IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Informática Forense

Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática

Structure of a Informatic Forensic Laboratory of de Informatic Security Departments

Oscar Lázaro Garcés Pérez

[1] Universidad de las Ciencias Informáticas, Dirección de Seguridad Informática Carretera a San Antonio de los Baños, km 2 ½, Boyeros, La Habana, Cuba. olgarces@uci.cu
Autor para correspondencia: olgarces@uci.cu

Resumen
En la actualidad el uso fraudulento de las redes ha elevado la cantidad de ataques a sistemas informáticos y muchas instituciones se han visto afectadas por las diferentes formas de delincuencia digital. La Informática Forense es la rama de las ciencias forenses encargada de investigar los delitos relacionados con las tecnologías de la información utilizando técnicas científicas para el procesamiento de las evidencias digitales. La presente investigación tiene como principal objetivo presentar el diseño de un laboratorio de informática forense en la Universidad de las Ciencias Informáticas. Con la implementación del laboratorio se mejora el procesamiento de las evidencias durante el análisis de un incidente de seguridad garantizando la integridad de los datos que serán presentados en un proceso investigativo.

Palabras clave: cibercrimen, informática forense, laboratorio, seguridad informática.

Abstract
Currently the fraudulent use of networks has increased the number of attacks on computer systems and many institutions have been affected by different forms of digital crime. The Informatic Forensics is the branch of forensic sciences responsible for investigating related crimes with information technologies using scientific techniques for the processing of digital evidence. The main objective of the present investigation is to present the design of a forensic computer lab at the University of Computer Science. With the implementation of the laboratory, the processing of evidences is improved during the analysis of a security incident guaranteeing the integrity of the data that will be presented in a process legal.

Keywords: *cybercrime, computer forensics, laboratory, computer security.*

Introducción

Estar preparado ante un incidente de seguridad aplicando mecanismos de defensa para las redes es fundamental, pero a pesar de las barreras de protección establecidas para salvaguardar los activos de información, los ataques a sistemas informáticos se siguen produciendo y evolucionando en paralelo con las nuevas tecnologías.

Una de las fases más importantes en la respuesta a un incidente de seguridad es identificar y recuperar la evidencia relacionada con el hecho. Sin embargo, las computadoras guardan la información de forma tal que a través de los medios comunes no se puede recuperar o analizar, por lo que son necesarios mecanismos diferentes a los tradicionales. La Informática Forense como ciencia, aplicando técnicas científicas y analíticas especializadas a la infraestructura tecnológica es la encargada de identificar, preservar, analizar y presentar la información obtenida de forma válida dentro de un proceso legal. (Zuccardi, 2006)

La Informática Forense no tiene como objetivo prevenir delitos, aunque puede brindar datos precisos para mejorar los mecanismos de seguridad utilizados en la protección de una red. El análisis forense pretende averiguar qué fue lo que ocurrió durante una intrusión buscando una respuesta de quién realizó el ataque, qué activos se vieron afectados y en qué magnitud, cuándo ocurrió, dónde se originó y contra qué blancos estuvo dirigido, cómo se perpetuó y el por qué. (Creutzburg, 2016)

Gracias a que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada, la Informática Forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes incidentes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. Esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en temas de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. (Shinder, 2008)

A través de esta ciencia es posible investigar quién es el dueño de sitios web, quiénes son los autores de determinados artículos y otros documentos enviados o publicados a través de redes. Son igualmente investigables las modificaciones, alteraciones y otros manejos a las bases de datos de redes internas o externas. Los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha de

creación, etc. a espaldas del usuario, pudiendo determinarse en algunos casos en qué dispositivo fue redactado el documento.

En el 2017 los ataques de ransomware WannaCry, ExPetr y BadRabbit fueron los más significativos. WannaCry se extendió a una velocidad asombrosa y se cree que se ha cobrado alrededor de 700,000 víctimas en todo el mundo. ExPetr fue más específico, afectando a las empresas, incluidas muchas marcas reconocidas a nivel mundial a través de software comercial infectado. Maersk, la compañía más grande del mundo de portacontenedores y buques de suministro ha declarado pérdidas anticipadas de entre $200 y $300 millones de dólares como resultado de una "interrupción comercial significativa" causada por el ataque. (Kaspersky Security Bulletin, 2017)

La mayoría de los malware responsables de los ciberataques se propagan utilizando los servicios que se publican Internet y son accesibles por los usuarios a través de los navegadores web.

En la Universidad de las Ciencias Informáticas (UCI) se imparte la asignatura Informática Forense como parte del proceso docente educativo, pero no cuenta con un las herramientas y condiciones adecuadas para su estudio y aplicación. Poner en práctica las técnicas científicas que propones esta rama de las ciencias forenses requiere la creación de áreas especializadas en el tema que brinden un entorno propicio y confiable para desarrollar la actividad.

Por lo antes expuesto en este trabajo se presenta el diseño general de un laboratorio de informática forense con las funciones de los departamentos que lo componen. Dándole respuesta a la siguiente interrogante:

¿Cómo mejorar el proceso de análisis de los delitos informáticos que ocurren la Universidad de las Ciencias Informáticas?

Materiales y métodos o Metodología computacional

Método histórico - lógico: permitió el estudio de la evolución y desarrollo de las diversas entidades dedicadas al análisis forense digital. Haciendo énfasis en las características más importantes que han surgido y que son aplicables en el diseño de la solución propuesta.

Método análisis - síntesis: este método viabilizó la realización del estudio teórico de la investigación y el análisis de la documentación referida a la informática forense, permitiendo que se sintetizaran los elementos

más importantes para el análisis de los documentos y la bibliografía con el objetivo de obtener información detallada relacionada con el objeto de estudio.

Conceptos básicos

Delitos informáticos: Son todas aquellas acciones ilegales que implican una computadora, su sistema operativo o sus aplicaciones. (Shinder, Scene of the Cybercrime, 2008)

Informática Forense: Es una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente y almacenados en un medio digital. (Iorio, 2017)

Evidencia digital: Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Es una denominación utilizada para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como prueba en un proceso legal. (Clérigues, 2016)

Metodología de análisis de las evidencias digitales

El análisis forense es una disciplina que requiere una estricta organización interna basada en principios y buenas prácticas de trabajo para los investigadores que intervienen en un caso. Para el laboratorio de informática forense se propone la utilización del modelo PURI (Proceso Unificado de Recuperación de Información) elaborado por un colectivo de autores pertenecientes a la Universidad FASTA de Argentina.

El modelo PURI es un esquema teórico de las tareas involucradas en la aplicación forense de las ciencias de la información. Este esquema agrupa las tareas en actividades de mayor abstracción, y a éstas en fases. A su vez, el modelo se complementa con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles que ejecutan dichas técnicas. (Iorio, 2017)

Las fases iniciales de Relevamiento y Recolección, son de tipo exploratorio esperado que sean ejecutadas por un profesional con perfil orientado a la investigación, donde el técnico tenga un rol de asistencia y asesoramiento. En cambio, las fases subsiguientes: Adquisición, Preparación, Extracción y Análisis, y Presentación, son netamente de informática forense, y se espera que las tareas involucradas sean desarrolladas por profesionales especializados en esta temática, con la asistencia que se requiera de los investigadores del caso. Más allá de las preponderancias de un perfil profesional sobre otro, en cada una de

las fases, se recomienda siempre el trabajo conjunto de las tres orientaciones, legal, criminalística y de informática forense, ya que, como en todo sistema, "el todo es más que la suma de las partes". (Iorio, 2017)

Resultados y discusión

La implementación de un Laboratorio Informática Forense (LIF), en la Universidad de Ciencias Informáticas debe garantizar el análisis de incidentes de ciberseguridad.

Estructura del laboratorio

- El LIF (Laboratorio de Informática Forense) estará compuesto inicialmente por 6 áreas principales:
- Seguridad de los datos
- Recuperación de archivos borrados y metadatos.
- Análisis de memoria RAM.
- Análisis de Red.
- Análisis de aplicaciones instaladas.
- Departamento legal.

Seguridad de los datos: Se encarga de la protección de los datos contra accesos no autorizados y corrupción de la información durante todo el ciclo de análisis. El departamento utiliza un procedimiento basado en los conceptos de encriptación de datos, función resume (hash) y prácticas de gestión de claves que ayudan a proteger la información en todas las aplicaciones y plataformas del área. Garantiza además que las etapas de la cadena de custodia de las evidencias se ejecuten correctamente. Interviene en la validación y preservación de los datos, ya que almacena todas las evidencias de los casos.

La protección de la subred del laboratorio es otro aspecto importante para garantizar la integridad de la información que se procesa en el mismo. Se deben instalar dispositivo para proteger cada punto de acceso como firewalls, IDS, y realizar pruebas periódicas de penetración a los sistemas que constituyen activos informáticos críticos.

Recuperación de archivos borrados y metadatos: El departamento tiene la función de ejecutar tareas en la fase de recuperación de información relacionadas con el incidente. Para este propósito se analizan archivos temporales, archivos borrados tanto de forma automática como de forma intencionada. Para la

recuperación de estos datos y su posterior análisis se utilizan las técnicas de File y Data Carving. Las herramientas que utilizan estas técnicas trabajan en base a la estructura de los formatos que reconocen, y pueden recuperar archivos aun cuando no quedan metadatos asociados, solamente en base al contenido. Al no depender de la información del sistema de archivos, solamente de la estructura de los formatos, las herramientas de carving son muy efectivas y pueden trabajar sobre cualquier medio de almacenamiento. Las técnicas de File Carving se basan en recuperar archivos completos que no estén dañados de un dispositivo de almacenamiento analizando el contenido de sus bloques, teniendo en cuenta características específicos de los formatos e ignorando las estructuras del sistema de archivos. Por su parte las técnicas de Data Carving pretenden recuperar fragmentos de datos más pequeños relacionales con algún fichero. (Merola, 2008)

Otras de las funciones del departamento es el análisis de los metadatos de los archivos encontrados o recuperados del dispositivo de almacenamiento. Los metadatos son campos de texto que van incrustados en casi todos los tipos de ficheros de forma automática y a espaldas de los usuarios. Añaden información adicional como la fecha de creación, resolución, tamaño, fecha de modificación, autor, etc.

Análisis de RAM: La RAM es uno de los componentes principales de un ordenador, también llamada memoria principal. Es la encargada de ejecutar todas las instrucciones del procesador y otras unidades de cómputo. Los datos que se almacenan en ella son temporales o volátiles ya que dependen de una fuente de alimentación constante.

Debido a esto, en la fase de recogida de evidencias si el equipo está encendido, una de las principales acciones a realizar es el volcado o captura de su memoria RAM. En el componente se pueden identificar drivers, ejecutables, ficheros, direcciones IP, contraseñas, comandos ejecutados por consola, rootkits, puertos abiertos y conexiones activas. El análisis de la memoria principal es relativamente complicado para los investigadores pues se deben considerar un conjunto de variables que relacionan los procesos nativos del sistema operativo y las acciones de los usuarios del equipo. Teniendo en cuenta su envergadura se propone asignar este procedimiento a un departamento específico del laboratorio.

Análisis de Red: Realiza monitoreo y control sobre la red implicada en un incidente analizando el tráfico de entrada y salida a las estaciones de trabajo y los servidores. Para las funciones del departamento se

recomienda la utilización de un sistema de detección de instrucciones (IDS) que permitan identificar accesos no autorizados a las computadoras.

Análisis de aplicaciones instaladas: Se encarga de analizar los navegadores web, clientes de mensajería instantánea, servidores web y ftp, bases de datos, etc., además de los registros del sistema operativo.

Departamento legal: Es departamento encargado de presentar el caso ante un tribunal proporcionando datos precisos sobre el incidente analizado a través de dos tipos de informe: Informe Técnico e Informe Ejecutivo.

Herramientas de análisis forense.

1. Sistema Operativo: Kali Linux 2018
2. Recuperación de archivos borrados: Scalpel, Disk Drill, CNWRecovery.
3. Metadatos: FOCA, ExifTool, Metagoodfil
4. Análisis de datos y ficheros: MFT Tools,INDXParse
5. Análisis de navegadores: DumpZilla, MozCache. SQLiteBrowser, RecoverRS
6. RAM: LiME, Volatility, YARA, FTK imager.
7. Hash: MD5SUM, MD5DEEP.
8. Pruebas de Penetración: Owasp's ZAP (Zed Attack Proxy).
9. Suite Forense: Autopsy, The Sleuth Kit, OSForensics
10. Montaje de discos: ImDisk ,OSFMount raw2vmdk

Infraestructura Tecnológica

El diseño interno LIF, debe brindar y garantizar un ambiente seguro e integral para la operación diaria del personal forense, así como de las evidencias, el área deberá contar con suministro eléctrico permanente, acondicionamiento térmico, circuito cerrado de televisión, sistema de seguridad y detección de incendios.

El servicio de Internet en el área Informática Forense deberá ser permanentemente monitoreado y controlado, así como el análisis de información de documentos entrantes y salientes, y bloqueo de correos electrónicos pertenecientes a dominios que no consten en las listas permitidas.

Adicionalmente el uso de dispositivos de almacenamiento de información y celulares de uso personal no estarán permitidos, excepto aquellos autorizados por los directivos del área y para funciones de trabajo específicas.

Se propone la instalación de un servidor con soporte de tecnología de virtualización el cual será utilizado para montar máquinas virtuales y brindará un servicio de aplicaciones forenses, de acuerdo a lo propuesto en este documento. Este servidor actuará funcionalmente equiparado a un NAS (Network Área Storage) para el almacenamiento de backups, evidencias digitales y reportes técnicos. Tendrá un espacio de almacenamientos en discos SATA de 10Tb.

Control de dispositivos de almacenamiento

El uso de memorias USB en las empresas constituye un riesgo relacionado con el robo de información y la propagación de virus informáticos que afectan el funcionamiento de las entidades. Para el laboratorio de informática forense se propone el uso de una herramienta que permita controlar los dispositivos y la información que se guarda en los mismos. A continuación, se muestra el funcionamiento básico de dicha herramienta.

USBControlPanel

La aplicación debe conectarse vía SSH a todas las máquinas del laboratorio para hacer los controles necesarios. Debe contar con un sistema de alerta que se ejecute de manera automática comprobando la integridad del dispositivo y crear un reporte sobre posibles violaciones. La aplicación debe tener 4 módulos principales: Control de accedo de dispositivos USB, Control de archivos almacenados en el dispositivo, Sistema de alerta y Sistema de reportes.

Control de accedo de dispositivos USB.

El módulo debe permitir:

1. Agregar un dispositivo de confianza en el servidor (se debe extraer el ID del dispositivo y agregarlo a una base de datos, asociarle la información básica del usuario: Nombre, solapín, usuario del dominio, área a la que pertenece; además se debe registrar los datos de la PC donde se va a utilizar: IP, MAC, Nombre-PC).

2. Definir las operaciones (Lectura, Lectura/Escritura) que pueden ejecutar los usuarios sobre el dispositivo.
3. Los dispositivos no autorizados además de generar una alerta no se deben montar en el sistema.

Control de archivos almacenados en el dispositivo.

El módulo debe permitir:

1. La aplicación debe ser capaz de generar registros de logs que guarden el estado de los archivos que se almacenan en el dispositivo con el siguiente formato:(dd/mm/aaaa-hh:mm:ss) ruta_del_archivo hash_del_fichero, id_metadatos).
2. La aplicación debe ser capaz de generar registros de logs que guarden el estado de los archivos eliminados que se almacenaron en el dispositivo con el mismo formato mencionado anteriormente.

Sistema de alerta.

El módulo debe ser capaz de generar una alerta cuando:

1. Se inserte un dispositivo no autorizado en la PC.
2. Se detecte información sensible o prohibida.
3. Existan archivos ocultos.
4. Las alertas deben enviarse por correo.

Sistema de reportes.

1. Dispositivos autorizados y los permisos que tienen.
2. Resumen de alertas semanales y mensuales.
3. Usuarios con más de un dispositivo registrado.

Seguridad Física:

En el LIF se debe establecer un control de acceso al personal para poder asegurar la integridad de la información que se gestiona y así prevenir incidentes como:

1. La ejecución de código malicioso (por ejemplo, activar un gusano desde el interior del laboratorio).
2. El robo de información sensible (por ejemplo, material probatorio, segundos originales, cintas de copia de seguridad y diagramas de red).

Valoración económica, novedad y aporte social

El LIF servirá de soporte para las instituciones legales, donde, a través de procedimientos estrictos y rigurosos puede ayudar a resolver incidentes de seguridad apoyándose en el método científico para la recolección, análisis y validación de todo tipo de pruebas digitales. Además, permite complementar el estudio de temas relacionados con la informática forense ayudando a la sociedad a adaptarse a la nueva era digital en la que se encuentra inmersa de una forma más segura.

Conclusiones

Luego de terminada la investigación se concluye que la necesidad de crear un laboratorio forense es debido al aumento de las ilegalidades informáticas por lo que el presente diseño servirá de guía para la implementación de infraestructuras similares que cumpla con las condiciones establecidas. Además, permitirá dar respuesta a la problemática actual, garantizando la seguridad de las evidencias relacionada con un delito informático. Se espera generar nuevos conocimientos científicos técnico, plasmados en un protocolo para la recolección y tratamiento de evidencias digitales extraídas de diferentes dispositivos acompañadas de un modelo para la gestión óptima de dichas evidencias. Permitirá dar solución a problemas de esta índole dentro de la propia institución sin depender directamente del órgano rector que atiende los temas relacionados con los delitos informáticos.

Referencias

Clérigues, J. N. (2016). *Guía actualizada para futuros peritos informáticos.*

Creutzburg, R. (2016). *Seguridad Informática y Análisis Forense Digital.*

Iorio, A. H. (2017). *El rastro digital del delito.* Argentina.

Kaspersky Security Bulletin. (2017). *Kaspersky Lab*. Obtenido de https://securelist.com/ksb-review-of-the-year-2017/83338/

Merola, A. (2008). *Data Carving Concepts.* Obtenido de https://www.sans.org/reading-room/whitepapers/forensics/data-carving-concepts-32969.

Shinder, D. L. (2008). *Cybercrime. Computer Forensics Handbook.*

Shinder, D. L. (2008). *Scene of the Cybercrime.*

Zuccardi, G. (2006). *Informática Forense.*