, las guías del NIST sobre estos temas particularmente en dispositivos móviles, web services, entre otros, así como las indicaciones del Departamento de Justicia de los Estados Unidos en los documentos como Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition a continuación se establece un cuadro comparativo entre algunas estas propuestas planteado por la ISO como referente para establecer el estándar ISO/IEC 27037:2012:

Tabla 1.

Tabla de comparación y armonización de los modelos existentes

	The harmonized model	DFWRS	Reith et al.	DOJ	Carrier et al.	Mandia et al.	Beebe et al.	Cuardhuain	Cohen	Casey	ACPO
	Deteccion del incidente	1. Identificacion	1. Identificacion		2. Deteccion y notificacion	2. Detection of the incident	2. Incident response*				
1						3. Initial response		1. Awareness			
							2. Incident response*				2.1 Secure and
2	First response					3. Initial response					control the crime scene
			3. Approach strategy*		1. Readiness group of phases *	4. Response					1. Preparations for investigation
3	Planeacion					strategy formulation*		3. Planning			
	Preparacion		2. Preparation		1. Readiness group of phases *	1. Pre-incident preparation					1. Preparations for investigation
4				1. Preparation*			1. Preparation*				
				3. Documentation of the crime scene	4.3 Document evidence and scene						2.1 Photograph

5	Documentación de la escena del incidente										and document the scene
											2.4 Attaching exibit labeles
										1.Gather	
6	Identificación de la evidencia potencial		6. Examination	2. Recognition and Identification;	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	information and make	5.1 The collection process
										observations,	
						5. Duplication				1.Gather information and make observations,	2.3 Initial collecting of volatile data
7	Colección de la evidencia digital	2. Preservation	4. Preservation	4. Collection and preservation	4.1 Preservation of digital crime scene	7. Secure measure implementation	3. Data collection*	6. Collection of evidence	2. Collection		5.1 The collection
		3. Collection	5. Collection			8. Network			3. Preservation		process
						monitoring					
	Transporte de la evidencia digital			5. Packaging				7. Transport of evidence			
8				and transportation					4. Transportation		3. Transport
9	Almacenamiento de la evidencia digital							8. Storage of	5. Storage		4. Storage
								evidence			

	Análisis de la evidencia digital	4. Examination		6. Examination	4.4 Search for			9. Examination of	6. Analysis		5.2 The analysis
10		5. Analysis	7. Analysis	7. Analysis	digital evidence	6. Investigation	4. Data analysis*	evidence			process
										2. Form hypothesis to explain observa-	
										tions,	5.3 The examination process
11	Interpretacion de la evidencia digital				4.5 Digital crime scene reconstruction			10. Hypothesis	7. Interpretation	3.Evaluate the hypothesis,	
									8. Attribution	4. Draw conclu-	
									9. Reconstruction	sions and commu-nicate findings.	
12	Escritura del reporte			8. Report*		10. Reporting*					5.4 The reporting process
					4.6 Presentation of digital scene theory*			11. Presentation of		4 .Draw	
13	Presentacion	6. Presentation*	8. Presentation*	8. Report*		10. Reporting*	5. Findings presentation*	hypothesis	10. Presentation	conclusions and communicate findings.	5.4 The reporting process
								12. Proof/			

						Defence of hypothesis		
14	Clausura de la investigacion	7. Decision*	9. Returning evidence*	9. Recovery 11. Follow-up*	6. Closure*	13. Dissemination of information	11. Destruction*	6. Disclosure

Fuente: Information technology- Security tecniques- Incident principies and process, ISO/IEC 2012

De lo anterior se definen tres subgrupos de actividades que en resumen pasó a paso el manejo de la evidencia digital desde su hallazgo hasta su documentación, aspectos que se refinan en el enunciado del estándar ISO/IEC 27037:2012, el cual proporciona directrices para las actividades específicas en el manejo de la evidencia digital, que son la identificación, recolección, consolidación y preservación del potencial de la evidencia digital que puede ser de valor probatorio. Proporciona orientación a las personas con respecto a las situaciones comunes que se encuentran en todo el proceso de manipulación de evidencia digital y ayuda a las organizaciones en sus procedimientos disciplinarios y para facilitar el intercambio de potencial evidencia digital entre jurisdicciones.

Este estándar ofrece un marco común en el contexto internacional para las siguientes etapas del manejo de la evidencia:

La identificación

Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.

La recolección y/o adquisición

Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos. Para la presente investigación también se utilizara como referente el RFC 3227 Directrices para la colección de archivo y Prueba.

La conservación/preservación

La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la Cadena de Custodia, la integridad y la originalidad de la prueba.

ANÁLISIS DEL ESTÁNDAR

Si bien es cierto que el estándar ISO/IEC 27037:2012 proporciona una excelente base para la realización del análisis forense, también plantea algunos interrogantes con respecto a la presentación, pero más importante aún con relación al análisis de la evidencia digital, por lo cual

solo nos proporciona lineamientos estructurales en cuanto a la fases iniciales del estudio.

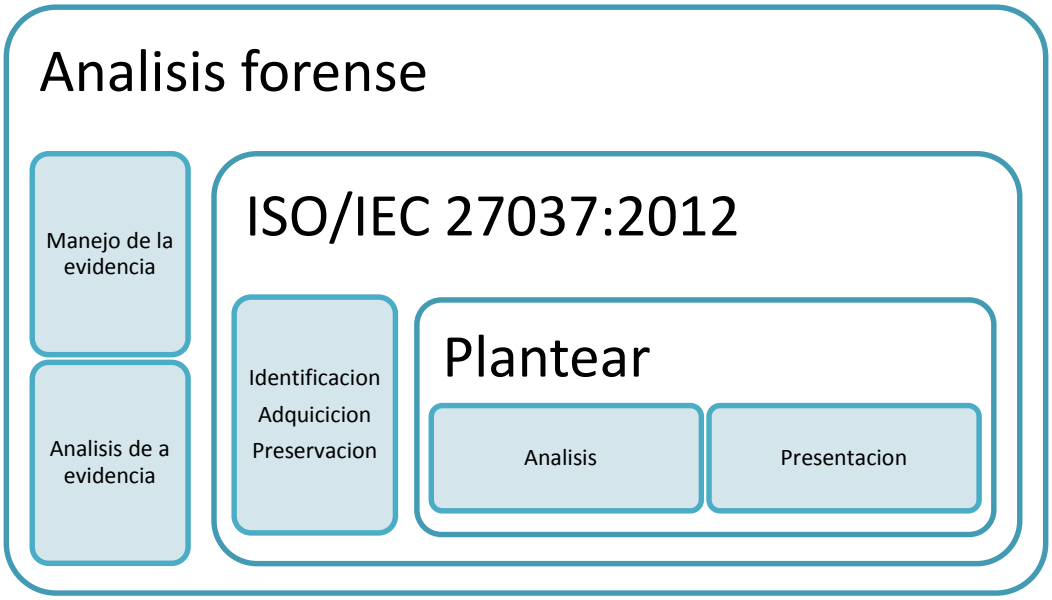


Figura 3: Estado del arte Metodologías análisis forense

Fuente: Autores de la investigación

Como se observa en la **Figura 2** se hace necesario establecer una estructura metodológica para la ejecución del análisis y la presentación, para esta última buscaremos apoyo en alguna de las metodologías teóricas más aceptadas, mientras que para el análisis nos basaremos en la observación experimental mediante el estudio de varios escenarios prácticos para establecer las actividades recurrentes.

Tomando como referente la Tabla de comparación y armonización de los modelos existentes se extraen las metodologías que se ajustan a los anteriores requerimientos y refinamos para establecer que metodologías se ajustan a de mejor manera a la identificación, adquisición y preservación. (Information technology- Security tecniques- Incident principies and process, ISO/IEC 2012)

Tabla 2.

Comparación de las metodologías

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

Fuente: Autores de la investigación.

De lo anterior se extrae que las metodologías SANS, DFRW, Mandia/ Prosise y Casey son las que mejor se adaptan a la totalidad de las fases del análisis forense.

La siguiente comparación muestra aspectos altenativos a tener en cuenta a la hora de apliacar una metodología para el estudio forense, donde resalta la naturaleza del software usado en cuanto a su licencia (Libre o propiestario).

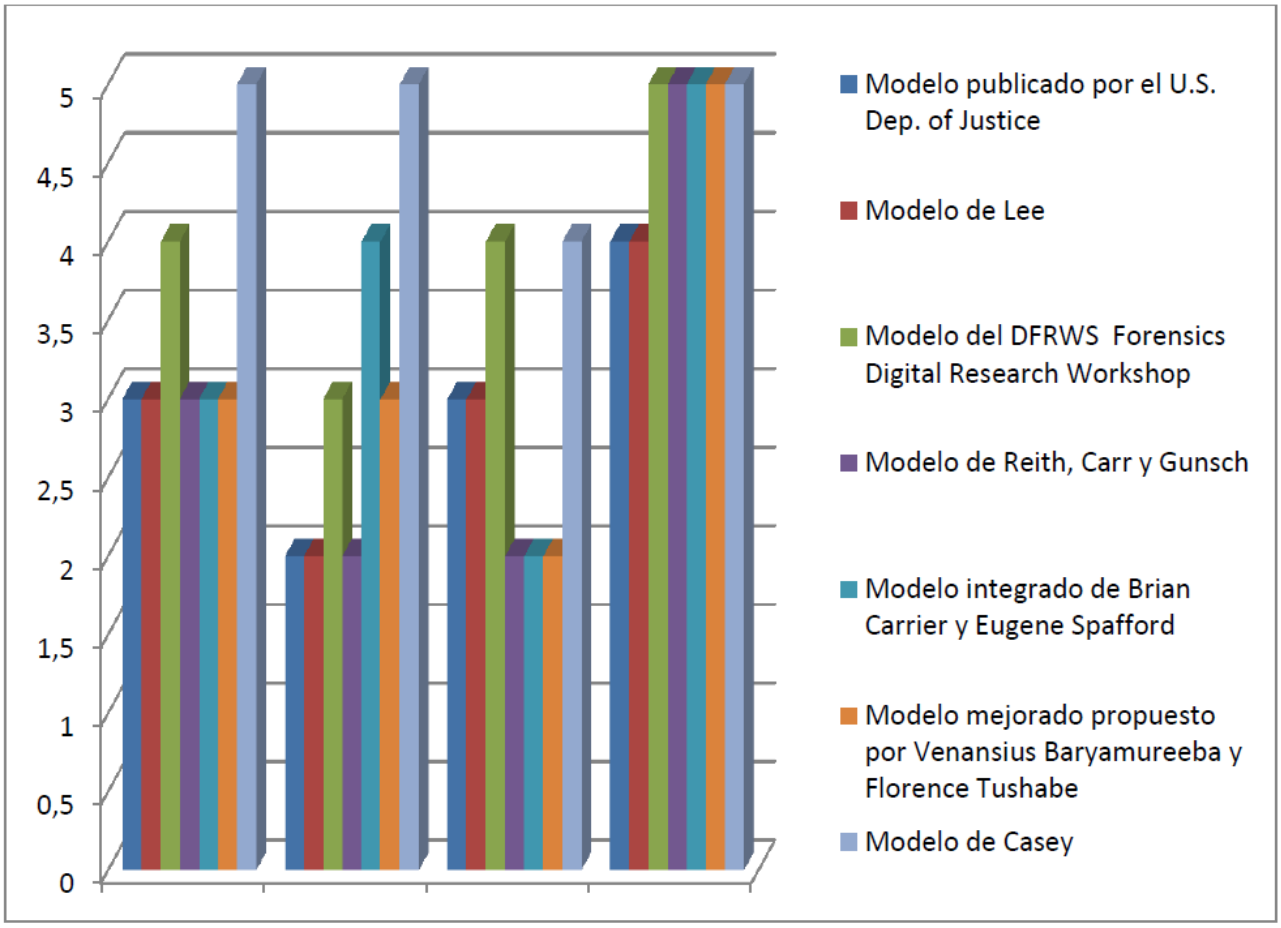


Figura 4: representación Gráfica de la comparación de metodologías
Fuente: LOBO LEONARD, desarrollo e implementación del análisis digital forense utilizando una metodología post-mortem, [En línea]: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/478

En los dos estudios la comparación muestra que el modelo Casey es la metodología que más se adapta al presente estudio, además de arrojar resultados interesantes tras abordar su análisis desde perspectivas diferentes.

3.4.2 Modelo de Casey (2004).

Como podemos apreciar, con el paso de los años los modelos tienden a tener más etapas para describir el proceso de investigación. El modelo de Casey ha evolucionado desde el primer modelo presentado en el 2002 hasta el modelo publicado en el 2004 en su segunda edición de su libro referencia que recoge los siguientes pasos:

Autorización y preparación

Identificación

Documentación, Adquisición y Conservación Extracción de Información y Análisis

Reconstrucción

Publicación de conclusiones

Autorización y Preparación. Lo primero que se debe hacer es ir a la escena del delito a recoger pruebas, pero antes debemos prepararnos con el material y los permisos necesarios para llevarlo a cabo.

Identificación. Una vez que estamos en la escena del delito debemos identificar todo el hardware y software que encontremos.

Documentación. Esta etapa se realiza durante todo el proceso. Debemos anotar todos los pasos realizados para ayudar a una reconstrucción final de los hechos y con mayor detalle aún si se va a presentar como prueba en un juicio.

Adquisición. Debemos extraer todo el hardware encontrado que pueda tener pruebas. Generalmente la prueba no es el hardware en sí (huellas digitales, números de serie de CPU), sino el contenido de los mismos. De modos que debemos extraer una imagen de cada dispositivo encontrado.

Conservación. El hardware debe conservarse de forma que no se altere su contenido y es primordial hacer varias copias de la imagen extraída de cada dispositivo y nunca manipular el original.

Examen y Análisis. Con todos los datos obtenidos en las etapas anteriores podemos tener una idea de dónde empezar a buscar, por lo que debemos elaborar una hipótesis y a partir de ella comenzar a recopilar datos que nos ayuden a confirmarla. Existen multitud de métodos para extraer datos de un sistema de ficheros que podemos usar para este fin.

Reconstrucción. Una vez que tenemos datos suficientes debemos ser capaces de responder a las preguntas ¿Qué pasó? ¿Quién lo hizo? ¿Cuándo? ¿Dónde? y en última instancia ¿por qué?

Publicación de conclusiones. Los resultados de los análisis forenses deberían publicarse en la medida de lo posible para incrementar el conocimiento de otros investigadores y en último caso para posibles sistemas expertos que en el futuro puedan ayudar en este campo.

El proceso puede verse como en la siguiente figura: cada flecha indica el flujo de información, de modo que la información que obtenemos en una etapa nos sirve para la siguiente y viceversa. En cualquier momento se puede usar lo que se sabe en una etapa para volver a la etapa anterior y obtener más datos. Toda la información generada se guardará como documentación que nos servirá para la publicación final.

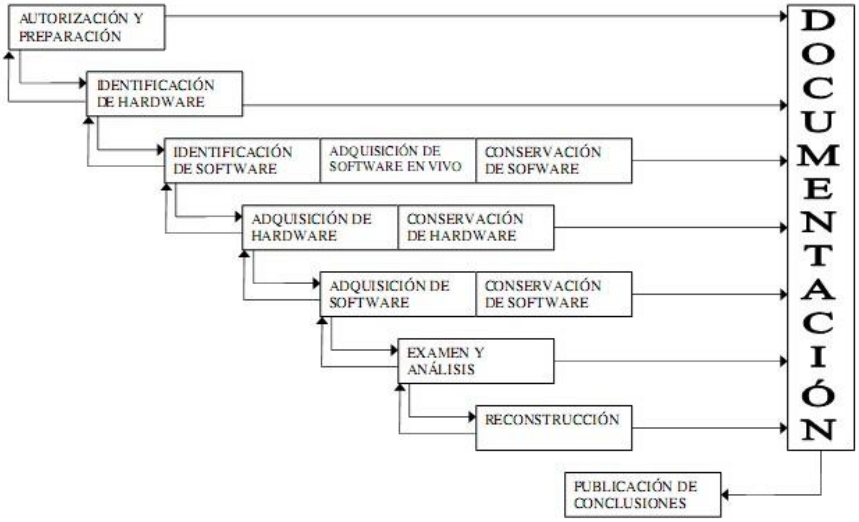


Figura 3. Esquema general modelo Casey

Fuente: Herramienta de apoyo para el análisis forense de computadoras, José Arquillo Cruz, Escuela Politécnica Superior de Jaén, Septiembre, 2007

Autorización y Preparación

Autorización. El objetivo detrás de cualquier investigación realizada por un forense o un equipo de respuesta rápida sobre un sistema de ficheros puede ser de tipo 'legal' o

'casual'. Teniendo en consideración que estos términos no tienen un significado estandarizado para describir los motivos de una investigación y cada uno de ellos se diferencia bastante del otro debemos detallar más.

Investigación Legal. La mayoría de las investigaciones forenses de tipo legal tienen como objetivo asistir a los órganos oficiales a llevar a cabo una investigación criminal a fin de llevar ante la justicia al culpable del delito. En investigaciones de este tipo es imprescindible seguir de forma estricta los procedimientos para el tratamiento de pruebas que van a ser presentadas en el juzgado. Por ejemplo, el mero error de sobrescribir cualquier prueba en el sistema de ficheros por información aleatoria pérdida de datos) es suficiente para considerar el resto de las pruebas de la misma índole como inviables por parte de un juez o fiscal. Investigaciones legales, a menudo, únicamente se limitan a la conservación de datos y esfuerzos de mantener la integridad de información en el sistema de ficheros una vez el hecho del compromiso ha sido probado. Las pruebas tras ser tratadas de forma correcta se transfieren al poder de órganos oficiales para ser analizados por parte de sus recursos. El nivel de participación del forense en la investigación una vez las pruebas han sido transferidas depende del deseo del denunciante y la voluntad de órganos oficiales.

Investigación Casual. Cualquier tipo de investigación casual no tiene como objetivo la persecución legal del individuo responsable del acto criminal. La investigación se realiza por el interés desde el punto de vista forense, por lo tanto las técnicas, herramientas y metodología utilizada puede ser usada de forma más agresiva. La realización de una investigación forense casual requiere más conocimiento y

experiencia por parte del investigador, ya que en estos casos no existen requerimientos estrictos de terceros referentes a la cantidad y calidad de pruebas obtenidas. Antes de manipular una evidencia digital, hay muchas cosas que se deben considerar. Una de ellas es que estemos seguros de que nuestra búsqueda no va a violar ninguna ley o dar lugar a responsabilidades legales. Los profesionales de la seguridad en computadores deberían obtener instrucciones y autorizaciones escritas de sus abogados antes de realizar cualquier investigación dentro de una organización. Una política de organización determina en gran parte si se pueden buscar en las computadoras de los empleados, analizar los e-mails y otros datos. Sin embargo, una búsqueda justificada normalmente se necesita para acceder a las áreas que un empleado consideraría personales o privadas sin su consentimiento. Hay algunas circunstancias que permiten búsquedas justificadas en un lugar de trabajo, pero los profesionales de la seguridad deben dejar estas decisiones a sus abogados.

Preparación. Antes de empezar un análisis forense se recomienda describir cómo se va a realizar la recolección de evidencias. Si es posible tener acceso a alguien que esté íntimamente relacionado con la computadora, obtener información general como el tipo de computadora, su sistema operativo, si está en una red LAN, en Internet, etc. Además puede que necesitemos algunas herramientas como CD's Forenses, contenedores adecuados para transportar el hardware, y otras herramientas como puede ser un destornillador.

Documentación. La documentación es esencial en todas las fases del manejo y procesamiento de evidencia digital. Documentando quien adquiere y maneja evidencias

en un momento dado es algo imprescindible para mantener la Cadena de Custodia. Esto no es algo inusual para alguien que maneja una evidencia para posteriormente presentar las conclusiones ante un juicio. La continuidad de la posesión o Cadena de Custodia debe ser establecida para que la evidencia sea admitida como válida, aunque frecuentemente todas las personas involucradas en la adquisición, transporte y almacenamiento de evidencias son llamados para testificar en un juicio. De modo que, para evitar confusiones y mantener el control completo de la evidencia en cada momento, la Cadena de Custodia debería estar obligada a cumplir un mínimo. Así que, debería anotarse cuidadosamente cuando se adquiere la evidencia, de donde y por quien. PoR ejemplo, si la evidencia se copia en un disquete, deberíamos anotar en la etiqueta del mismo y en la cadena de custodia la fecha y hora actuales, las iníciales de la persona que hizo la copia, como hizo la copia y la información relativa al contenido del disquete. Adicionalmente, los valores MD5 o SHA de los archivos originales deberían ser notados antes de copiarse. A continuación podemos ver un ejemplo de una Cadena de Custodia con información mínima para un disco duro cuyo número de serie es el 123456.

Identificación. La identificación de las evidencias digitales es un proceso con dos pasos: Primero, el investigador debe reconocer el hardware (por ejemplo, ordenadores, disquetes o cables de red) que contienen información digital.

Segundo, el investigador debe distinguir entre la información relevante y otros datos intrascendentes según lo que estemos buscando.

Identificación de Hardware. Hay muchos productos computarizados que pueden tener evidencias recogidos en, como teléfonos, dispositivos inalámbricos, PDAs, Routers, Firewalls y otros dispositivos de red. Hay muchas formas de almacenar datos multimedia, como disquetes, cds, cintas magnéticas, pen drives, memory cards, etc.

Identificación del software. Generalmente se considera que todo el contenido del hardware identificado contiene potencialmente evidencia digital. Por esto, una vez que se ha retirado el hardware para su análisis en el laboratorio, se debe extraer su contenido. Por esto no podemos identificar las evidencias digitales hasta que no hayamos adquirido el hardware y extraído el software que contiene. Pero existen algunos casos en los que se pueden identificar evidencias digitales en el lugar del delito. Es lo que llamamos una adquisición de datos en vivo, que se realiza cuando el sistema se encuentra encendido o no se puede apagar por diversas razones, como que se trate de un sistema crítico (sistemas informáticos de los hospitales).

En este punto debemos decir que hay dos tipos de datos:

Datos volátiles. Son datos que se pierden si el sistema es apagado. Ejemplos de los mismos puede ser una lista de procesos en ejecución y usuarios activos.

Datos No Volátiles. Son datos que no se pierden cuando apaga el sistema e incluyen el disco duro.

Por tanto sabemos que si apagamos un sistema encendido perderemos los datos volátiles y en algunos casos puede ser muy interesante obtenerlos. Para determinar que evidencia recoger primero debemos seguir el Orden de Volatilidad: una lista de fuentes de evidencias ordenadas por su volatilidad relativa.

En general puede verse de la siguiente manera:

Registros, memoria de periféricos, cachés, etc.	nanosegundos
Memoria Principal	Nanosegundos
Estado de la Red	Milisegundos
Procesos en ejecución	segundos
Disco	minutos
Disquetes, copias de seguridad, Discos duros, etc.	Años
CD-ROMs, DVDs, etc.	Decenas de años

Figura 5. Lista de volatilidad

Fuente: Herramienta de apoyo para el análisis forense de computadoras, José Arquillo Cruz, Escuela Politécnica Superior de Jaén, Septiembre, 2007

Un ejemplo de orden de volatilidad podría ser: Registros y cache

Tablas de enrutamiento

Cache Arp

Tabla de procesos en ejecución

Estadísticas y módulos Kernel

Memoria principal

Ficheros temporales del sistema Memoria secundaria

Configuración del Router Topología de red

Una vez que hemos obtenido la información volátil debemos pensar en apagar el sistema. Una de las decisiones más difíciles al encontrarse con una computadora sospechosa que está encendida es cómo apagar el sistema de manera que no se corrompa la integridad de los archivos. En la mayoría de los casos, el tipo de sistema operativo empleado en la computadora será la clave a la hora de tomar esta decisión. Con unos, bastará con tirar del enchufe del ordenador, y en otros, desconectando el PC sin permitir al sistema operativo iniciar sus comando internos de apagado podría resultar desde la pérdida de archivos vitales hasta la rotura del disco duro.

El problema es que si usamos cualquier comando o funcionalidad del sistema para apagar el sistema, corremos el riesgo de que se ejecute código malicioso o de que se modifiquen los logs del sistema. Por ejemplo, los comandos "shutdown" o "sync" podrían haber sido modificados de forma que cuando los ejecutemos el sistema borre ficheros críticos. Por lo tanto es preferible usar nuestros propios ejecutables de forma externa.

El riesgo típico de tirar del cable de la pared es que el sistema estará en un estado inconsistente, y cuando el sistema se encienda de nuevo iniciará un proceso intensivo de reconstrucción.

Generalmente parece que hay una regla aceptada que dice "si esta encendido, no lo apagues, y si está apagado, no lo enciendas". En caso de que esté encendido lo más común es simplemente fotografiar la pantalla y tirar del cable de la pared. Deberemos anotar que se

tiró del cable para tener en cuenta más tarde que el SISTEMAS OPERATIVOS puede estar en un estado inconsistente. Esto es útil saberlo sobre todo si más tarde se decide arrancar el sistema de nuevo en un entorno seguro.

En el caso de que no se pueda apagar el sistema por ser crítico su funcionamiento, se debe hacer un análisis mínimamente intrusivo intentando recopilar la mayor cantidad de datos posibles relacionados con la investigación. Esto puede verse con mayor detalle en la sección de "Examen y Análisis", donde se pueden ver los archivos que son interesantes según el tipo de delito.

Adquisición. Una vez identificadas, las evidencias deben ser recogidas y conservadas de modo que puedan ser identificadas después con facilidad. Una buena forma de hacer esta recogida es de forma que no se alteren. Imagínese por un momento una supuesta escena del crimen donde haya una nota suicida escrita en la pantalla. Antes de examinar el contenido digital de la computadora se debería antes fotografiar la pantalla y tomar huellas digitales. Pero aquí nos topamos con otro problema: ¿qué hacemos cuando nos encontramos una computadora encendida? ¿La apagamos directamente? Si manipulamos la computadora en busca de datos podemos alterar la evidencia. Por ejemplo, si encontramos una computadora con un sistema Linux y probamos a hacer un 'ls' para ver el listado actual de un directorio, modificaremos los registros de actividad, el contenido de la memoria ram, etc.

Adquisición del hardware. Aunque este apartado se base en los datos almacenados en las computadoras, vamos a hacer una mención al hardware para asegurarnos de que la evidencia que contiene se conserva correctamente.

Hay dos factores que se deben considerar al recolectar el hardware. En un lado, para no dejar ninguna evidencia atrás, un investigador puede decidir que hay que recoger todas las piezas que se encuentren. Por otro lado, un investigador puede recoger solo lo esencial para ahorran tiempo, esfuerzo y recursos. Algunas computadoras de instituciones en continuo funcionamiento, como hospitales, el hecho de modificar algo puede costar vidas humanas. En algunos casos, simplemente no es factible recoger el hardware por su tamaño o cantidad. ¿Qué hacer si una computadora está conectada a otra? En una era en la que las redes de computadoras son lo habitual, sería absurdo pensar que podemos obtener todas las computadoras que están conectadas a una dada. En una red de área local situada en un piso, edificio o en un campus universitario, un PC puede estar conectado a cientos de computadoras. Este PC puede además estar conectado a internet, por lo que deberíamos tomar muchas computadoras en todo el mundo. En definitiva, esta elección se debe tomar en función del número de pruebas que necesitemos y los recursos para almacenarlas que dispongamos. Si se decide recoger una computadora entera, deberían considerarse todos sus periféricos, como impresoras o unidades de cinta. Las hojas impresas que estén relacionadas con la computadora pueden contener información que ha sido cambiada o borrada de la computadora, como números de teléfono, direcciones de e-mail, etc. Además se recomienda mirar en la basura en busca de evidencias.

Adquisición del software. Cuando se trata con evidencias digitales, lo principal es el contenido de la computadora más que el hardware en sí. En este apartado veremos cómo se adquieren estos contenidos de forma que no se altere la información que contienen y podamos estar seguros de que tenemos una copia exacta.

Hay dos tipos de adquisición de datos: en vivo o post-mortem. La diferencia está basada en el sistema operativo usado durante la copia:

Una adquisición en vivo ocurre cuando los datos son copiados desde un sistema sospechoso usando el sistema operativo sospechoso. Esta se hace normalmente antes de la adquisición de hardware y fue mencionada previamente en el apartado de Identificación de Software.

Una adquisición post-mortem se realiza cuando el dispositivo a analizar no está en ejecución y por tanto los datos son copiados posteriormente en un entorno controlado. Esto ocurre cuando el disco es extraído del sistema sospechoso y ubicado en un sistema controlado, y también cuando el sistema sospechoso es arrancado con un dispositivo auto-arrancable, por ejemplo, un CD-Rom.

Cuando se quiere extraer una imagen de una computadora se debe hacer con la mínima alteración posible para la misma. Una forma de hacerlo es introduciendo un disco boot preparado con las herramientas para extraer la imagen y arrancar la máquina con él.

En algunos casos no es posible o deseable arrancar la máquina sospechosa, por lo que la mejor alternativa es quitar el/los disco/s duro/s de la computadora y ubicarlo en otra más segura, o insertarlo en un sistema especial de recolección de evidencias para su procesamiento. Los dispositivos de duplicación de Hardware como los fabricados por Intelligent Computer Solutions y Logicube son útiles para copiar datos de una unidad IDE o SCSI en otra.

Examen y análisis

Filtrado/reducción de los datos para análisis. Antes de profundizar en los detalles del análisis de una evidencia digital, es necesaria una breve discusión sobre la reducción de los datos a analizar. Con el decremento del coste del almacenamiento de datos y el incremento del volumen de ficheros comerciales en sistemas operativos y aplicaciones software, los investigadores digitales pueden sentirse abrumados fácilmente por la inmensa cantidad de ficheros contenidos en un disco duro. Por consiguiente, los examinadores necesitan procedimientos para centrarse en los datos potencialmente útiles. El proceso de filtrar los datos irrelevantes, confidenciales o privilegiados incluye:

- Identificar ficheros válidos del SISTEMAS OPERATIVOS y otras entidades que no tienen relevancia para la investigación.
- Enfocar la investigación en los datos más probablemente creados por el usuario.
- Gestionar ficheros redundantes, que es particularmente útil cuando se trata con cintas de respaldo.

Otras técnicas menos metódicas de reducción de datos como búsqueda de cadenas específicas de texto o extraer solo ciertos tipos de ficheros, puede no solo hacernos perder pistas importantes, sino que puede dejar al investigador en un mar de datos superfluos. En resumen, una reducción de datos cuidadosa generalmente permite un análisis más eficiente y minucioso.

Búsqueda y recopilación de información. En esta etapa es fundamental tener claro cuáles serían las categorías que llegarían a ser causales de delito o simple suspicacia para de este modo facilitar la búsqueda.

Reconstrucción. Una reconstrucción investigativa nos ayuda a obtener una imagen más completa del delito: que ha pasado, quien causó los eventos, cuando, donde, cómo y porqué. La evidencia digital es una fuente de información rica y a menudo inexplorada. Puede establecer acciones, posiciones, orígenes, asociaciones, funciones, secuencias y más datos necesarios para una investigación. Los ficheros Log son una fuente particularmente rica de fuente de información sobre conductas, ya que graba muchas acciones. Interpretando correctamente la información de varios ficheros log, es a menudo posible determinar lo que hizo un individuo con un alto grado de detalle. Las piezas individuales de datos digitales pueden no ser útiles por sí mismas, pero pueden revelar patrones cuando las combinamos. Si una víctima lee su correo a una hora específica o frecuenta una zona particular de internet, una ruptura en este patrón puede ser el indicativo de un evento inusual. Un delincuente puede solo trabajar los fines de semana, en un cierto lugar, o de una única manera. Teniendo esto en cuenta podemos decir que existen

tres formas de reconstrucción que deberían realizarse cuando se analizan evidencias para desarrollar una imagen más clara de un delito y ver discrepancias o brechas.

- Análisis Temporal (cuando): ayuda a identificar secuencias y patrones de tiempo en los eventos.
- Análisis Relacional (quien, qué y donde): los componentes de un delito, su posición e interacción.
- Análisis Funcional (como): qué fue posible e imposible

Análisis temporal. Cuando se investiga un delito, es normalmente deseable conocer la fecha, la hora y la secuencia de eventos. Afortunadamente, además de almacenar, recuperar, manipular y transmitir datos, los ordenadores mantienen muchos registros de tiempo. Por ejemplo, la mayoría de los sistemas operativos están al tanto de la creación, modificación y acceso de ficheros y directorios. Estos "sellos de tiempo" pueden ser muy útiles a la hora de determinar qué ocurrió en la computadora. En una investigación de robo de propiedad intelectual, los sellos de tiempo de los ficheros pueden mostrar cuanto tardó el intruso en localizar la información deseada en un sistema y a qué ficheros accedió. Una mínima cantidad de búsqueda (ficheros accedidos por el intruso), indica que conocía bien el sistema atacado y una gran búsqueda indica menos conocimiento del sistema. En una investigación de pornografía infantil, el sospechoso declara que su esposa puso pornografía en su ordenador personal sin su conocimiento durante su amarga separación para que repercutiera negativamente en la batalla por la custodia de sus hijos. Sin embargo, los sellos de tiempo de los ficheros indican

que fueron ubicados en el sistema mientras su enemistada esposa estaba fuera del país visitando a su familia. También, el ordenador del sospechoso contenía restos de e-mails y otras actividades online, indicando que había usado la computadora en ese tiempo.

Análisis relacional. En un esfuerzo para identificar relaciones entre sospechosos, la víctima y la escena del crimen, puede ser útil crear un grafo con nodos que representan lugares en los que se ha estado o acciones que se han realizado, como IPs, e-mails, transacciones financieras, números de teléfono marcados, etc., y determinar si hay conexiones destacables entre esos nodos. Por ejemplo, en una investigación de fraude a gran escala, representando transferencias de fondos dibujando linas entre individuos y organizaciones se puede revelar la mayor parte de la actividad en el fraude. Igualmente, trazando los mensajes de e-mail enviados y recibidos por un sospechoso podría ayudar a desvelar a supuestos cómplices por el gran número de mensajes intercambiados.

Es posible que con tanta información parezca que nada está conectado. Los investigadores deben decidir cuánto peso asignar a las relaciones que encuentren. Estas reconstrucciones dan mejores resultados en diagramas con pocas entidades. A medida que se incrementan las entidades y relaciones se incrementa la dificultad de identificar las conexiones importantes. Para facilitar esta tarea existen herramientas que ofrecen la posibilidad de realizar diagramas y asignar pesos a cada conexión. Además se están desarrollando otras herramientas que permiten trabajar con muchas entidades usando algoritmos sofisticados.

Análisis funcional. Cuando se reconstruye un delito, a menudo es útil considerar qué condiciones fueron necesarias para hacer que ciertos aspectos del delito fueran posibles. Por ejemplo, a menudo es útil testear el hardware original para asegurarnos de que el sistema fue capaz de realizar algunas acciones básicas, como chequear la capacidad de una unidad de disquetes para leer/escribir si tenemos un disquete con evidencias. En una investigación hay varios propósitos para evaluar cómo funcionaba un sistema computacional:

- Para determinar si el individuo o la computadora tenían capacidad para cometer el delito.
- Para ganar un mejor entendimiento de una parte de la evidencia digital o del delito en general.
- Para probar que la evidencia digital fue manipulada indebidamente.
- Para comprender los motivos e intenciones del agresor. Por ejemplo, si fue algo accidental o premeditado.
- Para determinar el funcionamiento del sistema durante el lapso de tiempo pertinente.

Debemos tener en mente que el propósito de la reconstrucción funcional es considerar todas las posibles explicaciones para un determinado conjunto de circunstancias, y no simplemente responder a la cuestión que se plantea.

Puede ser necesario determinar cómo un programa o computador estaba configurado para ganar un mejor entendimiento de un delito o una parte de una evidencia digital. Por ejemplo, si se requiere un password para acceder a cierta computadora o programa, este detalle funcional debería ser anotado. Conociendo que un cliente de e-mail estaba configurado para chequear automáticamente el correo en busca de mensajes nuevos cada 15 minutos, puede ayudar a los investigadores a diferenciar actos humanos de actos automáticos.

Publicación de conclusiones. La última fase de un análisis de evidencias digitales es integrar todo el conocimiento y conclusiones en un informe final que dé a conocer los descubrimientos a otros y que el examinador puede tener que presentar en un juicio. La escritura de un informe es una de las fases más importantes del proceso, ya que es la única presentación visual que otros tendrán sobre el proceso entero. A menos que los descubrimientos sean comunicados claramente en el informe, es improbable que otros aprecien su significancia. Un buen informe que describe claramente los descubrimientos del examinador puede convencer a la oposición a llegar a un acuerdo en un juicio, mientras que un informe pobre puede animar a la oposición para ir a juicio. Las suposiciones y la falta de fundamentos resultan en un informe débil. Por tanto, es importante construir argumentos sólidos suministrando todas las evidencias encontradas y demostrando que la explicación proporcionada es la más razonable.

Mientras sea posible, respaldar las suposiciones con múltiples fuentes independientes de evidencia e incluyendo todas las pruebas relevantes junto con el informe ya que puede ser necesario en un juicio hacer referencia a las mismas cuando se

explican los descubrimientos en el informe. Establecer claramente cómo y dónde se encontró toda la evidencia para ayudar a los que tomarán las decisiones a interpretar el informe y permitir a otros examinadores competentes a verificar resultados. Presentando escenarios alternativos y demostrando porqué son menos razonables y menos consistentes con respecto a la evidencia puede ayudar a reforzar las conclusiones clave. Explicando por qué otras explicaciones son improbables o imposibles demuestra que el método científico fue aplicado, es decir, que se hizo un esfuerzo para desmentir la conclusión alcanzada por el examinador, pero que esta resistió un escrutinio crítico. Si la evidencia digital fue alterada después de recopilarla, es crucial mencionar esto en el informe, explicando la causa de las alteraciones y sopesando su impacto en el caso (por ejemplo, insignificante, severo). A continuación se muestra una estructura simple para un informe:

Introducción: Número de caso, quien requirió el informe y qué se buscaba, quien escribió el informe, cuando y que se encontró.

Resumen de la evidencia: resumir qué evidencias se examinaron y cuando, valores MD5, cuando y donde se obtuvo la evidencia, de quién y su condición (anotar signos de daño o sabotaje)

Resumen del análisis: resumir las herramientas usadas para realizar el análisis, cómo se recuperaron los datos importantes (por ej: si se des-encriptaron, o se recuperaron ficheros borrados) y como se descartaron ficheros irrelevantes.

Análisis del sistema de ficheros: inventario de ficheros importantes, directorios y datos recuperados que son relevantes para la investigación con características importantes como nombres de ruta, marcas de tiempo, valores MD5, y localización física de los sectores en el disco. Nótese cualquier ausencia inusual de datos.

Análisis/Reconstrucción: describir e interpretar el proceso de análisis temporal, relacional y funcional.

Conclusiones: el resumen de conclusiones debería seguir a las secciones previas en el informe y debería hacer referencia a la evidencia hallada y a la imagen reconstruida a partir de ellas.

Glosario de Términos: explicaciones de términos técnicos usados en el informe - Apéndice de soporte: la evidencia digital usada para alcanzar las conclusiones, claramente numerada para su referencia.

Además de presentar los hechos en un caso, los investigadores digitales generalmente interpretan la evidencia digital en el informe final. La interpretación implica opinión, y cada opinión suministrada por un investigador tiene una base estadística. Por tanto en un informe el investigador debe indicar claramente el nivel de certeza que tiene cada conclusión y cada parte de la evidencia para ayudar en un juicio a darles un peso a cada una. La Escala de Certeza de Casey(C-Scale, Casey Certainly Scale) proporciona un método para transmitir certeza cuándo nos refereimos a una evidencia digital en un contexto dado y cualificar las conclusiones apropiadamente.

3.5 Procesamiento y Análisis de la Información

El respectivo análisis de la información se realizara cuando la fecha de observación estructurada contenga los resultados de los laboratorios, los cuales se generaran durante la ejecución de la investigación como se muestra en el cronograma de actividades.

Capítulo 4. Diagnostico Situacional

La informática forense es una disciplina relativamente nueva y poco aplicada en Colombia. Por ello, creemos que no existe una metodología que sea referencia nacional, la cual permita garantizar que el proceso forense cumpla con su cometido de aplicar técnicas científicas y analíticas e infraestructura tecnológica para identificar, preservar, analizar y presentar evidencia, de manera que sea admisible en un proceso legal. Se Considera que en muchos casos, la manipulación de la evidencia se hace de una forma equivocada, si no se respetan los protocolos internacionales del manejo de evidencia digital, sin embargo, lo que se toma como mundialmente válido son las mejores prácticas, como las del Servicio Secreto de EUA y recomendaciones de organismos especializados como el NIST o el proyecto CTOSE por lo que es necesario sentar las bases de un procedimiento que permita recuperar y preservar la información de un dispositivo de almacenamiento, como un disco duro. Por otra parte en Colombia se pueden ver los esfuerzos por avanzar en el tema ya que con el nacimiento de GITEC-DIJIN en el año de 2008, y su progresivo crecimiento tanto técnico como en infraestructura, en el marco de su estrategia de implementación tecnológica, se crea un punto departida en la estandarización de la investigación forense en el país.

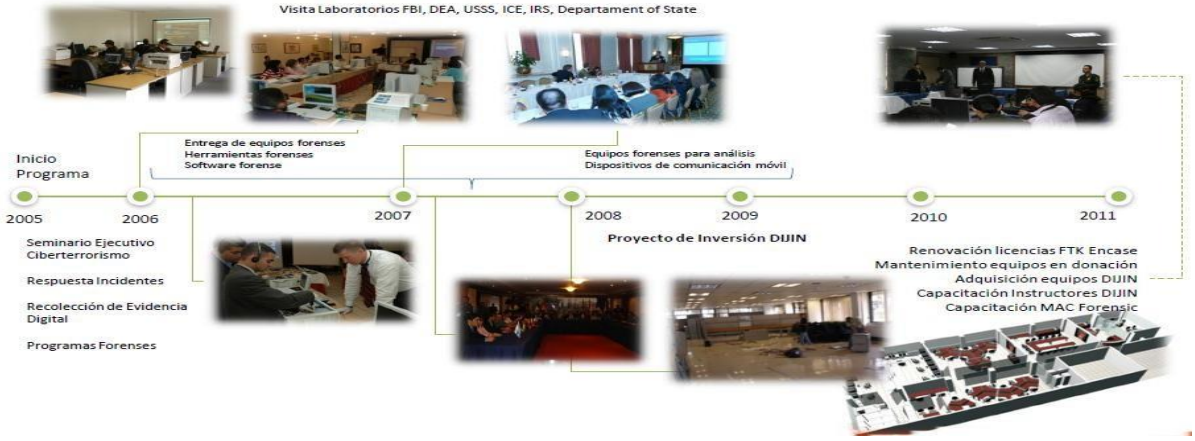
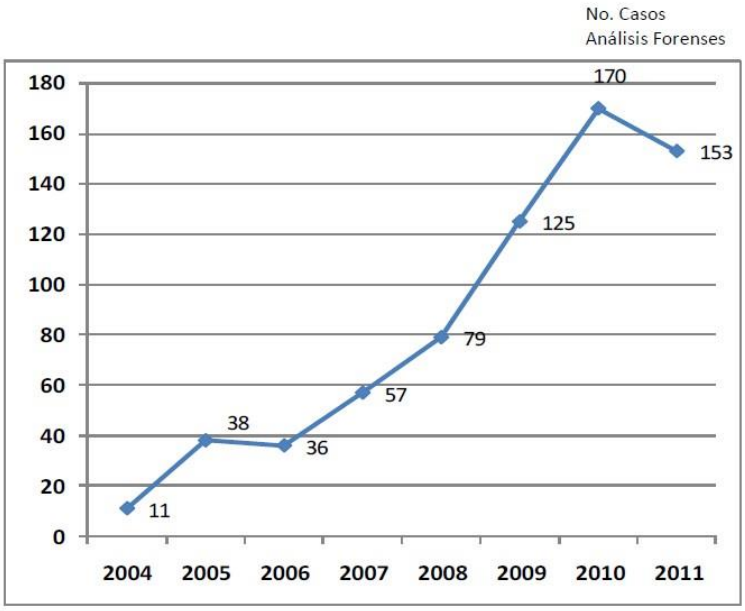


Figura 7. Desarrollo GITEC-DIJIN

Fuente: seminario internacional seguridad de la información: nuevos retos "recolección de evidencias". Policía Nacional. Subintendente, Yair Vanegas Rodríguez. Octubre 2011

Actualmente el grupo de investigación GITEC-DIJIN ha realizado enormes avances desde lo institucional con miras al fortalecimiento y evolución de la informática forense en Colombia; el trabajo de la DIJIN desde sus 45 seccionales y 145 expertos en ciber-terrorismo en aspectos como la extracción de archivos borrados, fragmentos de archivos, Desciframiento de contraseñas de archivos, Reconstrucción de actividades WEB – historial, Archivos ocultos – códigos malicioso y la cobertura en varias de las más importantes ciudades del país (Cali, Medellín, Bucaramanga, Barranquilla); han dado como resultado el crecimiento exponencial de los casos forneces entre 2004 y 2011(ver figura 8)



AÑO	GB
2004	804
2005	1795
2006	2767
2007	4900
2008	11.039
2009	20.480
2010	32.844
2011	40.670

No. Gigabytes
Analizados

Figura 8. Casos forense entre 2004 y 2011
Fuente: seminario internacional seguridad de la información: nuevos retos "recolección de evidencias". Policía Nacional. Subintendente, Yair Vanegas Rodríguez. Octubre 2011

El CONPES No. 3701 de 2011 que busca Contrarrestar el incremento de las amenazas informáticas que afectan la infraestructura critica del país contempla la creación de Grupo de respuesta a incidentes cibernéticos de Colombia colCERT, como respuesta al creciente número de incidentes en el país, así como la diversificación de los delitos informáticos. Dicho ente junto con el COMANDO CONJUNTO CIBERNETICO que es el Equipo encargado de la defensa del país en el ciberespacio y el CENTRO CIBERNÉTICO POLICIAL que es el equipo encargado de la seguridad ciudadana en el ciberespacio; colaboran activamente en la resolución de incidentes en lo que se refiere a Asistencia técnica, Coordinación en la gestión de incidentes, Asistencia ante emergencias, Desarrollo de capacidades operativas, Proveer información estratégica de inteligencia, Asesoramiento y apoyo en ciber-defensa así como en la Coordinación de respuesta ante incidentes. (Compes No. 3701 de 2011.)

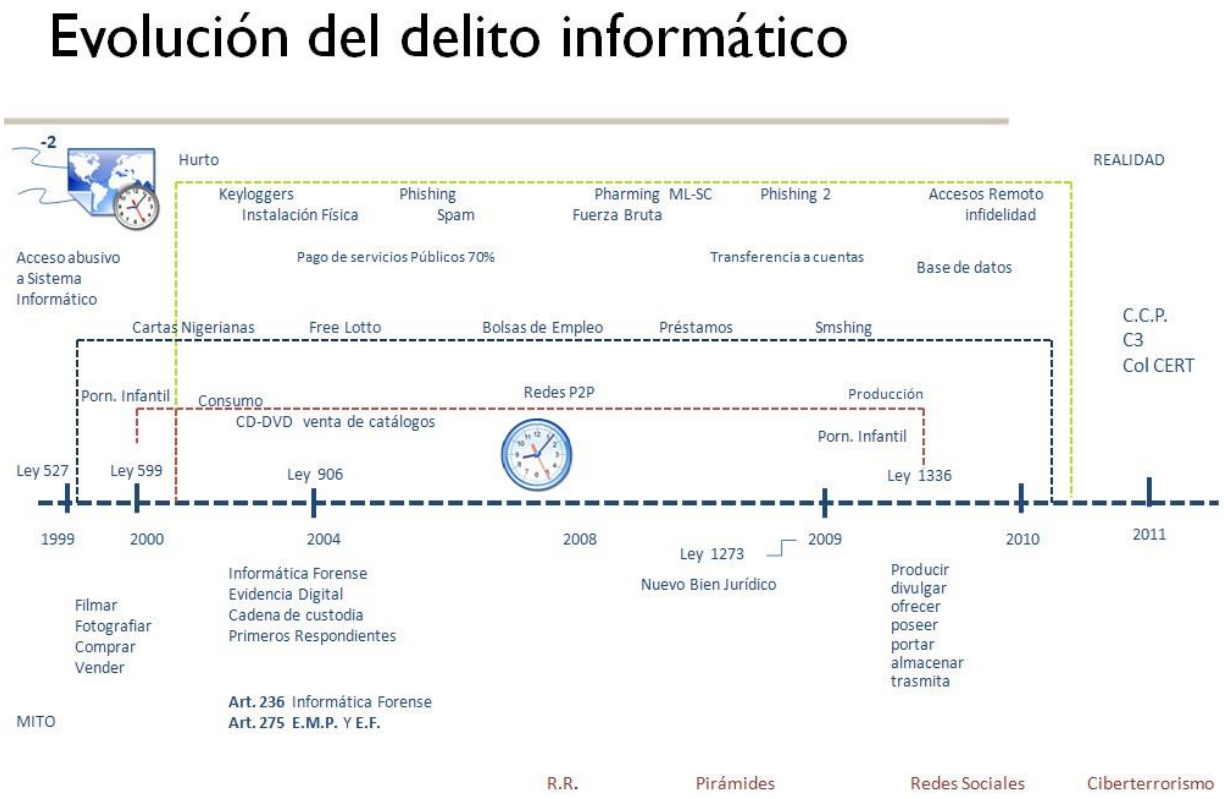


Figura 9. Evolución de los delitos informáticos
Fuente: Lineamientos de Política para Ciber-seguridad y Ciber-defensa, Centro Cibernético Policial, Policía Nacional de Colombia, marzo 2012

Algunos autores (como Brian Carrier y Eugene Spafford) prefieren omitir el término forense, ya que entonces el análisis variará en función de las leyes del país o países en los que se pretende presentar las evidencias como prueba judicial, y sin embargo, existen pautas comunes a la hora de realizar el análisis, al margen de las leyes que imperen en el país determinado. También es posible realizar un análisis de sistemas de información en un entorno corporativo, donde el término forense pierde su sentido.

Para Carrier el análisis forense se reduce a una investigación digital y esta es un proceso en el que se desarrollan y ponen a prueba las hipótesis que respondan a preguntas sobre los eventos digitales. Esto se hace utilizando el método científico en el que se desarrolla una hipótesis con evidencia que nos encontramos y luego probar la hipótesis mediante la búsqueda de más evidencia que muestra que la hipótesis es imposible. La evidencia digital es un objeto digital que contiene información confiable que apoya o refuta una hipótesis. (Carrier, Brian. 2005)

4.1 Selección de las Herramientas y SUIT FORENSE

Actualmente existen multitud de aplicaciones destinadas al análisis forense que trabajan sobre distintos aspectos de la máquina a analizar, por ejemplo, sobre las memorias, los discos de almacenamiento, los protocolos de red, las aplicaciones, etc.

También existen suites que ofrecen el análisis sobre varios de estos puntos ofreciendo herramientas verdaderamente potentes y útiles. No obstante, no existe ni la herramienta definitiva ni aquella aprobada y validada por ningún estándar. A continuación se hará un repaso de las herramientas más populares con una breve descripción y su ámbito de trabajo.

4.1.1. Herramientas de análisis de red

Snort: Es un sistema de detección de intrusiones basado en red aunque también se utiliza como analizador. Permite generar un registro de todos los sucesos que afecten al sistema que se está analizando. Funciona mediante filtros que se deben configurar de una manera u otra en función de nuestro objetivo.

Nmap: Este software es un potente analizador de puertos muy utilizado tanto a nivel de auditorías de seguridad como para extraer evidencias en una investigación forense.

Wireshark: Utilidad muy extendida que permite analizar protocolos de red y analizar el tráfico que se captura en una red. Genera reportes que son exportados a archivos de texto para un posterior análisis forense.

Xplico: Es un framework forense para realizar tareas de análisis de datos recopilados en capturas de red, soporta múltiples protocolos. Según cuenta en su página web, permite analizar archivos de captura de datos, en formato PCAP, y los separa en función de los distintos protocolos. Este método ayuda a una mejor comprensión de los datos capturados. Además es posible analizar archivos de gran tamaño. Destaca la funcionalidad de pre visualizar las imágenes que hayan sido accedidas durante el periodo de captura. También es de destacar el análisis de peticiones DNS que permiten analizar a qué sitios web se accedieron.

4.1.2. Herramientas para tratamiento de memoria

Volatility: Es un conjunto de herramientas desarrolladas en Python. Permite hacer volcados de memoria de máquinas con sistemas operativos Windows, Linux, Mac OSX e incluso Android. Trabaja con versiones tanto de 32 como de 64 bits. Volatility.

Es capaz de analizar volcados con datos en raw, crash dumps de sistemas Microsoft Windows, etc. A partir de los datos se pueden extraer, por ejemplo, tipo de sistema, fecha y hora, puertos abiertos, ficheros cargados por procesos, así como DLL, módulos del kernel, direccionamiento de memoria por procesos, claves de registro utilizadas en los procesos, etc.

Memoryze: Permite la captura de memoria RAM en equipos con sistemas operativos Windows y OSX. (Memoryze Mandiant.

RedLine: Como la aplicación anterior, también permite la captura de memoria y su posterior análisis. Además dispone de entorno gráfico

4.1.3. Herramientas para el análisis de aplicaciones

OllyDbg: Esta aplicación permite desensamblar y depurar aplicaciones o procesos para Windows. Carga y permite debugar DLLs y escaneo de todo tipo de archivos. No requiere instalación así que no creará nuevas entradas en el registro de la máquina donde se instala.

OfficeMalScanner: Es una utilidad que permite escanear archivos de la *suite Office*, en busca de códigos maliciosos, por ejemplo, en macros, conectores OLE o ficheros encriptados.

Radare: Aplicación multiplataforma, Linux, Android, OSX, Windows e incluso Solaris que permite aplicar ingeniería inversa para analizar código de una aplicación maliciosa que se ha ejecutado.

Process explorer: Muestra información de los procesos que hay abiertos en un máquina. Es una herramienta útil para la localización de problemas de versión de DLL o pérdidas de identificadores. También ofrece detalles internos acerca del funcionamiento de Windows y aplicaciones.

4.1.4. Selección de la suite forense

Inicialmente repasaremos algunas de las suites forenses más populares para partir de esta revisión realizar el análisis respectivo:

Encase: Es un software de investigación forense informática, que tiene la capacidad de realizar análisis complejo de evidencia digital. Entre sus principales características tenemos (Encase Forensic". 2011)

- Amplia compatibilidad de formatos disponibles.
- Amplia compatibilidad de correos electrónicos disponibles.
- Amplia compatibilidad con navegadores disponibles.
- Análisis y generación de informes de manera detallada.
- Recopilación inteligente de evidencia digital.
- Validado por los tribunales de justicia.

Deft extra: Es una interfaz Gráfica de Computo Forense que asiste en el análisis forense de discos, redes y navegadores. Esta herramienta está dividida en seis secciones que incluyen diversas herramientas forenses las cuales se detallan a continuación.

Información del Sistema (SysInfo)

Adquisición Viva (Live Adquisition)

Forense (Forensics)

Búsqueda (Search)

Utilidad (Utility)

Reporte (Report)

CAINE: (Computer Aided Investigative Environment) El Entorno de Investigación Asistido por Computadora es una distribución italiana de GNU/Linux que ofrece herramientas forenses como módulos de software. Ha sido diseñado de manera que garantice las siguientes características (C.A.IN.E)

- Entorno que sirva de apoyo al investigador en las cuatro fases
- Forenses Digitales.
- Interfaz gráfica amigable.
- Generación semiautomática de un informe final.

Digital Forensics Framework: Es una herramienta basada en Python con un módulo de sistema flexible para investigación forense digital de memorias USB, PDA, tarjetas de memoria y celulares. Entre sus principales características tenemos.

- Recuperación potente de archivos borrados.
- Análisis del sistema de archivos de teléfonos móviles.
- Descifrar contenido y metadatos de SMS para mostrarlos como en un teléfono móvil.

Forensc ToolKit: Es un estándar de tecnología de investigación informática forense. Entre sus características principales tenemos:

- Análisis de vanguardia.
- Descifrado y craqueo de contraseñas.
- Interfaz intuitiva.
- Es personalizable y fácil de usar.
- Potente velocidad de procesamiento.

Easy Recovery Professional: Es una solución para recuperar datos, reparar archivos, correo electrónico y realizar diagnóstico de discos. Posee soporte para

- Discos duros IDE/ATA/EIDE/SATA/SCSI
- Discos extraíbles.
- Disquetes.

- Soportes periféricos.
- Soportes digitales

Fox analysis: Es una herramienta que permite el análisis de los datos generados por el uso de Mozilla Firefox fue desarrollada con el fin de ayudar en investigación forense digital. Sus funcionalidades principales son (FoxAnalysis". 2010)

- Extracción de marcadores, cookies, descargas, inicios de sesión.
- Analizar datos con opciones de filtrado:
- Por palabras claves
- Rangos de fechas.
- Estado de la descarga.
- Por selección.
- Informe de actividad de exportación.

Chrome Analysis: Es una herramienta que permite el análisis de los datos generados por el uso de Google Chrome fue desarrollada con el fin de ayudar en investigación forense digital. Sus funcionalidades principales son (Chrome Analysis". 2010)

Extracción de marcadores, cookies, descargas, inicios de sesión.
Analizar datos con opciones de filtrado:
Por palabras claves
Rangos de fechas.

Estado de la descarga.

Por selección.

Informe de actividad de exportación.

Para la elección de las herramientas de software más adecuadas hemos tomado en cuenta varios criterios de selección, de acuerdo al laboratorio que deseamos plantear que cumpla con las necesidades actuales y sea factible de implementar. Dichos criterios se exponen a continuación:

Tabla 3.

Criterios para la selección de Suit Forense

Criterios de evaluación/ Suit forense	Deft Extra		Digital	Forensc	Recovery	Easy	Fox Analysis	Chrome
Software Libre	✓	✓	✓	✓			✓	✓
Estándar Industrial	✓	✓		✓	✓			
Multiplataforma	✓	✓	✓	✓		✓		

Fuente: Laboratorios del investigador y análisis bibliográfico

La comparación de la figura 10 ofrece una panorama inicial de las características de cada una de las herramientas con referencia a la licencia y la capacidad de realizar un análisis multiplataforma, lo cual es sumamente importante; no obstante es necesario además de esto

identificar y evaluar la funcionabilidad y versatilidad de cada una de estas, razón por la cual a continuación realizaremos una inspección un poco mas profunda.

Tabla 4.

Análisis de funcionamiento Suit Forense

Características/Suits		**Deft Extra**		**Digital**	**Forensc**	**Recovery**	**Easy**	**Fox Analysis**	**Chrome**
Clonación de discos	✓	✓			✓				
Comprobar integridad criptográfica	✓	✓		✓	✓				
Información del Sistema	✓	✓	✓		✓				
Adquisición en vivo	✓	✓	✓		✓				
Recuperación de contraseñas	✓	✓	✓		✓				
Recuperación de archivos borrados	✓			✓	✓	✓			
Recuperación de eMails borrados	✓				✓				
Análisis forense en redes	✓	✓	✓						
Análisis forense en Navegadores	✓	✓	✓		✓			✓	✓
Análisis de firmas de archivos	✓	✓							
Búsqueda de archivos	✓	✓			✓				
Utilitarios extra		✓	✓						
Reporte manual		✓							
Reporte automático	✓				✓				

Volcado de memoria RAM	✓	
Adquisición de evidencia RAM	✓	
Herramientas de automatización	✓	

Fuente: Laboratorios del investigador y análisis bibliográfico

A continuación se cuantifica el porcentaje de efectividad para las áreas en las cuales fueron evaluadas las diferentes Suit:

Tabla 5.

Comparación porcentual de herramientas forense.

Encase	Defta Extra	Cain	Digital Forensic Framework	Forensc Tool Kit	Easy Recovery Pro	Fox Analysis	Chrome Analysis
82%	**70%**	**41%**	**11%**	**41%**	**11%**	**5%**	**5%**

Fuente: Laboratorios del investigador y análisis bibliográfico

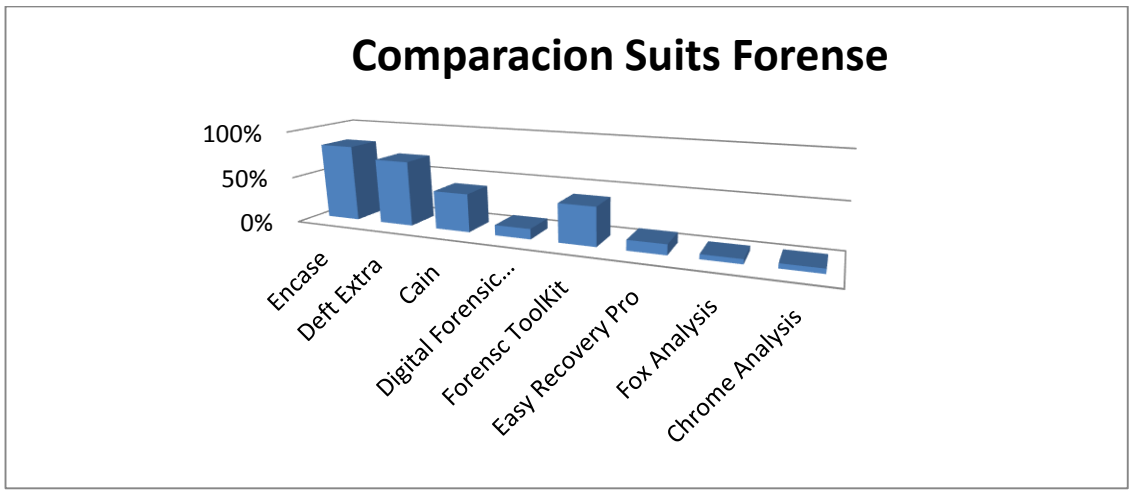


Figura 13: Comparación grafica de herramientas forense.
Fuente: Laboratorios del investigador y análisis bibliográfico.

Como se puede observar las Suits que mejor cumplen con las necesidades del estudio son en su orden:

- Encase
- Deft Extra
- Cain
- Forensic ToolKits

Dentro de estas el estudio se verá abocado a escoger Deft Extra como la Suit base, pero teniendo en cuenta que Cain será importante en el análisis de memoria. Las otras dos distribuciones no son tenidas en cuenta gracias a la naturaleza de su licencia ya que son software propietario.

4.2 Diseño de laboratorios

4.2.1. Análisis de las evidencias

La fase de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, así que en cualquier momento debemos poder montar un entorno donde reproducir la investigación y mostrarlo a quién lo requiera. Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

- Sistema operativo del sistema.
- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:
- Si dispone de *firewall*, ya sea físico o lógico.
- Si el equipo se encuentra en zonas de red especiales, por ejemplo, *DMZ.*

- Si tiene conexión a Internet o utiliza *proxies.*
- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Para ayudar al desarrollo de esta fase del análisis forense podemos centrarnos en varias subfases o puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar. No será lo mismo analizar un equipo con sistema operativo Windows o con Linux. Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un *malware* que destruya información de una ubicación de disco o un *malware* que envíe todo lo que se teclea en un equipo.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

4.2.2. Preparar un entorno de trabajo

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un análisis en frío, lo más sencillo es preparar una máquina virtual con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello, previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

Las pruebas realizadas en la presente investigación, se basan en escenarios experimentales con ambientes controlados, dentro de, los cuales se recrearon incidentes de seguridad que comprometían estaciones de trabajo a diferentes niveles; así mismo se recurrió a retos forenses para la adquirían de imágenes.

4.3. Metodología propuesta

Con la llegada de la sistematización de procesos, las diversas corporaciones y empresas pasaron a tener toda su información digital, con lo cual se agilizaron e hicieron mucho más eficientes los procesos; no obstante, esto trajo un nuevo problema, y este fue la seguridad puesto que con la instauración de la información como principal activo de las empresas, también se hizo el más apetecido por los atacantes.

Si hay algo claro en el mundo de la información es que no existe un sistema que sea totalmente seguro, y evádeteme mente se presentan incidentes de seguridad, ante los cuales las preguntas son muchas ¿Cuál fue el origen del ataque? ¿Qué implicaciones tuvo el incidente? ¿Qué medidas son necesarias para evitar situaciones similares en el futuro? Es entonces cuando el análisis digital forense hace su aparición para despejar todas las dudas, puesto que durante, y después del incidente fuere cual fuere su origen, el atacante deja rastros, los cuales son habidos de ser estudiados tanto en entornos de red como en el espacio local de la terminal atacada, así mismo la memoria RAM y demás dispositivos que puedan albergar información como lo son smatphone , impresoras, memorias USB, discos flexibles, DVD entre otros, son medios habidos de ser analizados.

No obstante dentro de la gran cantidad de enfoques y conceptos que encierra el análisis forense, es claro que la implementación de una metodóloga practica que indique de modo directo la forma en la cual realizar la investigación, constituye poco menos que una quimera pues la complejidad misma del estudio impediría tal iniciativa, pero a pesar de

ello se pueden ahondar esfuerzos para proporcionar a una guía que indique los pasos tanto metodológicos como prácticos en un sentido amplio que permita al investigador partir de un punto claro; en tal sentido se pretende a continuación fundamentándose en la metodología Casey, el RFC 3227 y la ISO/IEC 27037:2012.

Dentro del anexo 1 se encuentra desglosada la metodología que constituye el producto del presente trabajo.

.

Capítulo 5. Conclusiones

En este último capítulo vamos a repasar tanto el trabajo realizado como el posible trabajo futuro que se podría derivar de este. También destacaremos los principales problemas encontrados a lo largo del mismo y a qué conclusiones se puede llegar.

Como ya se ha visto a la largo de todo el trabajo, en la actualidad, no hay ninguna guía oficial, ni ningún estándar publicado que detalle todos y cada uno de los pasos que debe dar un investigador a lo largo de un caso. Esto provoca que cada profesional trabaje de un modo distinto y que cada uno aplique sus normas y conocimientos de la mejor manera posible o según los recursos de que disponga.

Aun así, existen varios documentos publicados por organismos de certificación y también por entidades dedicadas a la seguridad informática, así como departamentos de policía y de

justicia que han publicado diversos documentos que pueden servir de ayuda y referencia para los profesionales investigadores forenses.

Son ejemplos de estos documentos, la RFC 3227, las UNE 71505 y 71506 o incluso la ISO 7037 que pueden servir de guía para determinados casos y resultar un buen punto de partida para determinadas situaciones.

En este trabajo, tras el análisis de la situación actual y viendo la necesidad de una metodología para el análisis forense se ha determinado la necesidad de crear dicha metodología de trabajo y para ello se ha partido de las consideraciones y ayudas de muchos de estos documentos.

Uno de los problemas que han surgido para la elaboración de esta metodología ha sido la gran variedad de situaciones que se dan en un análisis forense. Resulta casi imposible analizar todas y cada una de estas situaciones y por lo tanto se ha optado por intentar describir las situaciones más habituales que se pueden dar en función del tipo de investigación, sea con unos fines u otros. La idea es generar una metodología de análisis lo más versátil posible y que se pueda adaptar al máximo de situaciones posibles. La metodología creada se basa en un análisis de 5 fases, a saber, asegurar la escena, identificar y recolectar las evidencias, preservarlas, analizar las evidencias obtenidas y redactar los informes pertinentes con los resultados obtenidos.

En base a esta consideración no cabe decir que ha resultado imposible, por la extensión y tiempo de dedicación de este Trabajo de Final de Máster, realizar un examen exhaustivo de todas las posibles variantes y como solucionar o afrontar todas ellas.

En este trabajo también se ha realizado un repaso a la normativa legal vigente, en el momento de redacción del trabajo, de las leyes, tanto nacionales como internacionales, que vale la pena conocer en este ámbito. El conocimiento de la legislación es importante de cara al investigador puesto que ayuda a conocer los límites de la investigación así como determinar qué casos pueden, o no, ser constitutivos de delito.

Del mismo modo, se ha realizado una pequeña investigación sobre los programas más utilizados en la investigación forense organizándolos en base a sus usos, por ejemplo, análisis de memorias, de discos, de redes u otros. Este resumen de aplicaciones es vigente en el momento de redacción de esta guía pero hay que recordar que la evolución del *software* y la aparición y desaparición de éste es constante.

Capítulo 6. Recomendaciones

En vista de las dificultades surgidas en cuanto a la gran diversidad de casos que se presentan en un análisis forense, un posible trabajo futuro sería crear un conjunto de guías en función de cada finalidad de la investigación.

En base a la clasificación realizada se podrían generar guías para cada finalidad, a saber, preventiva, correctiva, probatoria y auditoria. Además se podría ampliar sustancialmente para los análisis probatorios en función de los equipos involucrados, los sistemas operativos, si hay redes involucradas o no, tipo de ataque sufrido, etcétera.

Posiblemente cada una de estas metodologías detalladas podría dar lugar a varios trabajos de estas características.

Referencias

Camara colombiana de informatica y telecomunicaciones. delitos informáticos. la confianza, principal herramienta de los delincuentes. [en línea]. bogotá. [citado noviembre 25 de 2014] disponible en internet: <url: http://www.ccit.org.co/files/seguridad%20informatica/delitos_informaticos.pdf>

Camara colombiana de informática y telecomunicaciones. avances y retos de la defensa digital en colombia, ed. noviembre de 2014

Lázaro, 2013. Introducción a la informática forense. españa: ra-ma, 340 pp.

Acurio, 2009 acurio, s., 2009. perfil sobre los delitos informáticos en el ecuador. pontificia universidad católica, del ecuador (ecuador). disponible en http://www.criptored.upm.es/guiateoria/gt_m592d.htm

Corte constitucional. sentencia c-209 de 207. descubrimiento de pruebas. [en línea]. bogotá: [citado 24 de noviembre de 2014]. disponible en internet: <url: http://www.corteconstitucional.gov.co/relatoria/2007/c-209-07.htm>

Larrota ardila , martinez zabala, orjuela lópez diseño de una guía para la auditoría de análisis forense en dispositivos moviles basados en tecnología android para legislación colombiana, universidad católica de colombia 2014

The internet engineering task force (ietf). [en línea] https://www.ietf.org

International organization for standardization. [en línea] www.iso.org.

National criminal justice reference service. [en línea] https://www.ncjrs.gov

Brian carrier, Eugene spafford. "gettingphisycalwiththe digital investigationprocess". international journal of digital evidence. economiccrimeinstitute (eci) , utica college. fall 2013, volume 2, issue

Análisis forense informático. historia del análisis forense digital [en línea] disponible en internet en: <http://wwwdi.ujaen.es/~mlucena/bin/proy_forense.pdf>

Análisis forense. cómo investigar un incidente de seguridad [en línea] disponible en internet en: < http://www.k-nabora.com/index.php/blog/ana-lisis-forense.-ca-mo-investigar-un-incidente-de-seguridad-248.html>

Requestforcomments. [on line] disponible en internet en: http://es.kioskea.net/contents://es.kioskea.net/contents

Request for comments: 3227 guidelines for evidence collection and archiving. [on line] disponible en internet: http://www.ietf.org/rfc/rfc3227.txt

Norma iso 27001 [on line] disponible en internet en: http://es.scribd.com/doc/25034834/norma- iso27001

Soluciones en las empresas de ti mediante la aplicación de un sistema de gestión iso 20000 parte 1 integrado a un sistema iso 27001 e iso 9001, josé mª zubieta guillén, escuela técnica superior de ingenieros industriales y de telecomunicación, 2010.[en línea] disponible en internet en: http://academica - e.unavarra.es/bitstream/handle/2454/2166/577243.pdf?sequence=1

Administrar la mesa de servicios e incidentes de la cobit, proceso d8, [en línea] disponible en internet en: http://www.slideshare.net/bluedelacour/ds8-administrar-la-mesa-de-servicio-y-los-incidentes

William Stallings. network security essential, applications and standars. fourthedition. año 2011.

Experiencias de análisis forense en méxico. departamento de seguridad en cómputo / unam-cert en jornadas de análisis forense. madrid, septiembre 2013.

Secretaria senado, ley 1273 de 2009 [en LÍNEA].<HTTP://WWW.SECRETARIASENADO.GOV.CO/SENADO/BASEDOC/LEY/2009/LEY_1273_2009.HTML> [CITADO EL 11 DE ABRIL DE 2010]

Free software foundation, inc. gnu operatingsystem: licencias. [en linea] http://www.gnu.org/licenses/licenses.es.html> [citado el 11 de abril de 2010]

Fundacióncopyleft. copyleft. [en línea] < http://fundacioncopyleft.org/es/9/que-es-copyleft> [citado el 11de abril de 2010]

Instituto colombiano de normas técnicasy certificació. tesis y trabajos de grado. bogotá; icontec, 2002

Grajalestevni. tipos de investigacion [en línea]. disponible en internet en: http://tgrajales.net/investipos.pdf

Puente wilson. técnicas de investigación [en línea]. disponible en: internet en: http://www.rrppnet.com.ar/tecnicasdeinvestigacion.html

Information technology- security tecniques- incident principies and process, iso/iec 2012

Lobo leonard, desarrollo e implementación del análisis digital forense utilizando una metodología post-mortem, [en línea]: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/478

Easey, eoghan. digital evidence and computer crime, third edition: forensic science, computers, and the internet. academic press. p. 840. isbn 978-0123742681

National institute of standards and technology. [on line] disponible en internet en: http://www.nist.gov/public_affairs/general_information.cfm

Request for comments. [on line] disponible en internet en: http://www.ietf.org/rfc/rfc3227.txt

Code of practices for *digital forensics.* [on line] disponible en internet en: http://cp4df.sourceforge.net/porque.html

Compes no. 3701 de 2011. [en línea]. disponible en: internet en carrier, brian. file system forensic analysis. addison-wesley, 2005 http://www.mintic.gov.co/index.php/docs-normatividad?pid=698&sid=741:3701

foxanalysis". 2010.

Chrome analysis". 2010. forensic-software. 10 de mayo 2011. <http://forensic-software.co.uk/chromeanalysis.aspx>

Apoyo para el análisis forense de computadoras, josé arquillo cruz, escuela politécnica superior de jaén, septiembre, 2007

Easey, eoghan. digital evidence and computer crime, third edition: forensic science, computers, and the internet. academic press. p. 840. isbn 978-0123742681.

Experiencias de análisis forense en méxico. Departamento de seguridad en cómputo / unam-cert en jornadas de análisis forense. madrid, septiembre 2005.

Gutiérrez, roberto. párrizas, ángel alonso. curso de análisis forense - tissat-24, 12 enero 2005.

Seguridad en la red y análisis forense, hades. universidad de murcia – facultad de informática. murcia, españa: administración y seguridad en redes.

Apéndice

Apéndice A. Reto forense: Ordenador de un ministerio comprometido

En esta ocasión, nos ha llegado un ordenador de un ministerio que se supone está comprometido con un archivo malicioso. Se trata de un portátil utilizado por un agente de seguridad infiltrado que ha sido descubierto por un delincuente implicado en la trama que se investigaba, y se sospecha que ha sido por un malware que le han instalado en el ordenador que utilizaba.

Para esta ocasión se nos ha encomendado la tarea de realizar un análisis sobre el equipo afectado (máquina virtual). Este equipo se le ha revocado el acceso a la VPN ya que se sospecha que el compromiso ha sido total y hasta que no se extraigan todos los detalles de la intrusión volverá a estar "on-line" en dicha red.

Inicialmente y para conocer esta pericia, el análisis que se nos pide es de tipo "black-box" (sin ningún tipo de pista).

1. ¿Existe un malware en el equipo investigado? Extraer el nombre y contestar a las siguientes preguntas:

- ¿Se clasifica dentro de algún grupo?
- Cuándo se compiló
- ¿Migra el proceso cuando se ejecuta el archivo? ¿A cuál?
- ¿Cambia el ejecutable dependiendo de si se ejecuta en memoria o en disco?
- ¿Cuándo se ejecuta en memoria, el ejecutable tiene alguna cadena sospechosa?
- ¿Qué tipo de malware es?
- ¿Genera algún tipo de log donde guarde la información?

2. En alguna parte del HD del equipo comprometido hay una serie de logs que el agente infiltrado consiguió antes de ser descubierto, pero ante las prisas no recuerda donde lo metió. Menciona que lo guardó junto a una captura de red, es un *.txt y ambos están en el mismo directorio. Una vez encontrada los log:

- ¿Qué protocolo se usa según el archivo?
- ¿Es TCP o UDP?
- ¿Con que herramienta parece haber sido obtenido y cuál es el objetivo de esta herramienta?
- ¿Se puede obtener algún tipo de geolocalización a partir del log?

3. Ya puestos, aprovechamos para analizar la captura de red:

- ¿Qué protocolos se incluyen en la captura?
- ¿Se puede obtener algo más de la captura? En caso afirmativo indicar qué.

Desarrollo

Para la resolución de esta investigación se ha empezado por descargar la imagen que nos han proporcionado sobre el equipo afectado. Una vez descargada se ha realizado una copia sobre la que se ha trabajado manteniendo siempre la versión descargada, intacta, por si ocurría algún problema.

Posteriormente se ha ejecutado la máquina virtual, con sistema operativo Windows XP Service Pack 3. A partir de aquí se han realizado los siguientes pasos:

1. Volcado de memoria sin ejecutar ninguna aplicación para ver qué procesos están activos. También se buscan procesos ocultos y conexiones de red abiertas o puertos en escucha. Esta vía de análisis no arroja ningún resultado positivo. A simple vista no hay ningún proceso *malware* en ejecución ni conexiones sospechosas.

2. Volcado de memoria directamente de la imagen del sistema sin arrancar la máquina virtual. Esta opción está disponible ejecutando por consola de comandos Oracle VM VirtualBox. Con esta opción tampoco se detectan procesos ni ejecutables sospechosos.

3. Se intenta abrir la imagen del sistema con el *software* Autopsy pero este parece no reconocer la imagen y no carga nada. Se convierte el formato VMDK en RAW e IMGcon el *software* "qemu" pero Autopsy tampoco carga la imagen. Se abandona esta vía de análisis.

Hasta el momento se han intentado vías de análisis poco intrusivas con el equipo evitando al máximo las escrituras en disco. Como consecuencia del poco éxito en la búsqueda se decide ejecutar los programas que hay en el equipo y realizar las búsquedas con el buscador del sistema operativo.

1. Se ejecuta el antivirus del sistema, Avast, aun sabiendo que puede estar afectado por cualquier *malware.* No arroja ninguna amenaza.

2. Se utiliza el buscador del sistema operativo para buscar archivos de texto TXT y capturas de red PCAP. Las búsquedas no aportan ningún resultado.

3. Se decide ir directamente a directorios dónde habitualmente se esconden *malwares*, por ejemplo, carpetas de archivos temporales, carpeta SYSTEM32, carpeta WINDOWS, etc. Al intentar acceder a esta última el contenido está vacío a simple vista. Al parecer hay un problema con el sistema de archivos.

4. Reiniciamos el equipo para ver si se corrige y al cargar de nuevo el sistema operativo se solventan, aparentemente, todos los archivos de esa ubicación. Seguimos disponiendo de una copia sin tocar por si esto ha ido mal.

5. Volvemos a buscar todos los archivos TXT y se encuentra el *log* con la captura PCAP en el mismo directorio. Están en C:\WINDOWS\Stole_logs, los archivos son:

a. logs_honeypot_VoIP.txt

b. VoIP attack.pcap

6. A modo de prueba ejecutamos el antivirus del equipo para ver si nos puede ayudar. Efectivamente nos indica que hay un archivo *malware.* Su ruta:

C:\WINDOWS\system32\txu_Ng_0.exe

A partir de aquí podemos empezar a responder las cuestiones planteadas haciendo uso de varias utilidades, tanto instaladas en el propio equipo, como otras de análisis forense y páginas web, tales como virustotal.com

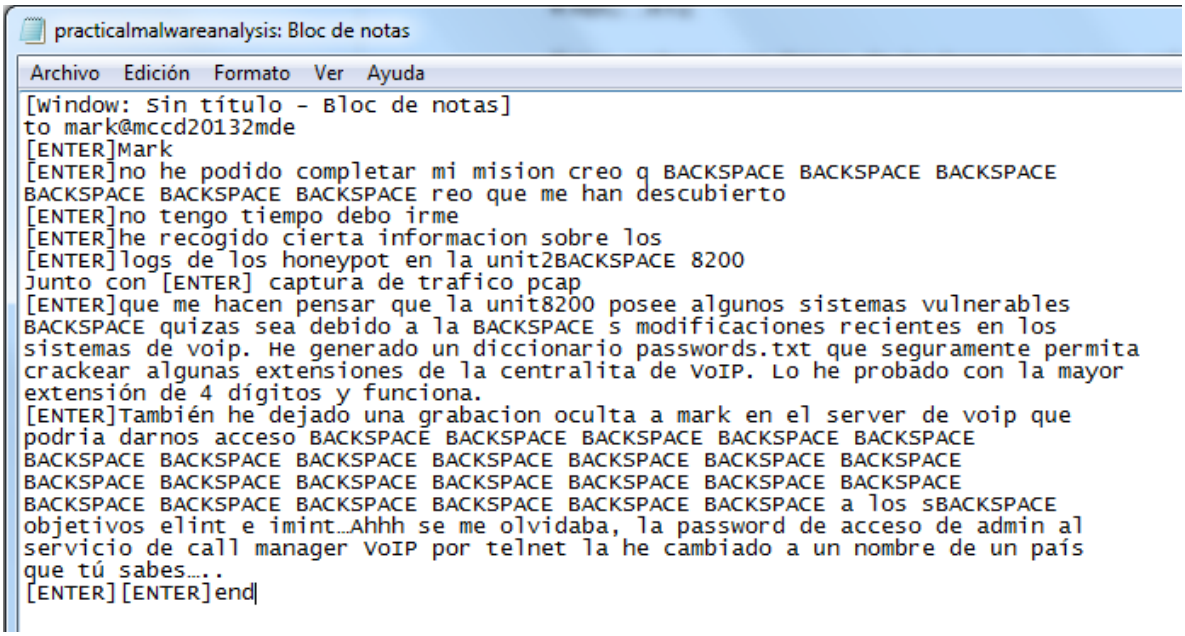
En cuanto al *malware* podemos decir que el ejecutable es de tipo troyano, compilado, según virustotal.com, en fecha 08/04/2011 a las 17:54:23. Se puede observar que cuando se ejecuta carga dos procesos. Por un lado svchost.exe e hijo de este txu_Ng_0.exe. Al poco tiempo de lanzar la ejecución desaparece txu_Ng_0.exe quedando sólo en ejecución svchost.exe, sin padre. Esta forma de actuación es sintomática de *malwares* ya que este tipo de procesos siempre dependen de otros en el sistema. Así pues se confirma que el ejecutable migra cuando se ejecuta.

Analizando las cadenas del ejecutable en memoria podemos ver varias de ellas que son sospechosas:

- [SHIFT]
- [ENTER]
- [TAB]
- abc…xyz
- ABC…XYZ

Estas cadenas son típicas de *keyloggers*, que son aplicaciones que capturan todas las pulsaciones del teclado para saber lo que se ha escrito durante la ejecución.

Lo más habitual es que todo lo que capturen se guarde en un registro. Sucede lo mismo en este caso. En las cadenas del ejecutable podemos ver “practicalmalwareanalysis.log”. Se localiza en la ruta: C:\WINDOWS\system32\practicalmalwareanalysis.log y en su contenido podemos leer, entre otros:



En cuanto al *log* que se guardó en la ubicación C:\WINDOWS\Stole_logs podemos ver que entre otros se usa el protocolo SIP *(Session Initiation Protocol)* que es un protocolo de señalización para VoIP. El otro protocolo que también se aprecia en el archivo es el conocido UDP, sobre el cual funciona el anterior.

Mirando el archivo parece que se ha usado una herramienta llamada “sipvicious”. Si buscamos un poco por Internet se encuentra su web dónde pone que SIPVicious es un conjunto de herramientas que pueden ser usadas para auditar sistema VoIP. Entre sus varias funciones encontramos un escáner SIP, un identificador de extensiones, un *cracker* de contraseñas, etc.

En cuanto a las direcciones IP y su geolocalización encontramos los siguientes datos, haciendo uso de cualquier *whois* en Internet:

- 147.237.72.71: Ministerio de Economía de Israel
- 210.184.120.120: Hong Kong
- 89.42.194.10: Romania

Finalmente en cuanto a la captura de red encontrada, usando Wireshark podemos ver los protocolos implicados en cada captura. En mayor o menor medida se incluyen HTTP, TCP, UDP, RTCP, ICMP, RTP y SIP.

Analizando la captura, concretamente el paquete número 1279 vemos como se accedió al archivo de configuración *sip_custom.conf*. Para acceder se puede ver como se usaron las credenciales de usuario "maint" y password "password". Credentials:
maint:password

Finalmente, Wireshark nos da la opción de descodificar las conversaciones VoIP, para ello
Telephony -> VoIP Calls -> Player -> Decode se seleccionan los dos audios y se escucha la conversación. En ella se puede escuchar que la palabra clave, correspondiente al país que anteriormente se hablaba en otro *log* es México.

Reto forense: maquina virtualizada comprometida

En este caso, hemos recibido un encargo urgente de una instancia de una máquina virtualizada sobre un servidor de un Ministerio, que se presume ha sido comprometido. Por

nuestra parte nos toca realizar el análisis de la memoria. Para ello utilizaremos la herramienta Volatility ya que nos han indicado que el sistema era Windows.

Las tareas que debemos realizar:

1. Instalar volatility

2. Conocer las opciones que nos serán de utilidad

3. Implementar un informe que dé respuesta a las siguientes preguntas:

- ¿De qué sistema operativo se trata?
- Indicar si la máquina ha sido comprometida. En caso afirmativo indicar, en la medida de lo posible extraerlo. Evaluar su persistencia en el sistema.
- ¿Existen procesos, dll's o módulos ocultos en el sistema o direcciones IP a las que se conecte? En caso afirmativo tratar de descubrirlos.

Resolución

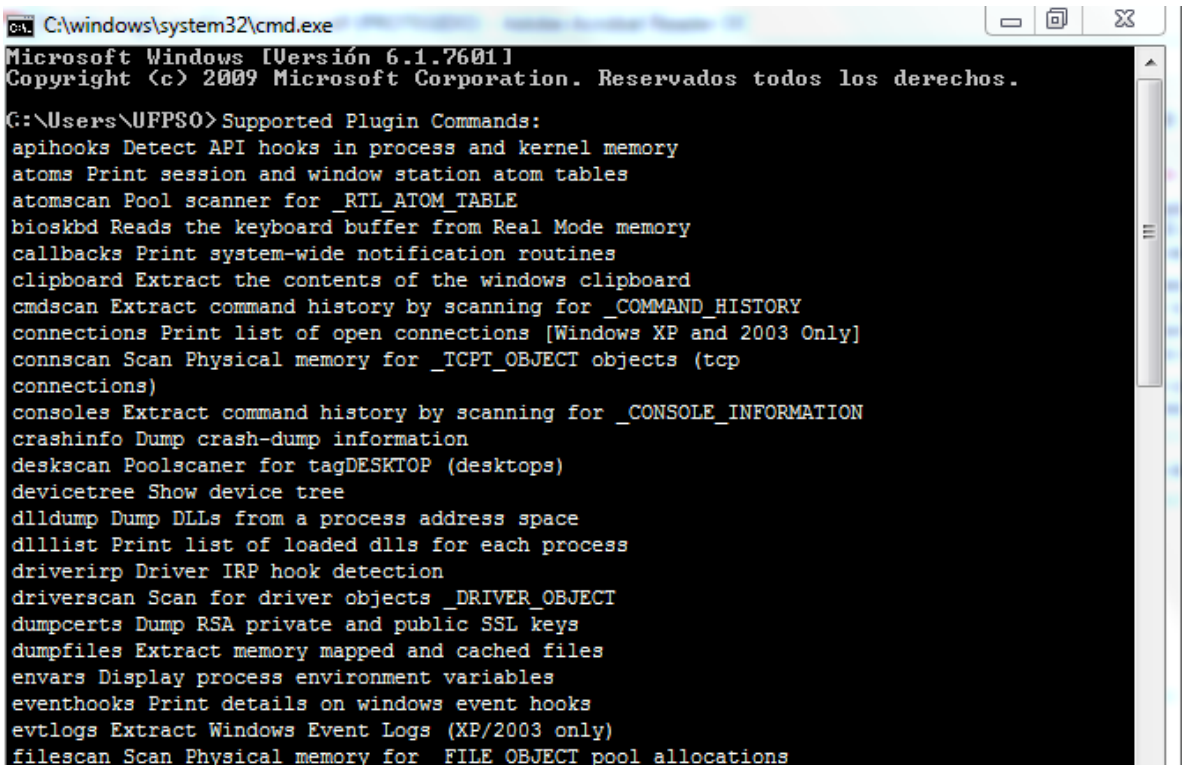
Para la realización del informe se ha usado la herramienta de análisis de memoria "Volatility". El contenido del fichero *memoria.dd* a analizar se corresponde con el volcado de la memoria de una máquina virtual con sistema operativo Windows.

El primer paso para solventar la práctica es la instalación de la herramienta. En este caso se va a utilizar la versión 2.3.1 y más concretamente el ejecutable que no requiere instalación de la herramienta. Esta herramienta se puede ejecutar directamente desde consola mediante los comandos que necesitemos para ir desgranando la información que buscamos.

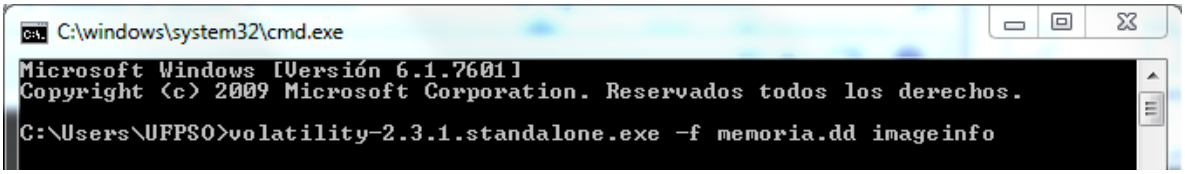
El siguiente paso consiste en analizar que comandos están disponibles en la aplicación y que datos nos da cada uno. Para ello ejecutamos la herramienta como sigue:

volatility-2.3.1.standalone.exe –h

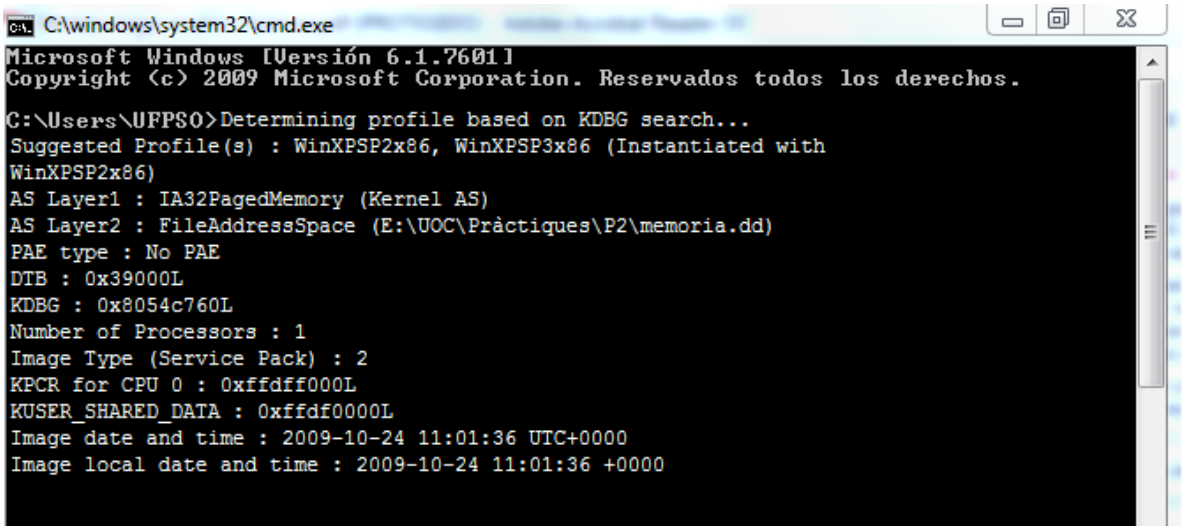
Lo cual nos da como salida la siguiente lista de comandos y su breve explicación:



Empezamos averiguando de qué sistema operativo se trata. Sabemos que es Windows pero desconocemos su versión y *service pack* instalado. Ejecutamos el comando siguiente para obtener dicha información.

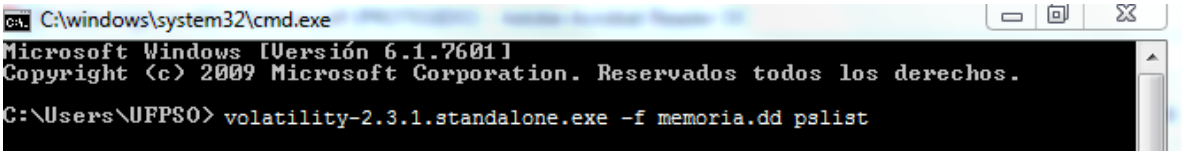


Esto nos da los siguientes datos:

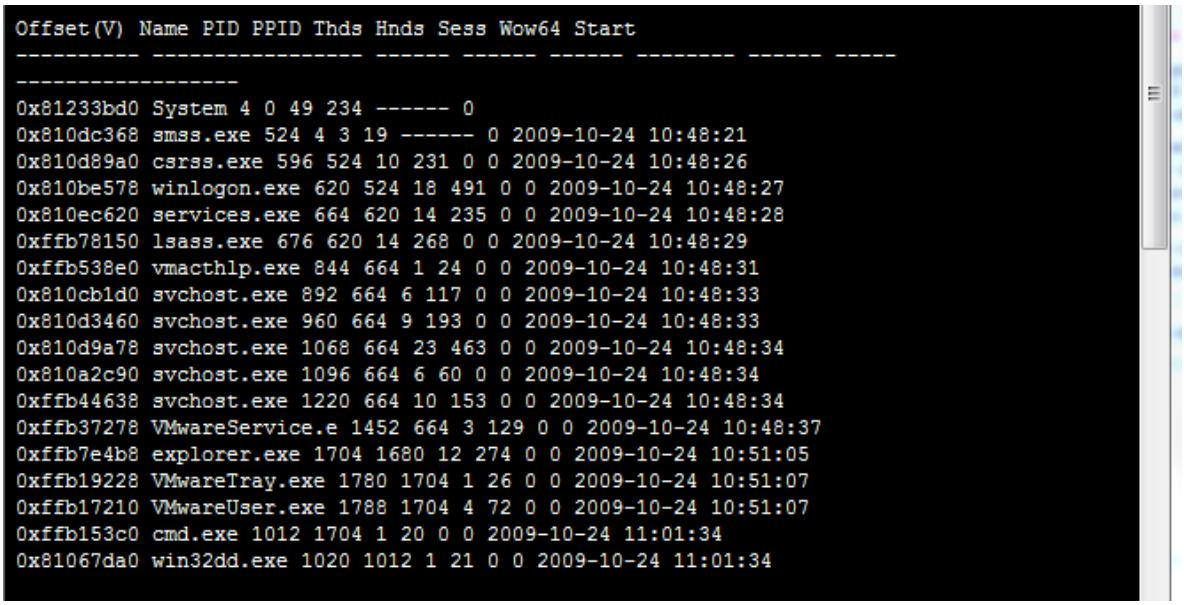


De lo cual se desprende que se trata de Windows XP con *service pack 2* ó *service pack 3*. También podemos ver a qué hora se hizo el volcado de memoria, así como el número de procesadores del equipo entre otros datos técnicos de la memoria.

A continuación puede ser interesante ver que procesos se estaban ejecutando en el momento del volcado de memoria, para ello ejecutaremos:



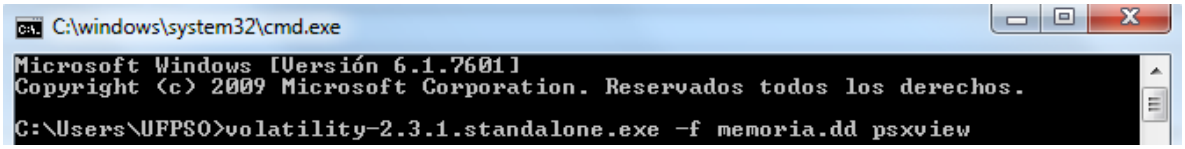
Que nos da las siguientes pistas:



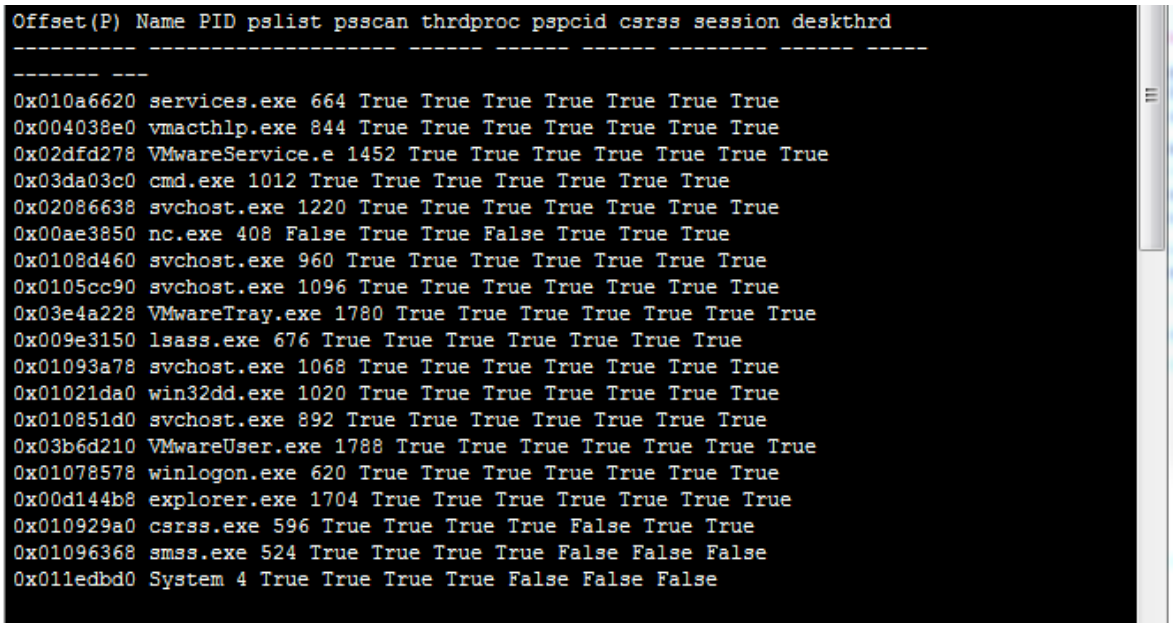
```
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start
---------- ---------------- ------ ------ ------ -------- ------ -----
------------------
0x81233bd0 System 4 0 49 234 ------ 0
0x810dc368 smss.exe 524 4 3 19 ------ 0 2009-10-24 10:48:21
0x810d89a0 csrss.exe 596 524 10 231 0 0 2009-10-24 10:48:26
0x810be578 winlogon.exe 620 524 18 491 0 0 2009-10-24 10:48:27
0x810ec620 services.exe 664 620 14 235 0 0 2009-10-24 10:48:28
0xffb78150 lsass.exe 676 620 14 268 0 0 2009-10-24 10:48:29
0xffb538e0 vmacthlp.exe 844 664 1 24 0 0 2009-10-24 10:48:31
0x810cb1d0 svchost.exe 892 664 6 117 0 0 2009-10-24 10:48:33
0x810d3460 svchost.exe 960 664 9 193 0 0 2009-10-24 10:48:33
0x810d9a78 svchost.exe 1068 664 23 463 0 0 2009-10-24 10:48:34
0x810a2c90 svchost.exe 1096 664 6 60 0 0 2009-10-24 10:48:34
0xffb44638 svchost.exe 1220 664 10 153 0 0 2009-10-24 10:48:34
0xffb37278 VMwareService.e 1452 664 3 129 0 0 2009-10-24 10:48:37
0xffb7e4b8 explorer.exe 1704 1680 12 274 0 0 2009-10-24 10:51:05
0xffb19228 VMwareTray.exe 1780 1704 1 26 0 0 2009-10-24 10:51:07
0xffb17210 VMwareUser.exe 1788 1704 4 72 0 0 2009-10-24 10:51:07
0xffb153c0 cmd.exe 1012 1704 1 20 0 0 2009-10-24 11:01:34
0x81067da0 win32dd.exe 1020 1012 1 21 0 0 2009-10-24 11:01:34
```

De esta lista se desprende que se estaban ejecutando los servicios propios del sistema operativo así como los relativos a la máquina virtual, que al parecer es “VM Ware”. También podemos ver que se ejecutó la consola “cmd.exe” y acto seguido “win32dd.exe”. Esta aplicación sirve para hacer volcados de memoria y corresponde con la hora que antes se ha visto con imageinfo, a las 11:01:34 – 11:01:36.

Según esta información parece que no hay ningún proceso en ejecución fuera de lo normal, al menos en el momento del volcado de memoria. Para asegurarnos de esto ejecutaremos la siguiente instrucción que nos dará como resultado todos los procesos del sistema aunque estén ocultos por cualquier motivo.



Nos da la siguiente información:



```
Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ -----
------- ---
0x010a6620 services.exe 664 True True True True True True True
0x004038e0 vmacthlp.exe 844 True True True True True True True
0x02dfd278 VMwareService.e 1452 True True True True True True True
0x03da03c0 cmd.exe 1012 True True True True True True True
0x02086638 svchost.exe 1220 True True True True True True True
0x00ae3850 nc.exe 408 False True True False True True True
0x0108d460 svchost.exe 960 True True True True True True True
0x0105cc90 svchost.exe 1096 True True True True True True True
0x03e4a228 VMwareTray.exe 1780 True True True True True True True
0x009e3150 lsass.exe 676 True True True True True True True
0x01093a78 svchost.exe 1068 True True True True True True True
0x01021da0 win32dd.exe 1020 True True True True True True True
0x010851d0 svchost.exe 892 True True True True True True True
0x03b6d210 VMwareUser.exe 1788 True True True True True True True
0x01078578 winlogon.exe 620 True True True True True True True
0x00d144b8 explorer.exe 1704 True True True True True True True
0x010929a0 csrss.exe 596 True True True True False True True
0x01096368 smss.exe 524 True True True True False False False
0x011edbd0 System 4 True True True True False False False
```

Analizando estos datos vemos que nos aparece el proceso “nc.exe” que anteriormente no aparecía, efectivamente indica *false* en la columna *pslist.* Una breve búsqueda en la red nos da información sobre este ejecutable que corresponde con la herramienta *netcat*. *Netcat* permite la ejecución remota de comandos a través de consola y abrir y cerrar puertos y conexiones en equipos remotos.

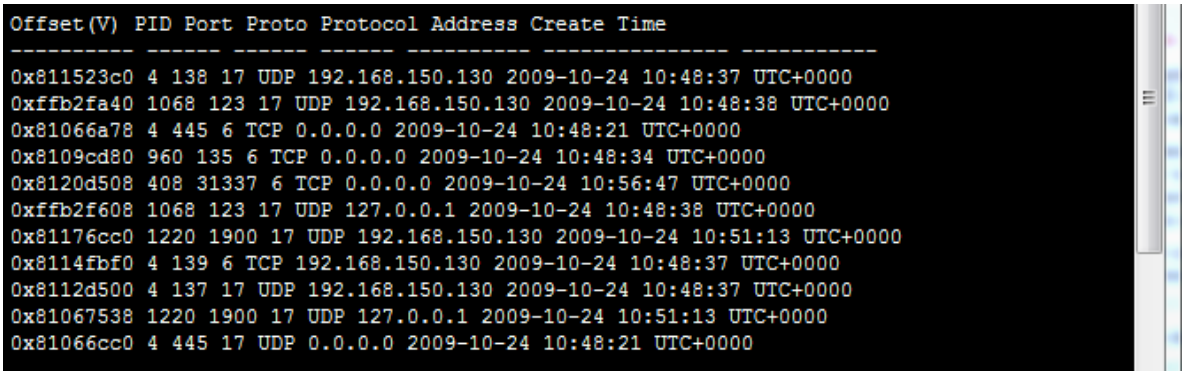
Con esta información la línea de investigación puede proseguir por dos caminos. Por un lado, ver si existen conexiones abiertas en la máquina que se está analizando. Por otro lado ver el

contenido de la consola del equipo para ver si se ha digitado algún comando que pueda aportar más datos.

Vamos primero con el análisis de conexiones abiertas. Para ello ejecutaremos la siguiente opción:

Esta ejecución no nos devuelve ningún resultado lo cual indica que en el momento del volcado de memoria no existía ninguna conexión activa. Ello no quiere decir que no se puedan realizar conexiones, de hecho, esta es la utilidad de netcat, poder establecer comunicaciones con la máquina comprometida. Con la siguiente instrucción veremos si hay puertos abiertos esperando comunicación:

La salida de este comando es la siguiente:

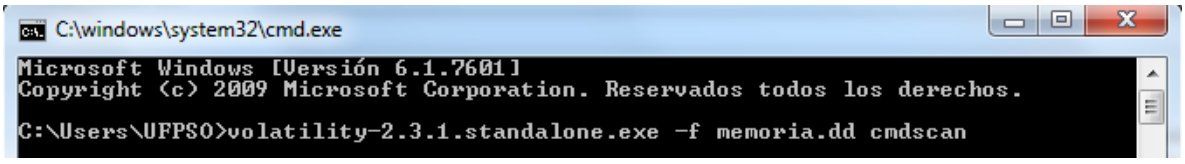


```
Offset(V)  PID  Port  Proto  Protocol  Address  Create Time
---------- ------ ------ ------ ---------- --------------- -----------
0x811523c0 4 138 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000
0xffb2fa40 1068 123 17 UDP 192.168.150.130 2009-10-24 10:48:38 UTC+0000
0x81066a78 4 445 6 TCP 0.0.0.0 2009-10-24 10:48:21 UTC+0000
0x8109cd80 960 135 6 TCP 0.0.0.0 2009-10-24 10:48:34 UTC+0000
0x8120d508 408 31337 6 TCP 0.0.0.0 2009-10-24 10:56:47 UTC+0000
0xffb2f608 1068 123 17 UDP 127.0.0.1 2009-10-24 10:48:38 UTC+0000
0x81176cc0 1220 1900 17 UDP 192.168.150.130 2009-10-24 10:51:13 UTC+0000
0x8114fbf0 4 139 6 TCP 192.168.150.130 2009-10-24 10:48:37 UTC+0000
0x8112d500 4 137 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000
0x81067538 1220 1900 17 UDP 127.0.0.1 2009-10-24 10:51:13 UTC+0000
0x81066cc0 4 445 17 UDP 0.0.0.0 2009-10-24 10:48:21 UTC+0000
```

En ella podemos ver que el PID 408, que corresponde con la ejecución de la aplicación "nc.exe" tiene abierto el puerto 31337, a la espera de conexiones usando el protocolo TCP.

Según la información que dan los dos anteriores comandos parece ser que no hay ninguna dirección IP conectada, pero sí que la máquina que estamos analizando está comprometida ya que tiene puertos abiertos a la espera de posibles conexiones, además de haber ocultado el proceso en memoria para no levantar sospechas.

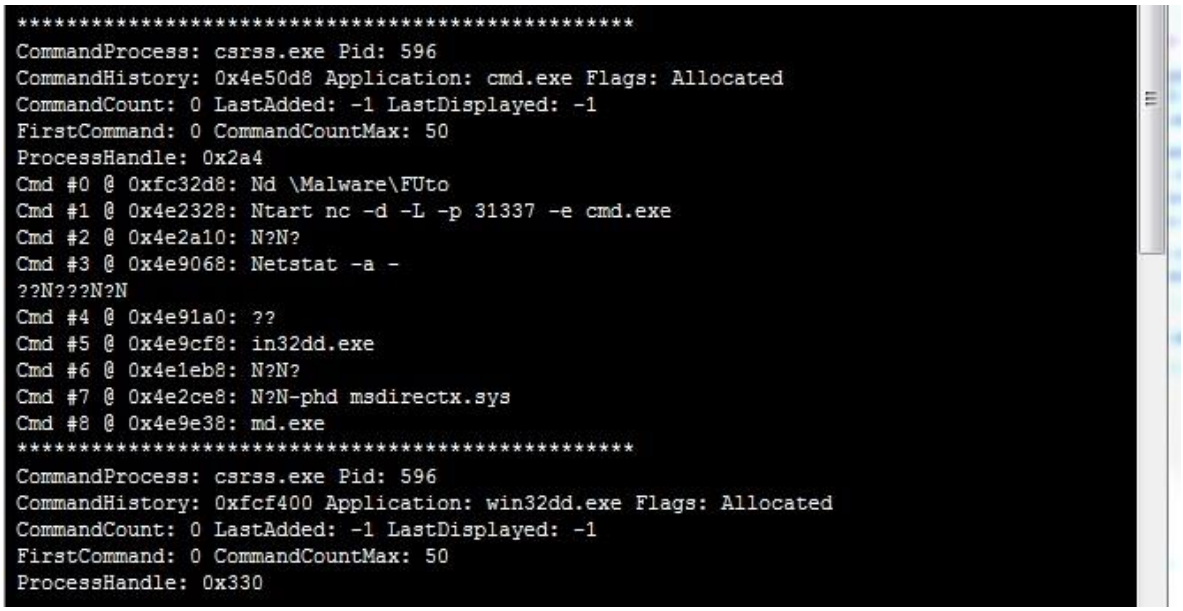
A continuación podemos analizar el contenido de los últimos comandos escritos por la consola del equipo comprometido para ver si podemos obtener alguna información más y acabar de ligar todo lo que ya se ha encontrado. Para ello disponemos de la siguiente opción:



```
C:\windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\UFPSO>volatility-2.3.1.standalone.exe -f memoria.dd cmdscan
```

Ello nos devuelve lo siguiente:



De esta información podemos recalcar tres puntos. El primero es la llamada al *malware FUto*. Buscando por la red se puede leer que se trata de un *rootkit* que oculta procesos en memoria para dificultar la tarea de un posterior análisis forense. Ello explicaría porque no aparece el proceso en la lista de procesos en ejecución.

A continuación vemos la llamada a la aplicación “nc.exe” y la abertura del puerto 31337 que ya hemos visto relacionado con los puertos abiertos. Lo cual confirma que la máquina está comprometida ya que está a la espera de recibir comandos desde ese puerto.

Finalmente comentar la aparición del archivo “msdirectx.sys” que también está relacionado con el *malware Futo* y la ejecución de “nc.exe”.

Con todos estos datos vamos a intentar extraer el código del ejecutable y del módulo oculto.

Para esta tarea contamos con la instrucción procexedump que necesita como parámetro el PID del ejecutable, el offset en memoria del mismo y un directorio donde volcar el código. Ejecutamos pues:

```
C:\Users\UFPSO>volatility-2.3.1.standalone.exe -f memoria.dd procexedump -p 408
-o 0x00ae3850 - dump exedump
```

Obteniendo la siguiente salida:

```
Process(V)  ImageBase Name Result
----------  ---------- ------------ ------
0xffaf6850 0x00400000 nc.exe Error: ImageBaseAddress at 0x400000 is paged
```

En este caso no se puede obtener el código del ejecutable ya que se ha paginado la memoria en esas direcciones. Vamos a probar con “msdirectx.sys”. En este caso disponemos de moddump que requiere la dirección base y un directorio donde volcar el código. Ejecutamos como sigue:

```
C:\Users\UFPSO>dlldumpvolatility-2.3.1.standalone.exe -f memoria.dd moddump -bas
e=0xfc3b6000 -dump dlldump
```

Obteniendo:

En este caso sí que podemos obtener el código del módulo. Cabe destacar que nuestro *software* antivirus del equipo donde se desarrolla esta práctica detecta el archivo como potencialmente peligroso y lo elimina inmediatamente para evitar su ejecución.

Así pues, tras toda la información que se ha obtenido con la aplicación *volatility* y tal como se ha ido explicando durante todo el análisis podemos llegar a las siguientes conclusiones.

- Se han ejecutado programas para dificultar la detección de otros programas maliciosos.
- Se ha detectado la presencia de puertos abiertos preparados para ejecutar comandos remotamente.
- Se ha detectado una aplicación oculta esperando peticiones por los puertos anteriores.
- Se ha detectado un módulo potencialmente peligroso y se ha podido extraer su contenido.
- Se concluye que la máquina analizada está actualmente comprometida y que su uso no es seguro.