El reto de los investigadores informáticos para contrarrestar las técnicas anti-forense

Marulanda Juan Carlos, Acosta Luis Hernando
Juancmarulanda@gmail.com, lucho.acosta@gmail.com
Especialización Seguridad Informática, Universidad Piloto de Colombia, Bogotá, Colombia

***Abstract* - Speaking about forensic computing in a legal process, it is common to use trusted and documented techniques that allows the evidence to be appreciated and become relevant and valid to use. Through the use of these techniques the reconstruction of the digital evidence is sought by using software or hardware that leads to meet the incorruptibility and integrity of the evidence. With all this, ciber-criminals make use of anti-forensic techniques to avoid being discovered or incriminated, that's the reason why they make use of tools that allows to destroy or even make all evidence unrecoverable, achieving that proofs don't get to be validated at any legal instance. This because it's a true challenge for investigators to defy all techniques that come every day and let crimes in impunity.**

Key words: computer forensics, controls, evidence, information security, integrity.

***Resumen* - Al hablar de informática forense se hace uso de técnicas ya documentadas y veraces ante un proceso legal ya que deben cumplir con reconocimiento, confiabilidad y relevancia de la información que se utilice en este tipo de procesos. Por medio de estas técnicas se busca la reconstrucción de la evidencia digital ya sea haciendo el uso de software o hardware que lleven a cumplir con la inalterabilidad y la integridad de la evidencia, con todo esto los ciber delincuentes hacen uso de técnicas anti-forenses para evitar ser incriminados o descubiertos, por eso hacen uso de diferentes herramientas que permiten destruir o hacer irrecuperable toda evidencia o parte de ella y lograr que esta no se validad ante cualquier instancia legal. Es por esto que significa un verdadero reto para los expertos investigadores, el contrarrestar todas estas técnicas que día a día surgen y que dejan muchos crímenes en la impunidad.**

Palabras Clave: controles, evidencia, informática forense, integridad, seguridad de la información.

I. INTRODUCCIÓN

Debido a que los delitos informáticos aumentan considerablemente cada día, los investigadores deben prepararse mucho mejor en cuanto a estudiar y analizar la mayoría de las formas utilizadas para cometerlos.

Existen muchas herramientas para analizar las evidencias recuperadas en este tipo de delitos, y en la gran mayoría de los casos son efectivas, por lo cual quienes infringen la ley buscan también la manera de burlar estos procedimientos, para que si llegan a perder algún dispositivo en el que tengan almacenada información sensible, no pueda ser recuperada y presentada como evidencia ante algún eventual proceso que se pueda llevar a cabo por versen comprometidos en el contenido de dicho dispositivo.

El reto de los investigadores o peritos informáticos es el de contrarrestar estas técnicas "anti- forenses" por medio de la ejecución de nuevas tecnologías, realizando una actualización de los métodos implementados en busca de información que permita ser presentada como evidencia relevante en un determinado juicio.

II. INFORMÁTICA FORENSE

Es una disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso [1].

Se conoce también como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos [1].

Según esto por medio de la informática forense se pueden obtener resultados valiosos que permiten llegar a una verdad, por medio de un procedimiento concertado, el cual procura garantizar de alguna manera el origen de los datos, así como la preservación de la información para una consulta posterior.

También se conoce como una disciplina que se basa en las nuevas tecnologías para cumplir con el propósito de analizar adecuadamente las pruebas recolectadas en incidentes o casos en los que se ha cometido algún delito para que dicha evidencia no sea rechazada por algún manejo inadecuado de las herramientas actualmente disponibles.

Cuando hablamos de informática forense es donde comprobamos la efectividad de las políticas de seguridad de la información sino también de las tecnologías que se utilizan poder disponer de la información.

III. EVIDENCIA DIGITAL

La evidencia digital es un tipo de evidencia física, es aquella evidencia construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados, almacenados y analizados con herramientas técnicas especiales [2].

La evidencia digital es una denominación usada de manera amplia para describir cualquier registro generado o

almacenado en un sistema computacional que puede ser utilizado como prueba en un proceso legal [2].

La evidencia digital es de gran importancia en la informática forense ya que realmente lo que se analiza es la información contenida o almacenada en cualquier sistema digital presentado como evidencia, sin ella no se tendría nada para analizar en un proceso que se quiera esclarecer usando técnicas forenses.

Podemos considerar de vital importancia que toda información digital debe ser considerada y evaluada para su uso ante cualquier ente acusatorio ya que como esta sea manejada puede ser útil o no.

Existe un procedimiento que se debe llevar a cabo para la recolección de evidencias y que se debe cumplir sigilosamente para no alterar la información y también para que la evidencia recolectada sea válida en los procesos judiciales según las leyes Colombianas. Este proceso incluye documentar cada paso que se realice en la adquisición de la evidencia, de lo posible grabarlo o tomar fotografías, embalar la evidencia de tal forma que no sufra cambios es decir se preserve tal cual se adquiere, analizar la evidencia con las herramientas adecuadas para que esta no se altere y presentar el informe conforme a la ley.

IV. TÉCNICAS ANTI-FORENSES

El reconocimiento de muchas de las técnicas y vulnerabilidades que tienen los O.S. se genera procedimientos de informática forense, por eso se generaron las llamadas técnicas anti-forenses. "cualquier intento de comprometer la disponibilidad de la evidencia para un proceso forense" [3].

Las técnicas anti-forenses es el momento en que cualquier evidencia se compromete en el proceso de forense permitiendo afectar la disponibilidad, la confiabilidad y la relevancia de la evidencia del proceso forense de un delito informático; estas acciones que realicen los atacantes son definidas por investigadores informáticos como técnicas anti-forenses ya que comprometen con facilidad y claridad el proceso forense lo que exige replantear todos los procesos para la investigaciones futuras.

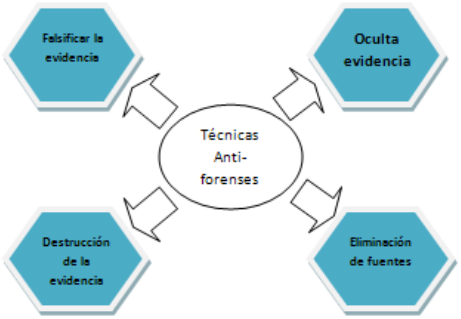
V. CLASIFICACIÓN DE MÉTODOS ANTI-FORENSES

La definición de los métodos anti-forenses se generan acorde al tipo de ataque que se genere por eso vamos a tomar calificaciones básicas y estándar que podemos hacer uso ante un ataque.

Para efectos de este trabajo se tomará la clasificación planteada por (Harris 2006) a saber [4]:

- Destrucción de la evidencia.
- Ocultar la evidencia.
- Eliminación de las fuentes de la evidencia.
- Falsificación de la evidencia.

Figura 1
Clasificación de métodos anti-forenses



De acuerdo a los diferentes niveles de complejidad de los métodos que utilicen los atacantes estos siempre hacen uso de software o hardware para hacer sus acciones.

Según Harris para el acercamiento a cada método propuesto hacen uso de herramientas anti-forenses para realizar:

A. Destrucción de la evidencia

Con este buscan evitar que la evidencia se encontrada de manera fácil, en el momento que el investigador la encuentre a este no se le facilitara o le será inaccesible recuperarla o accederla para ser usada como una evidencia en el momento de una audiencia judicial, ya que los daños que se pueden realizar a la evidencia pueden llegar a ser lógicos o físicos y estos pueden realizarse por medio de herramientas diseñadas para esta acción por ejemplo: PGP, SSWAP, Wipe. [4] entre otras.

B. Ocultar la Evidencia

Esta busca que el investigador no pueda acceder a la evidencia de una manera fácil o que por lo menos no le sea de una manera fácil visualizarla, para esto generalmente hacen el uso de software como de estenografía o marcas de agua por ejemplo: Hide and Seek, StegoDos, White Noise Storm S-Tools, Jpeg-Jsteg. Estas herramientas no hace que sean imposibles de recuperar pero si complica mucho su proceso.

C. Eliminación de la fuentes de la evidencia

Este método busca que la evidencia se pueda anular desde su inicio ya que no han sido destruidas desde su creación, esto se produce haciendo uso de herramientas que de la ventaja de ocultar cualquier tipo de rastro que lo incrimine como log o registros; dependiendo el tipo de ataque la herramienta cambia.

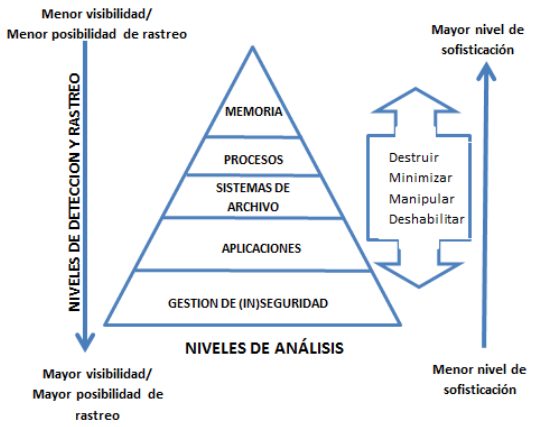
D.Falsificación de la evidencia

Con esto se busca por parte del atacante engañar a los investigadores de donde está la verdadera evidencia o desviar al investigador para que le quede imposible encontrar las verdaderas evidencias ante cualquier investigación o no sean legales y válidas.

VI. MODELO CONCEPTUAL DE DETECCIÓN Y RASTREO DE TÉCNICAS ANTIFORENSES – MODERATA[1]

Con este modelo se pretende establecer una serie de pasos que permitan brindar ayuda en los procedimientos forenses con el fin de evitar o contrarrestar las técnicas anti-forenses, dando a los investigadores una guía para recolectar adecuadamente la información.

Figura 2
Modelo conceptual de detección y rastreo de técnicas anti-forenses – MODERATA [1]



VII. FUNDAMENTOS DE LAS INVESTIGACIONES EN MEDIOS INFORMÁTICOS

La informática forense tiene como objetivo principal conseguir información relevante no solamente para procesos judiciales, también es usada para recuperar información accidentalmente borrada y que pueda ser relevante para el funcionamiento de la empresa, para algunas auditorías internas dentro de organizaciones, entre otras situaciones en las que se hace necesaria la ejecución de un proceso informático forense.

Figura 3
Fundamentos de las investigaciones en medios informáticos [1]

A. Reconocimiento

Utilización exhaustiva de diferentes métodos, prácticas y herramientas que han sido desarrolladas para operar en un ambiente particular para recolectar, recuperar, decodificar, extraer, analizar y convertir datos que serán mantenidos en medios de almacenamiento verificables y accesibles como evidencia [1].

B. Confiabilidad

Mantenimiento de la cadena de custodia durante la extracción, análisis, almacenamiento y transporte de los datos [1].

C. Relevancia

Está relacionada con el peso y la utilidad de la evidencia en el proceso. Si existe una orientación sobre qué se debe recoger durante el proceso, esto puede ayudar a mejorar el esquema de tiempos y costos [1].

Las investigaciones en medios informáticos deben cumplir con las etapas de reconocimiento, confiabilidad y relevancia, en las que se debe insistir para que se lleven a cabo buenas prácticas que permitan realizar un adecuado análisis, para que las evidencias recolectadas sean de gran ayuda en determinada situación.

VIII. CONSIDERACIONES PARA CONTRARRESTAR LAS TÉCNICAS ANTI-FORENSES

Un analista forense debe, además de estar muy bien entrenado, conocer todas las herramientas que puede utilizar para tomar las medidas adecuadas en los procesos que involucran técnicas anti-forenses, realizar actualizaciones de los cursos, certificaciones y demás niveles de estudios relacionados con la informática forense, utilizar una metodología en la que pueda llevar una bitácora y toda forma que pueda implementar para registrar los pasos utilizados durante el proceso de recolección y análisis de las evidencias.

También se deben realizar ajustes a las políticas que se lleven en cuanto a seguridad, para lograr realizar controles efectivos que permitan identificar a tiempo los malos procedimientos que se lleven en cuanto al manejo de información.

En cuestiones físicas se deben usar herramientas y toda clase de hardware con lo más avanzado en tecnología posible, para no dar ventajas a los delincuentes que usando técnicas anti-forenses en muchos casos no tienen los recursos necesarios para actualizar sus equipos.

IX. LAS TECNOLOGÍAS DE INFORMACIÓN Y LA IMPLEMENTACIÓN DE NUEVAS LEYES

Debido a que cada vez se implementan más las tecnologías de la información de parte de las organizaciones se hace

necesario implementar un control para que su uso, no permita que se cometan delitos informáticos, es por esto que los investigadores de informática forense además de las herramientas para analizar evidencia, cuentan con nuevas leyes aprobadas en Colombia como la ley 1266 de 2008, llamada también Ley de Habeas Data, la ley estatutaria 1581 de 2012 para la protección de datos personales, ley 1273 de 2009 de la protección de la información y de los datos, entre otras, y día a día se estudian nuevas leyes para no dejar nada al libre albedrío de los delincuentes.

Una de las formas de garantizar que los datos sean seguros sería dejar de usar las tecnologías y volver al correo escrito en papel, pero debido al auge económico que con lleva la implementación de las TIC'S, todo apunta a que cada día los investigadores en informática forense tendrán más retos y cambios en la forma en que realizan sus análisis, y la parte legislativa tendrá que ir cambiando acorde a estas nuevas tecnologías.

X. Conclusiones

A medida que las infraestructuras de seguridad informática se vean mayormente afectadas por el aumento de ataques tendrán que incrementar las barreras para proteger sus datos, esto se verá reflejado en nuevas o mejores oportunidades de encontrar fallas en las políticas de seguridad que se implementen en las organizaciones.

La informática forense tiene dentro de sus funciones realizar la prevención de la fuga de información dentro de una organización, por eso es muy importante auditar y hacer pruebas técnicas de los elementos de protección implementados e instalados, para poder detectar cualquier vulnerabilidad de seguridad que se tenga, para que sea corregida antes de que pueda causar algún daño sensible de la información que se maneja.

Día a día podemos observar que no basta solo con técnicas para recuperar evidencia informática, sino que también es de vital importancia Implementar técnicas que no permitan la inhibición de evidencia por procedimiento de parte de los delincuentes. Además, es de anotar que un investigador informático debe estar en constante actualización con dichos temas, para estar un paso adelante siempre de aquellos infractores de la ley.

Una de las partes más delicada en el proceso de los sistemas informáticos tiene que ver con el manejo de la seguridad de la información, este proceso tiene muchas falencias porque la información puede ser manipulada y alterada por terceros para fines delictivos.

Los sistemas presentan vulnerabilidades, por lo que se deben tomar medidas preventivas como la encriptación de la información relevante, mantener un backup actualizado de la información, monitorear y registrar log's de las transacciones, tener un sistema de alarmas para situaciones anormales, además se debe hacer un buen manejo de la información que circula por cache, entre muchas otras situaciones que se pueden presentar para mantener la seguridad de la información y poder de alguna manera reducir los ataques que se gestan en todo este tipo de situaciones.

Se debe tener en cuenta que las bases de la información a pesar de las nuevas tecnologías, cada vez son más susceptibles y presentan más vulnerabilidades, por lo que se debe llevar una adecuada documentación de los registros que se lleven en una investigación.

XI. Referencias

[1] Cano, J., "Introducción a la Informática Forense, Una Disciplina Técnico-Legal," Revista SISTEMAS, Asociación Colombiana de Ingenieros de Sistemas (ACIS), No. 96, www.acis.org.co

[2] CANO, J. (2007) Inseguridad informática y Computación anti-forense. Dos conceptos emergentes en seguridad informática. Disponible en: http://www.virusprot.com/computaci%F3n-anti-forense.htm

[3] Arckoff R., Addisson H. (2007), Management F-Law. How Organizations Really Work.

[4] R.Harris. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. http://dfrws.org/2006/proceedings/6-harris.pdf

Autores

Juan Carlos Marulanda, es Ingeniero de sistemas de la Fundación Universitaria San Martín, tiene diez años de experiencia en infraestructuras tecnológicas, trabaja en Dafiti Colombia como ingeniero de redes y sistemas implementando todo la infraestructura y seguridad de la empresa.

Luis Hernando Acosta, es Ingeniero de Sistemas de la Universidad de Cundinamarca, tiene más de cinco años de experiencia en el desarrollo de aplicaciones, trabaja como Analista SOA en Assist Consultores de Sistemas, su trabajo consiste en analizar, diseñar, desarrollar, probar e implementar servicios web para ATH y el grupo Aval.