Aspectos Relevantes de la Informática Forense en la actualidad y su importancia

Oviedo Calderón Javier Eduardo
ing.javieroviedo@yahoo.com.co
Universidad Piloto de Colombia

Abstract - Computer forensics is one of the most important and promising in computer security specialties. In recent times have increased significantly cases where the means and tools have been key to the commission of crimes either right inside an organization, where usually a person inside helps commit the crime, or either from outside where people with specific skills and training manage to penetrate computer networks to infringe in any way against their technological infrastructure affecting the confidentiality, integrity and availability of information; this thanks to security holes that sometimes managers fail to identify and therefore fail to correct, or simply weak controls that are within organizations in all aspects. That's where computer forensics as a technical and legal discipline, it is essential to achieve clarify facts that at first glance seem indecipherable providing key evidence in supporting the legal process.

Resumen-La informática forense es una de las especialidades más importantes y con mayor futuro dentro de la seguridad informática. En los últimos tiempos se han incrementado de manera significativa los casos en donde los medios y herramientas informáticas han sido claves para la perpetración de delitos, ya sea desde el interior mismo de una organización, en donde generalmente una persona de adentro ayuda a cometer el ilícito, o bien sea desde afuera donde personas con formación y habilidades específicas logran penetrar a través de las redes informáticas para atentar de alguna manera contra su infraestructura tecnológica, afectando la confidencialidad, integridad y disponibilidad de la información; esto gracias a los huecos en la seguridad que algunas veces los administradores no logran identificar y por lo tanto no logran corregir, o simplemente por los débiles controles que se tienen al interior de las organizaciones en todos los aspectos. Ahí es donde la informática forense, como una disciplina técnica y legal, se hace indispensable para lograr esclarecer hechos que a simple vista parecen indescifrables aportando evidencias fundamentales a la hora de apoyar procesos legales.

Índice de Términos - Evidencia digital, computación forense, sistema de información, autenticidad, confiabilidad, suficiencia, leyes y regulaciones, proceso judicial, hash.

I. INTRODUCCIÓN

Hace unas décadas atrás no era tan frecuente encontrar en las noticias casos importantes en donde se cometieran delitos mediante la utilización de herramientas informáticas, en cuanto a la informática forense como especialización, ni siquiera existía; esto es debido a que años atrás no se contaban con tantas y tan diversas tecnologías en el mercado como las que se tienen hoy día, incluyendo la internet. Años atrás, pensar que se podía tomar dinero, información u otros recursos de personas o entidades de cualquier tipo incluyendo gobiernos mediante la utilización de herramientas informáticas para beneficio propio o el de terceros, era impensable, por lo que tampoco existía ningún tipo de legislación que permitiera definiciones claras de lo que se podía considerar como delito o no.

Hoy en día las tecnologías han crecido de manera significativa, generando nuevos riesgos a nivel de seguridad de la información, lo que ha obligado a gobiernos de todo el mundo a tomar en serio dicha seguridad y empezar a legislar con el fin de controlar y tipificar en la ley diferentes acciones como delitos informáticos, para el caso de Colombia por ejemplo, se crea la ley 1273 del 05 de enero de 2009, "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" [1].

Posteriormente aparece la ley estatutaria 1581 del 17 de octubre de 2012 [2], "por la cual se dictan las disposiciones generales para la protección de los datos personales". En estos nuevos tiempos la importancia de la informática forense radica en que puede ser útil para manejar desde un simple

incidente de pérdida de información u ocultamiento de la misma, hasta aspectos de seguridad nacional.

II. LA INFORMÁTICA FORENSE ES CONSIDERADA COMO UNA DISCIPLINA TÉCNICA Y LEGAL

La informática forense es considerada en muchos aspectos como una disciplina que ayuda, apoya o auxilia a la justicia ofreciendo garantía de veracidad en procesos judiciales, ya que se apoya en diferentes técnicas, herramientas y conocimientos que logran evidenciar las acciones de los diferentes intrusos informáticos.

Para definir en pocas palabras la informática forense, podemos decir que es una rama de la informática relacionada con obtener y analizar datos que pueden estar almacenados en medios tecnológicos como discos duros, memorias USB, discos compactos, entre otros.

El objetivo de dicho análisis es que la información obtenida pueda ser utilizada como una evidencia probatoria ante un ente judicial para casos de litigios o alguna autoridad dentro de una empresa, ya sea un jefe, coordinador, administrador, gerente, etc. En todo caso es información que prueba que se cometió una conducta inapropiada o que va en contra de normas, decretos, leyes, políticas, procedimientos, entre otros.

Ya se había mencionado anteriormente que cada vez son más frecuentes los reportes de violaciones y ataques a diferentes plataformas tecnológicas y sistemas de información gracias al aprovechamiento de las vulnerabilidades encontradas por los atacantes, las cuales pueden tratarse de fallas humanas, tecnológicas y hasta fallas en procedimientos.

Cabe recordar que los atacantes poseen diferentes motivaciones, cada atacante es diferente de otro, cada uno utiliza diferentes estrategias lo que hace del trabajo del forense algo fascinante pues entre un caso y otro pueden existir diferencias abismales. Es precisamente esa experiencia la que hace que el profesional adquiera cada vez más elementos de juicio que le ayudan a indagar e interrelacionar la información entre un caso y otro con el fin de encontrar pistas importantes que le ayuden con la investigación y finalmente con la solución del caso.

La parte técnica la informática forense provee procedimientos y técnicas indispensables para el manejo de la evidencia en la escena del crimen, tales como:

A. Identificación.

Debe tenerse en cuenta los procesos para una buena identificación de los elementos y el lugar de los hechos los cuales servirán de pruebas posteriormente.

B. Extracción.

Deberán seguirse los procedimientos adecuados y definidos por las técnicas forenses para la extracción de los datos en equipos de cómputo y demás elementos encontrados en la escena en donde se pueda almacenar información.

C. Preservación.

Los procedimientos orientados a la preservación de la evidencia recolectada son claves para evitar daños o corrupción de la misma garantizando su integridad y conservando su valor probatorio, es indispensable la cadena de custodia.

D. Análisis e interpretación.

Se refiere al análisis de los datos obtenidos en el proceso de extracción para poder convertirlos en información más clara que aporte valor a la investigación, posteriormente dicha información deberá ser interpretada de la mejor manera posible para convertirla en material probatorio preciso, irrefutable, claro y entendible para todos los públicos.

E. Documentación y presentación.

La informática forense nos obliga a cumplir los requisitos documentales, como por ejemplo en la manera de presentar los informes técnicos o periciales.

La información debe cumplir con un propósito, teniendo en cuenta la redacción, ortografía, la terminología empleada, la cual debe ser clara y las expectativas del público al que está dirigida.

III. OTRAS CONSIDERACIONES JURÍDICAS DE ASPECTO GENERAL

Considerando que en nuestro país ya se dieron pasos importantes en materia de legislación informática dada la creciente aparición de casos en donde las nuevas tecnologías se convierten en herramientas principales para la comisión de delitos como se mencionó anteriormente, ejemplo de ese interés por controlar, normalizar y penalizar actuaciones consideradas como delictivas son las diferentes leyes creadas:

- Ley 527 de agosto de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [3].
- Ley 1266 del 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones [4].
- Ley 1273 de enero 5 de 2009, 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 más reciente decreto que entro en vigencia para aportar a este tema, fue el decreto 1377 del 27 de junio de 2013, por el cual se reglamentó parcialmente la ley 1581 de 2012 para protección de datos personales [5].
- Por otra parte en el año 2013 entra en vigencia en la ciudad de Bogotá el proyecto de acuerdo 037 de 2013, "Por medio del cual se establece la Estrategia de Ciberseguridad para enfrentar ciberdelitos y amenazas contra el Distrito Capital", esto con el fin de: "establecer una estrategia sobre Ciberseguridad en el Distrito Capital, como un mecanismo para enfrentar amenazas contra la Ciberseguridad o Seguridad Informática en el territorio de Bogotá [6].

Algunas entidades del Estado, como del Distrito Capital, han padecido ataques a sus bases de datos, información, infraestructura y equipos de sistemas y cómputo (informáticos), alterando productos y resultados, con la consecuencia inmediata de demora en la información o pérdida de la misma. Como ejemplo de ello, se pueden mencionar los ataques que sufrió la Registraduría Nacional del Estado Civil durante las elecciones legislativas de 2010- 2014, los ataques a la Empresa de Acueducto y Alcantarillado entre otros.

Entre otros, algunos casos de ciberataques contra el Estado o el Distrito Capital se mencionan: Ataque masivo de hackers contra la Registraduría.[1] Conforme lo cita la fuente de El Universal, "Pese a que un informe del Cuerpo Técnico de Investigación de la Fiscalía (CTI), elaborado en mayo de 2010, determinó que hubo un ataque masivo de hackers al programa informático de la Registraduría Nacional durante las elecciones parlamentarias del 2010, que a la postre hizo colapsar al sistema de datos; la Fiscalía decidió archivar la investigación por considerar que las pruebas no eran suficientes. Dichos ataques provinieron del Ministerio de Defensa, el Departamento Administrativo de Seguridad (DAS) y, en especial, desde la Policía Nacional". Citó la fuente."

En este mismo documento se presenta el siguiente gráfico de proyección de crecimiento de la amenazas en internet, solo para la ciudad de Bogotá.

Malware Evolution

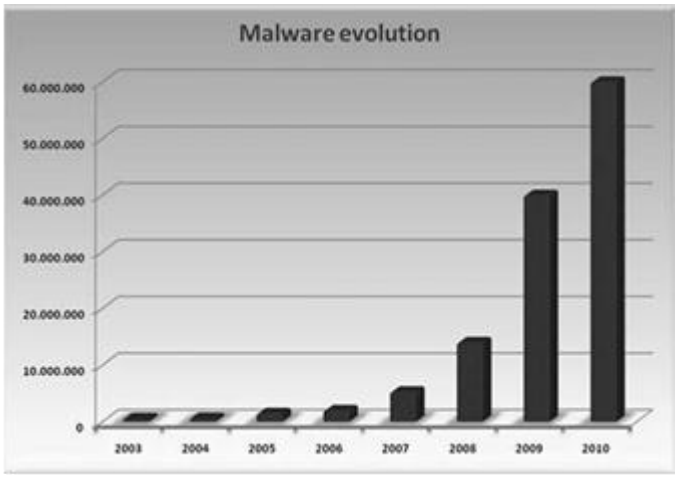

Fig. 1. Proyección de Crecimiento de las amenazas en Internet en Bogotá. [7]

De igual manera se indica como resultado del informe que: “las tendencias en cuanto a amenazas se destaca, entre otras cosas, el aumento dramático en frecuencia y sofisticación de los ataques dirigidos a las empresas; el crecimiento continuo de sitios de redes sociales como plataforma de distribución de ataques; y un cambio en las tácticas de infección, cada vez más focalizados en vulnerabilidades de Java para irrumpir en los sistemas informáticos tradicionales.

En conclusión, el informe resalta que los ataques segmentados, las amenazas en las redes sociales, la seguridad de los dispositivos móviles y la proliferación de herramientas de ataque son las principales tendencias en el panorama actual de amenazas y seguirán dando de qué hablar en el mundo tecnológico en los próximos meses, más aun si se tiene en cuenta las posibilidades de saboteo de parte de enemigos políticos, y delincuencia de todo tipo en contra de los sistemas de información del Distrito Capital.”

El acuerdo 037 es una muestra de la criticidad del asunto y los riesgos que afrontan las organizaciones. Sin embargo el tema no termina allí, nuestro gobierno ha empezado a pensar el tema a un nivel superior pensando en escenarios que afectan la seguridad nacional como ciberataques a gran escala provenientes de otros países. Es allí cuando el ministerio de Tecnologías de la información y las comunicaciones incluye en su agenda estratégica de innovación el tema de la Ciberseguridad en Julio de 2011, y surge el documento Conpes 3701 de 2011el cual describe los lineamientos de la política para Ciberseguridad y Ciberdefensa [8].

Aunque estas leyes y decretos constituyen avances importantes en materia legislativa, es de considerar que aún falta mucho camino por recorrer, los delincuentes informáticos siguen buscando cada día nuevas y mejores formas de camuflarse, esconder rastros, pasar desapercibidos y hasta aprovechar el desconocimiento mismo de las leyes por parte de los investigadores e incluso aprovechar aquellos errores cometidos al aplicar mal el debido proceso u omitirlo. Por esta situación se puede convertir fácilmente la evidencia digital encontrada, la cual es el insumo principal para un proceso legal, en evidencia que carece completamente de validez y llevar a que se pierda un proceso judicial [9].

Esta es una razón más que hace que la informática forense sea de enorme importancia en el momento de enfrentar un proceso jurídico ya sea como acusado o acusador.

Es importante tocar un poco el tema de la evidencia digital y su tratamiento, de lo cual se hablará un poco más adelante.

Para poner un ejemplo claro de situaciones en donde los errores en procedimientos afectan la decisión de un tribunal, se expone uno de los casos más sonados en nuestro país en donde muchas personalidades de la vida política nacional se vieron involucradas con grupos al margen de la ley, y en donde jurídicamente no fue posible hacer nada al declarar como inválidas dichas pruebas, el caso de los computadores del jefe guerrillero Raúl Reyes [10]. Esto fue lo que dijo la Corte Suprema de Justicia: “En este caso no puede haber generalizaciones. La Corte solo se pronunció en lo de su competencia y los jueces internacionales pueden abocar el tema", indicó el presidente de la Sala Penal de la Corte, magistrado Javier Zapata, en referencia a los procesos judiciales iniciados en países como España y Chile, gracias a la información de los computadores.

Según los magistrados, las autoridades judiciales extranjeras, y eventualmente la Corte Penal Internacional (CPI), que requieran esos elementos cuentan con plena libertad para analizarlos como prueba y con la autoridad para darles validez, si así lo consideran.

La Corte negó un recurso de reposición del procurador Alejandro Ordóñez y se mantuvo en que las pruebas son ilegales en Colombia por haber sido obtenidas en un país extranjero sin autorización de las autoridades locales, y además porque supuestamente se violó la cadena de custodia. Sin embargo, los magistrados reiteraron que la información puede ser utilizada, no como prueba principal, en investigaciones judiciales.

Los computadores y USB fueron obtenidos por la Policía después del bombardeo al campamento que 'Reyes' había montado en Sucumbíos, a pocos kilómetros de la frontera con Colombia, en marzo del 2008.

Tampoco aceptaron la tesis del Procurador, que en la apelación dijo que la actuación de las Fuerzas Militares y de Policía se enmarcó dentro del

suficientes que son utilizadas como material probatorio dentro del proceso, normalmente este se viene abajo y se termina o se dilata en el tiempo.

El profesional en informática forense debe agotar todos los recursos y tratar de aprovechar al máximo cada una de las evidencias recolectas y tener la capacidad de correlacionar dichas evidencias con otras, a fin de hacer un mejor y más preciso análisis y así aportar cada vez más valor a la investigación representado en más evidencia. Si se logra esto se ayuda más con el principio de suficiencia, como ya se dijo, entre más pruebas existan mayor será la probabilidad de evitar que un proceso de defensa o de acusación se vaya de las manos; el objetivo finalmente es que no hayan dudas de la evidencia presentada.

D. Conformidad con leyes y regulaciones.

Esta es otra de las características consideradas como factor de éxito al recoger, almacenar y analizar las evidencias digitales, ya que éstas deben tratarse conforme a las regulaciones y leyes de cada país. Anteriormente, en este mismo documento se mencionaron algunas leyes y decretos que aportan definiciones importantes en temas de delitos informáticos.

Cabe recordar que la importancia radica en que muchos casos judiciales se pierden debido al incumplimiento de los procedimientos y mandatos encontrados en dichas leyes, acuerdos y regulaciones. Como ejemplo se expuso el sonado caso de los computadores del jefe guerrillero Raúl Reyes, en donde al final las pruebas fueron anuladas por no seguir el procedimiento de recolección.

A nivel de derecho procesal en Colombia, se cuenta con el Código de Procedimiento Penal, ley 906 de 2004, esta ley contempla también algunos aspectos relacionados con los procedimientos para la investigación de delitos informáticos [12].

La Organización de los estados Americanos (OEA) presenta un documento resumen de 3 páginas en donde destaca aquellos artículos de Ley 906 de 2004, que están relacionados con la recolección de evidencia digital. Documento titulado Ley 906 de 2004, El congreso de la República [13].

En este mismo documento se hace énfasis en lo que está contemplado como evidencia física y material probatorio de la siguiente manera: “Se anota que en los términos del artículo 275 del código de procedimiento penal se consideran elementos materiales probatorios y evidencia física: el mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen”.

Una buena evidencia debe contener por lo menos los cuatro aspectos mencionados con el fin de que sea declarada como admisible, por su parte, el Dr. Peter Sommer experto en investigación y evidencia digital, en su documento llamado Directors and Corporate Advisors’ Guide to Digital Investigations and Evidence, indica lo siguiente: “La evidencia es la que se ofreció ante un tribunal para persuadir a llegar a una visión particular de eventos que pueden ser objeto de controversia [14].

En general, las evidencias pueden ser:

- Reales: Un objeto que puede ser llevado a los tribunales y se examina en el lugar.
- Testimoniales: Las observaciones de testigos oculares de alguien que estaba presente y cuyos recuerdos se pueden probar ante el tribunal.
- Documentales: Un registro de negocios u otro en cualquier forma que, una vez que este ha sido autenticado, se puede examinar el contenido.
- Técnicas: Donde un técnico forense ha llevado a cabo algunos procedimientos en la prueba original "real" y ha producido algunos resultados. Las pruebas técnicas, a los ojos de la corte, no son lo mismo que las pruebas periciales, que también incluye dar opiniones.
- De expertos: Las opiniones de alguien que es experto en un campo y/o las conclusiones de ese experto después de llevar a cabo una investigación específica.
- Derivados: un gráfico, vídeo, etc. creado a partir de la evidencia primaria para ilustrar cómo ciertas conclusiones se pueden sacar”.

Los aspectos anteriores son claves en los resultados de una investigación. La evidencia lo es todo y no pueden dejarse aspectos a la imaginación de nadie, las evidencias deben satisfacer todos escenarios, deben ser precisas, claras, contundentes e irrefutables con el fin de llevar a los delincuentes ante la justicia e impedir que estos se salgan con la

suya y así contribuir de manera activa y responsable con nuestra sociedad que tanto lo necesita.

IV. CONCLUSIONES

La informática forense es una disciplina que cada vez toma más importancia debido a la creciente aparición de nuevas formas de delinquir, utilizando para ello elementos tecnológicos y digitales en donde el informático forense pueda aplicar sus conocimientos y destrezas con el fin de recolectar evidencias digitales sólidas y concretas que ayuden a dar soporte en un proceso judicial.

El buen manejo de la evidencia digital, la aplicación de procesos y procedimientos adecuados conforme a las buenas prácticas internacionales y regulaciones de cada país, hará que dicha evidencia posea mayor credibilidad y autenticidad aportando de esa manera a que un proceso judicial sea ganado.

La suficiencia también es una característica de la evidencia que debe tenerse en cuenta para evitar controversia.

Un buen profesional en informática forense es aquel que tiene la capacidad de pensar como lo haría un delincuente para cometer un acto criminal y así encaminar su investigación, aprovechando su gran experiencia y conocimientos técnicos para llevar a cabo su tarea sin cometer errores, consiguiendo la mayor cantidad de evidencia posible y cuidando meticulosamente cada etapa del proceso de investigación para evitar que sus evidencias sean declaradas como invalidas en posibles procesos judiciales.

REFERENCIAS

[1] Alcaldía Mayor de Bogotá “Ley 1273 de 2009” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] Alcaldía Mayor de Bogotá “Ley estatutaria 1581 de 2012” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[3] Alcaldía Mayor de Bogotá “Ley 527 de agosto de 1999” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[4] Alcaldía Mayor de Bogotá “Ley 1266 del 31 de diciembre de 2008” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

[5] Alcaldía Mayor de Bogotá “Decreto 1377 del 27 de junio de 2013” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[6] Alcaldía Mayor de Bogotá “PROYECTO DE ACUERDO 037 DE 2013” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

[7] Alcaldía Mayor de Bogotá “PROYECTO DE ACUERDO 037 DE 2013” [online]. Imagen disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

[8] MINTIC “Conpes 3701 de 2011” [online]. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[9] HB:171 2003 Guidelines for the Management of IT Evidence, pp. 9. [online]. Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[10] El Tiempo.com “Caída de pruebas del PC de Reyes no afecta proceso de Piedad Córdoba” [online]. Disponible en: http://www.eltiempo.com/archivo/documento/CMS-10064845

[11] Jeimy J. Cano M. “Computación Forense” (descubriendo los rasgos informáticos) 3thr ed. México: Alfaomega, 2009, pp. 108

[12] Alcaldía Mayor de Bogotá, “LEY 906 DE 2004” [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787

[13] Organización de Estados Americanos, “LEY 906 DE 2004” (República de Colombia), [online]. Disponible en: http://www.oas.org/juridico/spanish/cyb_col_ley_906_2004.pdf

[14] Institute for Advanced Architecture of Catalonia (IAAC) “Directors and Corporate Advisors’ Guide to Digital Investigations and Evidence” [online]. Disponible en: http://www.4law.co.il/cr31005.pdf

[15] Jeimy J. Cano M. “Computación Forense” (descubriendo los rasgos informáticos) 3thr ed. México: Alfaomega, 2009

Autor

Javier Eduardo Oviedo Calderón
Ingeniero de Sistemas – Universidad Cooperativa de Colombia
Estudiante Especialización en Seguridad Informática - Universidad Piloto de Colombia