Investigación y Tecnología Vol. 4. Nro. 1: pag.105 – pag.110. Octubre 2016. ISSN 2306-0522

Informática Forense

Computer Forensics

*** Iver Flores Flores, Leonardo Vargas Peña**
Carrera Ingeniería de Sistemas
Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones
Universidad Autónoma Gabriel René Moreno
Santa Cruz - Bolivia
Autor de correspondencia:* leonardovargas@uagrm.edu.bo

Resumen

El avance tecnológico y comercial a través de los últimos años ha ido incrementando de manera exponencial, lo cual ha revolucionado el mundo de manera tal que casi todo los que se realiza a diario se lo realiza de manera casi automática gracias a las nuevas tecnologías de información, permitiendo tanto a empresas grandes y pequeñas como a sus clientes y/o usuarios poder comunicarse, realizar transacciones, tramites, etc. De manera casi instantánea.

Esta evolución tecnológica también ha sido aprovechada por personas inescrupulosas quienes utilizan una gama de herramientas tecnológicas para fines incorrectos, como lo es la realización de un crimen de índole informático, valiéndose muchas veces de que la información queda almacenada en forma digital pudiendo sustraerla y manipularla de manera errónea.

Cuando pasa una situación de este tipo se presenta un problema, debido a que las computadoras guardan la información que puede servir como evidencia de forma tal que no puede ser recolectada por medios comunes, si no que se requiere la utilización de herramientas y mecanismos diferentes a los tradicionales. Es de aquí que surge la informática forense como una ciencia relativamente nueva, que permite el esclarecimiento de este tipo de delitos por medio de su aplicación.

En la actualidad Bolivia puede que no experimente una amplia variedad de delitos informáticos, aun así este sería uno de los problemas que a la larga podría afectar a la ciudadanía y a empresas ya sean nacionales o extranjeras de nuestro país. Este tipo de delitos no excluyen a nadie, afecta a todos los sectores que conforman nuestro país desde empresarios a ciudadanos, como todo tipo de violencia afecta las posibilidades de desarrollo del país.

La informática forense involucra la participación de profesionales de las tecnologías de la información y de los profesionales del derecho debido a que los resultados obtenidos por medio de la aplicación de informática forense están sujeto al análisis judicial.

El Estudio y Análisis sobre la informática forense en Bolivia permite dar a conocer cuál es la situación actual de esta especialización en nuestro país, para obtener esta información fue necesario como primer punto hacer una investigación preliminar sobre la informática forense y todos los elementos que están involucrados en su proceso de aplicación. A continuación se muestra en detalle las partes por las cuales está comprendida la presente investigación, desde la fase teórica hasta la fase práctica de la informática forense.

Palabras clave: activo informático; análisis forense; aplicaciones ofimáticas; ciberbulling; ciencias forenses.

Abstract

Technological and commercial progress over recent years has been increasing exponentially, which has revolutionized the world so that almost everything that is done on a daily basis is done almost automatically thanks to new information technologies , allowing both large and small businesses and their customers and / or users to communicate, transact, paperwork, etc. Almost instantly.

This technological evolution has also been used by unscrupulous people who use a range of technological tools for improper purposes, as it is the realization of a crime of computer nature, using often that information is stored in digital form can subtract it and manipulate it incorrectly.

When you pass a situation like this presents a problem because computers store information that can serve as evidence in a way that can not be collected by ordinary means, if not the use of different tools and mechanisms required to traditional. It is here that computer forensics emerges as a relatively new science, which allows the investigation of such crimes through its application.

Currently Bolivia may not experience a wide variety of computer crimes, yet this would be one of the problems that eventually could affect citizens and companies whether domestic or foreign in our country. This type of crime do not exclude anyone, affects all sectors that make up our country for entrepreneurs to citizens, as all kinds of violence affects the possibilities of development.

Computer forensics involves the participation of professionals in the information technology and legal professionals because the results obtained through the application of computer forensics are subject to judicial review.

Study and Analysis on computer forensics in Bolivia allows to present what the current situation of this specialization in our country, for this information was necessary first point to make a preliminary investigation into computer forensics and all the elements that are involved in its implementation process. The following shows in detail the parts for which this research ranges from the theoretical stage to the practical phase of computer forensics.

Keywords*:* IT asset; forensic analysis; office applications; cyberbullying; Forensic Science.

Introducción

Desde la aparición de internet, durante la década de los 90 los sistemas computacionales comenzaron a ser ampliamente utilizados en entornos muy distintos a aquellos que los vieron nacer, es decir, el uso de este tipo de sistemas no solo se veía en el campo militar o en las universidades sino que también en las oficinas de diferentes compañías que ofrecían diferentes productos o servicios ya sean grandes o pequeños. Este crecimiento exponencial fue gracias a que dichos sistemas contribuían a mejorar la productividad y la calidad de tales productos o servicios, pronto pasaron de ser una herramienta de apoyo a un artículo de primera necesidad.

Con el paso de los años, el crecimiento abrumador de Internet y la necesidad de comunicarse a lo largo y ancho del mundo convirtieron a los sistemas computacionales en un elemento indispensable para el desarrollo de toda empresa u organización. Sin importar el tipo de empresa, o que tan grande o pequeña sea, existe un elemento latente involucrado en el desarrollo de estas organizaciones que resulta de vital importancia al igual que los sistemas que contribuyen a este crecimiento: *el activo de información.*

El activo de información es la representación digital de cualquier elemento de información que tenga un valor para una organización, esta información puede ser tan "irrelevante" como la distribución de los lugares de estacionamiento o tan "sensible" como la nómina de la compañía. La información es poder.

Existe una estrecha relación entre estos dos elementos, los sistemas computacionales manejan los activos de información, ya sea transportándolos, almacenándolos o generándolos. La mayoría de las interacciones posibles con los activos de información es a través de los sistemas computacionales.

Desgraciadamente los sistemas utilizados no son perfectos, simplemente son perfectibles, es por esto que la pérdida de información es un riesgo latente dentro de una organización.

Existen muchas formas de perder información, ya sea involuntariamente: daños en los equipos, accidentes, desastres naturales, entre otros o intencionalmente: robo, sabotaje, violaciones a la integridad de la información, por mencionar algunos. La pérdida de información se traduce en una pérdida de dinero, hecho intolerable para cualquier tipo de organización.

La implementación de medidas o practicas destinas a evitar la pérdida de información por alguna de estas causas puede resultar costosa y compleja según la cantidad de formas o riesgos que se pretendan evitar o disminuir.

Actualmente existen muchas acciones que atentan contra los activos de información de cualquier organización, estas acciones malintencionadas son realizadas por diferentes personas alrededor del mundo que pueden tener, o no, un objetivo bien definido que los motiva a cometer estas acciones.

Entre los principales motivos de estas personas malintencionadas se encuentra el dinero. Una persona puede conseguir activos de información de una organización y venderlos al mejor postor, puede conseguir datos personales y utilizarlos para realizar fraudes, puede inhabilitar parcial o totalmente a una organización

como forma de protesta o utilizar la infraestructura de una organización para realizar estas actividades mal intencionadas, por mencionar algunas.

Estas actividades o prácticas pueden ser consideras como delitos, según la legislación correspondiente. En Bolivia no existen suficientes leyes o talvez no están lo suficientemente elaboradas, que contemplen estas acciones y establezcan sanciones para los infractores, sin embargo aún hace falta trabajo para contemplar toda la gama de actividades malintencionadas que atentan contra los activos informáticos de las organizaciones.

Estas prácticas mal intencionadas pueden ser perseguidas para sancionar a los infractores. Para lograr este propósito es necesario realizar las investigaciones correspondientes para determinar qué fue lo que sucedió y quién es el responsable.

Para lograr este cometido existe una disciplina de la computación que se encarga del estudio de sistemas para determinar, con base en la información disponible, qué fue lo que pasó, cuándo, cómo, y quién es el responsable de las acciones que afectaron los activos de información de un sistema, esta disciplina es el cómputo forense.

El *cómputo forense* o *informática forense* es una disciplina compleja que requiere de personal altamente capacitado para realizar investigaciones que sean de utilidad para una organización que se ha visto sus activos de información afectados por algún tipo de actividad malintencionada.

El contratar los servicios de este tipo de profesionales puede ser tan costoso que no es viable para cierto tipo de empresas, por ejemplo las pequeñas y medianas empresas, también conocidas como PYMES.

Métodos

Para llevar a cabo esta disciplina se debe seguir un conjunto de métodos o procedimientos que de manera objetiva y precisa son capaces de producir resultados repetibles y verificables en una investigación al ejecutarlos de manera sistemática, prácticamente se debe ser muy cuidados al momento de extraer los datos a analizar o las pruebas necesarias para llevar a cabo la investigación, ya que un error que se cometa en este proceso podría comprometer toda la investigación y todos los datos que se hayan obtenidos serian obsoletos.

Las metodologías de investigación son herramientas que facilitan el estudio de diversos problemas, que pertenecen a una misma área, esta característica es una ventaja cuando se pretende investigar delitos informáticos, ventaja que se traduce en una reducción en el tiempo de la investigación ya que la metodología a utilizar es la misma para cada delito que se presente y se requiera estudiar.

Otra de las ventajas del uso de una metodología es que permite una fácil identificación del objeto de estudio, así como del propósito del estudio, el sujeto a quien va dirigido el estudio, el sujeto que realiza el estudio y los alcances del mismo. Toda esta ayuda se traduce en una reducción de tiempos y en una agilización de los procesos relacionados con la preparación necesaria antes de iniciar la investigación.

Una ventaja más que se obtiene al implementar una metodología de investigación es la reducción de recursos invertidos en la análisis de un problema ya que la metodología señala las pautas a

seguir de una manera clara y precisa, lo que se traduce en un menor tiempo al investigar un caso.

Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso bien sea legal u organizacional. En este sentido, se detalla de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado: Los procedimientos llevados a cabo se dividen en las siguientes etapas:

Identificación

Estando en el lugar de la escena donde se realizó el ataque informático se debe rotular con sus respectivas características físicas el elemento que va ser objeto del análisis forense, para preservar el elemento que puede ser desde un disquette o un disco rígido de un computador hasta un conjunto de discos de un servidor, un juego de cintas, o varias computadoras de una organización.

Validación y preservación de los datos adquiridos

Con el elemento identificado se procede a realizar una imagen exacta del contenido de la evidencia asignando un código único correspondiente a una combinación única de bytes que constituye la totalidad del medio en observación.

Este código de validación ha de ser lo suficientemente complejo como para evitar vulneraciones en la información rescatada e impedir que cualquier auditor pueda por su cuenta verificar la autenticidad de la imagen tomada, es decir, crear un código que solamente personal calificado y legalmente autorizado pueda manipular para proteger el elemento a ser analizado; esto con el fin de establecer una cadena de custodia consistente. Desde este momento ya se pueden efectuar copias exactamente iguales de la imagen a los efectos de que diferentes actores puedan conservar una copia de seguridad.

Análisis y descubrimiento de evidencia

Se procede a realizar una colección de pruebas en el laboratorio sobre la copia validada. Es posible analizar y buscar información a muchos niveles.

El punto de partida del análisis comienza al detectar una tipo de ataque informático o la sospecha de manipulación no autorizada de información. Una actividad ilícita reportada puede ser el borrado la información que puede comprometer a una persona o información que pudo haber sido ocultada o almacenada en medios no convencionales como disquetes, cd rom, dvd rom, flash drive. El análisis forense está orientado por un caso en particular y aquí es necesaria la información que provee quien solicita la investigación forense

En el análisis forense se pueden buscar: archivos borrados, archivos creados, accedidos o modificados dentro de determinado rango de fechas, tipos de archivos con un formato particular que hayan sido alterados, por ejemplo archivos de un sistema de contabilidad renombrados como archivos de un procesador de texto, imágenes, mensajes de correo electrónico, actividad desarrollada en internet, a diferentes niveles palabras claves tales como un número telefónico, el nombre de una

ciudad o una empresa, etc. En base a este análisis se determina un patrón de comportamiento del usuario en cuanto a la creación, modificación y borrado de mensajes, actividad de correo electrónico, etc.

Informe

Se presenta un informe escrito en un lenguaje a la vez técnico y claro y un Cd donde se hace accesible al usuario no especializado de una forma ordenada la evidencia recuperada y su interpretación.

Aunque a menudo se subestima la importancia de los pasos 1 y 2 y se considera el paso 3 el específico de la informática forense, hay que tener en cuenta que la evidencia informática es por definición frágil y puede ser alterada haciendo que la misma pierda su validez frente a un tribunal.

Resultados

Con este trabajo de investigación se espera contribuir a la concientización sobre problemas relacionados con la seguridad de la información a través de herramientas diseñadas para ser un apoyo en la investigación de delitos informáticos basados en cómputo forense, de fácil acceso y de libre distribución.

Discusión

El conocimiento de informática forense por parte de las entidades involucradas en el esclarecimiento de delitos informáticos es escaso, es decir, teórico; lo que indica que en el país se está iniciando esta especialidad. Por la razón de que esta temática es nueva, tanto para jueces, abogados y fiscales estos tienen desconfianza de la utilización de esta especialidad como herramienta para el análisis de evidencias digitales porque no poseen bases sólidas sobre ella.

Conclusiones

Hace falta mucho trabajo de difusión y concientización en temas de seguridad entre las empresas, entidades de gobierno y el público en general, hace falta gente especializada que se encargue de hacer esa difusión y que sea capaz de generar soluciones en materia de seguridad de la información para hacer frente a todas las amenazas a las que está expuesta la información ya sea del gobierno, empresas e incluso nuestra propia información.

Agradecimientos

A los docentes de la Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones que me brindaron su apoyo en el proceso de la investigación realizada.

Referencias

Cabrera M. H. Informática Forense - UNAD

Martines C., Jeimy J. Introducción a la informática forense. Revista ACIS junio de 2006 Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf
http://www.informaticaforense.com/criminalistica/
http://www.nist.gov/itl/
Rifa H. et al. Análisis forense de sistemas informáticos

Presentado: Santa Cruz, 17 de Septiembre de 2016.

Aceptado: La Paz, 10 de Octubre de 2016.