Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto

Pereyra, Damián; Eterovic, Jorge

Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales
Universidad de Morón
Cabildo 134, (B1708JPD) Morón, Argentina. Tel: (54 11) 5627-2000
pereyrad@gmail.com, jeterovic@hotmail.com

Resumen

La facilidad de acceso a Internet y el desarrollo del mercado relacionado con los dispositivos que permiten acceder a las nuevas TICs han cambiado no solo la forma en la que se pasa el tiempo libre y la forma en la que se llevan a cabo los negocios sino también la forma en la que los delincuentes comenten sus crímenes.

En este panorama complejo, se propone desarrollar un ambiente con las adecuadas condiciones de seguridad física y la metodología para la utilización de herramientas informáticas para la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para dañar individuos, organizaciones, empresas o a la sociedad en general. Las computadoras y las redes pueden verse involucrados en un delito informático [13], siendo las herramientas utilizadas para cometerlo, las víctimas del delito o ser utilizadas para propósitos incidentales relacionados con el delito.

El Análisis Forense Informático (Computer Forensics) comprende el proceso de extracción, conservación, identificación, documentación, interpretación y presentación de las evidencias digitales de forma que sean legalmente aceptadas en cualquier proceso judicial, proporcionando las técnicas y principios que facilitan la investigación del delito.

Palabras clave: Análisis Forense Informático, Informática Forense. Computación Forense, Análisis Forense Digital, Cómputo Forense, Examen Forense Digital, Pericias Informáticas.

Contexto

El presente proyecto se desarrolla en el marco del PID 01-003/12 de la Universidad de Morón, esta integrado por investigadores de la Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales de la Universidad de Morón.

En colaboración con uno de los objetivos propuestos en el proyecto, se incorporan alumnos de la Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales de la Universidad de Morón, para el desarrollo de pruebas de instalación, configuración, personalización y documentación de productos de Software para el análisis forense informático.

Introducción

El Análisis Forense Informático, también llamado informática forense, computación forense, análisis forense digital, cómputo forense o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a la

infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.[1].

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos. [2] [3].

Cada vez es más frecuente que las organizaciones hayan sufrido ataques a sus sistemas de información. El Instituto de Seguridad Informática CSI (Computer Security Institute) [5] publica cada año un reporte llamado "CSI Computer Crime and Security Survey" [6] en el cual se expone la situación actual de la seguridad informática y del crimen informático, ofreciendo estadísticas basadas en los incidentes de seguridad de múltiples organizaciones en los Estados Unidos.

Para saber qué fue lo que realmente ocurrió, cómo pasó, quien lo realizó, desde donde y que buscaba obtener, la respuesta la puede dar el Análisis Forense Informático.

El trabajo de investigación tratará de formular una guía de asistencia sobre las cuestiones básicas principales: para qué sirve, en qué consiste, cuáles son sus objetivos, la selección de la metodología propiamente dicha de cómo ha de llevarse a cabo y cómo debería ser el ambiente controlado para adecuarse al derecho y sus resultados poder ser utilizados como un elemento de prueba en la justicia. [3] [8].

El Análisis Forense Informático permite encontrar la solución de conflictos tecnológicos relacionados con la seguridad informática y la protección de datos. Gracias a ésto, las organizaciones obtienen una respuesta a problemas de privacidad de datos, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial realizados a través del uso indebido de las tecnologías de la información.

Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

Se busca dar respuesta al planteo de las siguientes preguntas de investigación: ¿para qué sirve el Análisis Forense Informático?, ¿en qué consiste?, ¿cuál es su finalidad?, ¿qué metodologías existen?, ¿cuál es la forma correcta de proceder? y ¿por qué?

El alcance del proyecto de investigación es formular una guía (obtenida del estudio comparativo y de la experiencia), la que se implementará en un Framework de asistencia que correrá en una ambiente piloto con las mínimas medidas de seguridad física y lógica para realizar el Análisis Forense Informático.

Se analizarán, estudiarán y seleccionarán los mejores productos de software de libre distribución para su utilización en distintos dispositivos de hardware. [4].

No se incluye el desarrollo de productos de software ni el equipamiento de un laboratorio específico para el Análisis Forense Informático.

El Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos NIST define la informática forense como la ciencia que se encarga de recuperar y recolectar evidencia digital bajo una serie de condiciones forenses usando unos métodos aceptados [7].

Para realizar una guía metodológica que permita llevar a cabo el Análisis Forense Informático orientado a incidentes de seguridad, es necesario entender principalmente la informática forense debido a que, es en ésta área del conocimiento en donde se establecen los

conceptos y procedimientos que permiten realizar el presente trabajo de investigación.

Es necesario hacer una revisión del contexto general de la disciplina, exponiendo de forma general el propósito, los objetivos y algunas definiciones básicas como ser las evidencias digitales y los aspectos legales que deben ser tenidos en cuenta. [8].

Seguidamente se deberá hacer una revisión de las herramientas forenses existentes en la actualidad, clasificándolas en dos sistemas diferentes: Por funcionalidad y por su naturaleza de distribución (código abierto / comerciales). Finalmente se deberá realizar una revisión de los procedimientos y estándares existentes con el fin de entender la forma en la que se realizan los análisis forenses en la actualidad. [1][7].

Líneas de Investigación, Desarrollo e Innovación

Como disciplina, la informática forense tiene como fin el aplicar los estándares y procedimientos estándar que se utilizan en una investigación de crímenes e incidentes de seguridad de la información, para enfocarlos hacia el análisis de datos y evidencia digital, todo esto soportado por herramientas tecnológicas de extracción y análisis de datos. [9].

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense: [9]

1. Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Una de las metas de la informática forense, es poder realizar un estudio total de todo tipo de evidencia digital que se encuentre involucrada en un incidente (es decir, realizar recopilación, preservación, análisis y reportes de la evidencia), con el fin de hacer que esta evidencia tenga un valor legal, y que asimismo, sea en un proceso judicial en el cual esta evidencia tenga un carácter determinante en el mismo. [9].

Para llevar a cabo este proceso y desarrollarlo de forma confiable, a la hora de hacerlo legalmente válido, es necesario considerar la evidencia digital de dos formas. [8]. La primera de ellas consiste en ver la evidencia digital como una prueba ordinaria en un caso ordinario, en el sentido que esta dado su contenido, generalmente ayuda a identificar

involucrados en un incidente delictivo y sus responsabilidades en él.

La segunda forma de consideración, va más allá y considera la evidencia digital, como una forma de evidencia, requiriendo ser tratada dentro de un marco legal válido, dado por los estándares, para realizar su recolección y preservación.

Éste proyecto de investigación sobre informática forense busca estudiar, entender, analizar y enfocar los conceptos referentes a esta ciencia, para poder llevar a cabo la construcción de una base de conocimiento sólida en la materia, la cual será el punto de partida para la construcción de la guía metodológica propuesta en el proyecto.

El objetivo de esta investigación es la utilización del Análisis Forense Informático con dos fines, uno preventivo y otro reactivo.

Como fin preventivo, servir a las organizaciones para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes.

Asimismo, permitir detectar las vulnerabilidades de seguridad con el fin de corregirlas, tratando que las políticas sobre uso de los sistemas de información no atenten contra el derecho a la privacidad de esas personas.

Con fin reactivo, cuando la seguridad de la organización ya ha sido vulnerada, el Análisis Forense Informático permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración interna o externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos de la organización, para determinar las actividades realizadas desde uno o varios equipos concretos y analizar y preservar las evidencias digitales para ser usadas como evidencia probatoria, tratando de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Una de las principales formas en las que los investigadores tratan de entender la base científica de una disciplina es la construcción de modelos que reflejen sus observaciones.

El campo del Análisis Forense Informático está entrando en una rápida metamorfosis: está cambiando de una simple destreza a una verdadera ciencia forense [10]. Debido a las circunstancias previamente expuestas, es importante la revisión de los modelos de investigación más aceptados en esta disciplina en la actualidad, ya que permite entender de una mejor manera los procedimientos y estándares que rigen hoy la informática forense en el mundo.

Un buen modelo de investigación de Análisis Forense Informático debe contar con una serie de principios los cuales se exponen a continuación: [11]

- Principio 1: Considerar el sistema completo.
- Principio 2: Guardar la información de registro a pesar de que el sistema falle en su totalidad.
- Principio 3: Considerar los efectos de los eventos, no solo las acciones que los causan.
- Principio 4: Considerar el contexto para ayudar a la interpretación y el entendimiento de significado de un evento.
- Principio 5: Presentar los eventos de manera en que puedan ser analizados y entendidos por un analista forense.

Para el trabajo se realizará la búsqueda y análisis de metodologías, software comercial y de libre disponibilidad y estándares para desarrollar una guía que se implementará en un Framework de

asistencia que correrá en una ambiente piloto con las mínimas medidas de seguridad física y lógica para realizar el Análisis Forense Informático.

Los escenarios de prueba y desarrollo de la metodología serán en un laboratorio del CIENTIC, de la Universidad de Morón. Se instrumentaran las siguientes actividades principales para el desarrollo del proyecto: Definición del Proyecto de Investigación, Elaboración del Estado del arte, Análisis, Desarrollo del trabajo (Framework), Pruebas con casos reales, Análisis de los resultados y Confección del informe final.

Resultados y Objetivos

El aporte del proyecto de investigación se centra en implementación de un Framework de asistencia para la realización de pericias informáticas que se ejecutará en un ambiente piloto. El mismo deberá contar con las medidas de seguridad física y lógica recomendadas por los estándares internacionales.

La investigación continuará con el desarrollo y la implementación de un laboratorio que se presentará para ser certificado para prácticas de Análisis Forense Informático cuyas pericias tengan validez legal. Se formarán los profesionales para que puedan actuar como peritos forenses informáticos.

Formación de Recursos Humanos

El proyecto contribuirá a la comunidad académica de la Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales de la Universidad de Morón con un ambiente de investigación para la asignatura Auditoria y Seguridad Informática de la Licenciatura en Sistemas y la Ingeniería en Informática y Tesis de Grado – Proyecto Final Integrador y Tesis de Posgrado de la Maestría.

Los objetivos del proyecto apuntan a prevenir y mejorar la seguridad informática de la Universidad de Morón y de distintas organizaciones de la comunidad, asesorar a la justicia y preparar profesionales para realizar peritajes.

Se identifican como usuarios directos:

- Alumnos de la Licenciatura en Sistemas y de la Ingeniería en Informática y de la Maestría
- El área de informática de la UM
- Organizaciones del área de influencia de la UM
- Egresados
- Tribunales

Se prevé la realización de convenios para la Transferencia del Framework de asistencia para la realización de Análisis Forense Informático, capacitación de profesionales y técnicos y asesoramiento al poder judicial.

Referencias

1. Michael G. Solomon, K Rudolph, Ed Tittel, Neil Broom and Diane Barrett; Computer Forensics JumpStart 2nd edition; Wiley Publishing Inc, (2011).
2. Bill Nelson, Amelia Phillips, Christopher Steuart; ed. Cengage Learning; Guide to Computer Forensics and Investigations 3rd edition; Cengage Learning Inc., (2010).
3. Carhuatocto, Roger;; Code of practices for Digital Forensics - CP4DF; (Sourceforge.net; (2003).
4. Bevilacqua Trabado, Matías; Open Source Computer Forensics Manual; Sourceforge.net; (2003).

5. CSI. Computer Security Institute. http://www.gocsi.com/.
6. CSI. "Computer Crime and Security Survey". 2010/2011. http://gocsi.com/Survey_(2010).
7. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang; Guide to Integrating
8. Forensic Techniques into Incident Response, National Institute of Standards and Technology Special Publication 800-66; (2006).
9. Electronic Crime Scene Investigation: A Guide for First Responders and Forensic Examination of Digital Evidence: A Guide for Law Enforcement; U.S. Department of Justice; https://www.ncjrs.gov/pdffiles1/nij/187736.pdf; (2001).
10. O López, H Amaya, R León, B Acosta. "Informática forense: Generalidades, aspectos técnicos y herramientas". Universidad de los Andes Bogotá, Colombia. http://www.criptored.upm.es/guiateoria/gt_m180b.htm. (2002).
11. M Pollit,; An Ad Hoc Review of Digital Forensic Models; National Center for Forensic Science; Department of Engineering Technology; University of Central Florida; (2007).
12. S Peisert, M Bishop, S Karin, K Marzullo; Toward Models for Forensic Analysis; In Proceedings of the Second International International Workshopon Systematic approaches to digital forensic engineering (SADFE'07); (2007).
13. Ley 26388 – Delitos Informáticos. http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm