

Introducción a la informática forense

Jeimy J. Cano, Ph.D, CFE

Una disciplina técnico-legal

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos. [KSHETRI 2006, SUNDT 2006] Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos de especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar

donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En consecuencia, este breve documento busca ofrecer un panorama general de esta especialidad técnico-legal, para ilustrar a los lectores

sobre los fundamentos generales y bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, unos nuevos científicos que a través de la formalidad de los procesos y la precisión de la técnica buscan decirle a los intrusos informáticos que están preparados para confrontarlos y procesarlos.

Definiciones

Existen múltiples definiciones a la fecha sobre el tema forense en informática [MCKEMMISH 1999]. Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, *digital forensics* (forensia digital), *network forensics* (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

Es importante anotar, que al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asumen dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen como son: identificación, preservación, extracción, análisis, interpretación, documentación y pre-

sentación de las pruebas en el contexto de la situación bajo inspección.

Iniciemos con computer forensics, cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras: 1. 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; o 2. 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.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de *network forensics*, forensia en redes, estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como

resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Finalmente, *digital forensics*, forensia digital, trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (*¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?*) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Como hemos revisado, las definiciones abordan aspectos generales y específicos que convergen en todos los casos hacia la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de evidencia digital para detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado. No obstante lo anterior, es pertinente anotar que aquellos dedicados a esta disciplina emergente como la informática forense, deben ser profesionales no con altos niveles de ética y respeto por las instituciones, sino con los más altos niveles, pues en ellos está el soporte de las decisiones que sobre los hechos analizados se tomen.

Evidencia digital

De acuerdo con el HB:171 2003 Guidelines for the Management of IT Evidence, la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

En este sentido el documento mencionado establece que la evidencia

digital puede ser dividida en tres categorías a saber:

1. Registros almacenados en el equipo de tecnología informática (P.e. correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.)
2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

- 1.Es volátil
- 2.Es anónima

- 3.Es duplicable
- 4.Es alterable y modificable
- 5.Es eliminable

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

Procedimientos

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 [WILSON 2003, TAYLOR, R., CAETI, T., KALL LOPER, D., FRITSCH, E y LIEDERBACH, J. 2006]. En este sentido

do, detallamos de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado:

1. Esterilidad de los medios informáticos de trabajo

Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

2. Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en

firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. Adicionalmente, es preciso que el software u aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad científica, para que conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

3. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

4. Mantenimiento de la cadena de custodia de las evidencias digitales

Este punto es complemento del anterior. La custodia de todos los ele-

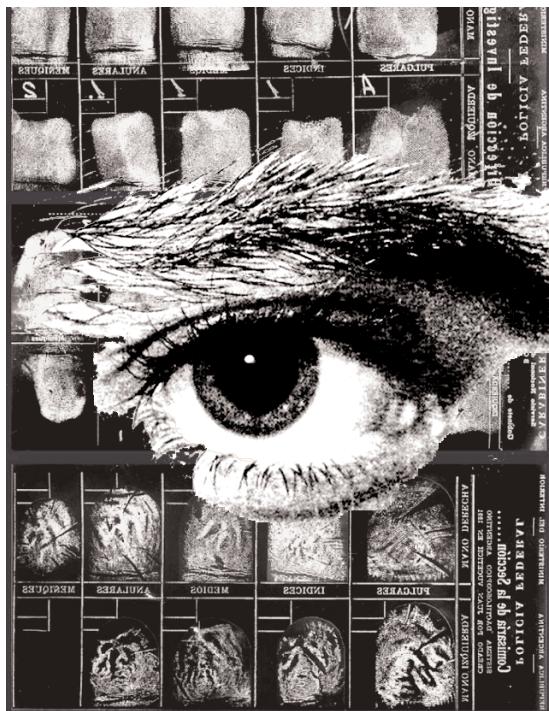
mentos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

5. Informe y presentación de resultados de los análisis de los medios informáticos

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

6. Administración del caso realizado

Los investigadores forenses en informática deben prepararse para



declarar ante un jurado o juicio, por tanto, es probable que en el curso de la investigación o del caso, lo puedan llamar a declarar en ese instante o mucho tiempo después. Por tanto, el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

7. Auditoría de los procedimientos realizados en la investigación

Finalmente y no menos importante, es recomendable que el profesional

investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.

Herramientas

Hablar de informática forense sin revisar algunas ideas sobre herramientas es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en

los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general de los lectores, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática:

ENCASE - http://www.encase.com/products/ef_index.asp

	LICENCIA	IMAGEN	CONTROL INTEGRIDAD	ANÁLISIS	ADMON CASO
ENCASE	si	si	si	si	si
FORENSIC TOOLKIT	si	si	si	si	si
WINHEX (Forensic edition)	si	si	si	si	si

FORENSIC TOOLKIT - <http://www.accessdata.com/products/utk/>
WINHEX - <http://www.x-ways.net/forensics/index-m.html>

Si bien las herramientas detalladas anteriormente son licenciadas y sus

precios oscilan entre los 600 y los 5000 dólares americanos, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código

abierto (entre otras, Sleuth Kit - <http://www.sleuthkit.org/>, Coroner Toolkit

<http://www.porcupine.org/forensics/tct.html>). Estás últimas a pesar de que son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas, vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta en un futuro próximo que éstas estén compitiendo mano a mano con las licenciadas mencionadas anteriormente. Para mayor información de otras herramientas forenses en informática se sugiere revisar el enlace: <http://www.e-evidence.info/vendors.html>.

Retos

La informática forense es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o fraudes en las organizaciones. En este sentido, se tienen agendas de investigación a corto y mediano plazo para que se avancen en temas de especial interés en la conformación y fortalecimiento de las ciencias

forenses aplicadas a los medios informáticos. Dentro de los temas seleccionados están:

1. El reconocimiento de la evidencia digital como evidencia formal y válida

La evidencia digital en la administración de justicia en muchas partes del mundo continua siendo una situación problemática por resolver [BRUNGS, A y JAMIESON, R. 2003]. Dada las características mencionadas previamente, se hace un elemento que requiere un tratamiento especial, más allá de las características legales requeridas, pues éstas deben estar articuladas con los esfuerzos de seguridad de la infor-





mación vigentes en las organizaciones.

2.Los mecanismos y estrategias de validación y confiabilidad de las herramientas forenses en informática

Las herramientas utilizadas actualmente en investigaciones forenses en informática están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos. Sin embargo, la fragilidad inherente del software, la vulnerabilidad presentes en las mismas y las limitaciones propias de los lenguajes y prácticas de programación hacen que la comunidad académica y científica redoble sus esfuerzos para hacer de estos programas, herramientas más confiables y predecibles para los cuerpos de investigaciones judiciales y organizacionales.

3. La formación de especialistas en informática forense, que apoyen

labores de peritaje informático tanto en la administración de justicia como en investigaciones organizacionales internas.

Al ser la informática forense una ciencia aplicada naciente, se hace necesario iniciar las reflexiones sobre la formación de un especialista en informática forense [WHITE, D., REA, A., MCKENZIE, B y GLORFLED, L 2004, CANO 2006]. Esta formación necesariamente deberá ser interdisciplinaria y para ello se requiere el concurso de los profesionales del derecho, la criminalística, las tecnologías de información y la seguridad informática, como mínimo, sin perjuicio de que otras disciplinas académicas puedan estar presentes en la estrategia de profesionalización de estos nuevos especialistas.

A lo largo de este documento hemos querido mostrar de manera básica y concreta una aproximación a la informática forense, no con el ánimo de sugerir un curso de acción sobre el tema, sino de ilustrar los diferentes escenarios y elementos que componen esta naciente disciplina auxiliar de la criminalística. Es preciso aclarar, que los conceptos expresados en este artículo responden a una revisión de la práctica internacional sobre el tema y que el análisis para el caso colombiano requiere aún un estudio particular.

La informática forense es la respuesta natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos) con el fin de enviar un mensaje claro a los intrusos: estamos preparados para responder a sus acciones y continuamos aprendiendo para dar con la verdad de sus acciones.

Referencias

- KSHETRI, N. (2006) *The simple economics of cybercrime*. IEEE Security & Privacy. January/February.
- SUNDT, C. (2006) *Information security and the law*. Information Security Technical Report. Vol.2 No.9
- CANO, J. (2006) *Estado del arte del peritaje informático en Latinoamérica*. Alfa-REDI. Disponible en: <http://www.alfa-redi.org/ar-dnt-docu->mento.shtml?x=728
- TAYLOR, R., CAETI, T., KALL LOPER, D., FRITSCH, E y LIEDERBACH, J. (2006) *Digital crime and digital terrorism*. Pearson Prentice Hall. Cap. 11 y 12.
- WILSON, A. (2003) *Investigation by computer. Digital evidence - data in the box!*. Association of Certified Fraud Examiners. Proceedings of 14th Annual Fraud Conference. Chicago, IL. August.
- BRUNGS, A y JAMIESON, R. (2003) *Legal issues for computer forensics*. Proceedings for 14th Australasian Conference on Information Systems. Perth, Western Australia. November.
- WHITE, D., REA, A., MCKENZIE, B y GLORFLED, L. (2004) *A model and guide for an introductory computer security forensic course*. Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August.
- MCKEMMISH, R. (1999) *What is forensic computing?*. Australian Institute of Criminology. Issues and Trends in crime and criminal justice. No. 118.

Jeimy J. Cano, Ph.D, CFE. Es egresado del Programa de Ingeniería y Maestría en Sistemas y Computación de la Universidad de Los Andes. Cuenta con un doctorado en Filosofía de la Administración de Negocios, título otorgado por Newport University en California, Estados Unidos. Además de una certificación como Examinador Certificado de Fraude - en inglés CFE. Es profesor e investigador a nivel nacional y latinoamericano en temas de seguridad informática, computación forense y sistemas de información. Actualmente, es Presidente de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).