Almacén computacional para evidencias digitales forenses

Sergio Bonilla, Carlos Castillo, Mauricio Rodríguez, Michael Miller, and y Prof. Investigador Randall Barnett Villalobos

Escuela de Ingeniería
Universidad Latinoamericana de Ciencia y Tecnología
ULACIT Urbanización Tournón, 10235-1000
San José, Costa Rica
sergiobo82@gmail.com, carlosnocastillo@gmail.com, mauroal@outlook.com,
miller0406@gmail.com, rbarnettv200@ulacit.ed.cr
http://www.ulacit.ac.cr

Resumen ¿Cómo debería de ser el proceso de implementación técnica necesario para que en Costa Rica se inicie un proyecto de almacén digital de información forense para el resguardo de los datos sensibles vinculados a delitos informáticos
Actualmente se han identificado diferentes escenarios de ataques cibernéticos, en este país, en los cuales queda como resultado distintos delitos informáticos. Ante estas acciones algunos departamentos especializados han aportado sus conocimientos, implementando técnicas forenses para estudiar las escenas de delitos informáticos. Al custodiar estas evidencias como fuentes de investigación, es necesario mantener un almacén forense, que permita el resguardo para este tipo de datos. El principal problema es que no existe un almacén de datos digital el cual permita resguardar y administrar este tipo de evidencia, por lo que se requiere presentar una propuesta basada en el análisis de los requerimientos técnicos implementados en sistemas similares de otros países. De esta manera se busca un nuevo enfoque, aplicado a la realidad nacional.
La creación de un sistema que permita el almacenamiento e indexado de evidencia digital ayuda a centralizar evidencia forense para su posterior análisis. El resguardo de evidencia será la principal función de un repositorio, así como de proporcionar acceso al personal autorizado para subir, resguardar, analizar, compartir y descargar los datos. Parte de la delimitación será enfocarse en aspectos técnicos requeridos para la creación de un almacen digital forense, así como comparar el sistema actual en Costa Rica con sistemas extranjeros, para aplicar en el diseño las mejores prácticas aplicadas a la necesidad del entorno actual.

Keywords: Ataques cibernéticos, delítos informáticos, técnicas forenses, almacén forense, resguardo, evidencia digital forense.

1. Introducción

Comprender la situación problemática que conllevan los delitos informáticos no es tarea fácil, por lo que es necesario profundizar en el estado del arte y ahon-

dar en los procesos que conforman esta actividad. El objetivo principal es brindar en una corte de justicia evidencia verificable, reproducible, independiente e íntegra, con el fin de que sea aceptada como prueba fiable del delíto cometido. Esta evidencia se obtiene mediante el proceso forense digital, el cual engloba mecanismos y métodos especializados para identificar, obtener, presentar y almacenar la evidencia digital.

El problema se enfoqua hacia una inexistencia de un almacén digital para el apoyo a la entidad que regula y da control sobre los delítos informáticos que se desarrollan en Costa Rica. Como elemento adicional, el obstáculo se ve arraigado por la ausencia del punto de una cadena de custodia íntegra y auditada.

Con esta investigación se analizan los datos incautados de una forma exhaustiva, mediante métodos especializados y herramientas forenses, con el fin de obtener resultados completos y confiables para ser presentados en un juicio formal y así alcanzar el desarrollo del concepto de justicia cuando el juez dicte sentencia. Si se obtiene una íntegra cadena de custodia, y un almacenamiento adecuado para analizar la información, se lograrán resultados congruentes para interponer la pena al delito cometido. Según (Del-Pozo; Elford; Pearson, 2009), el producto deseado consiste en "un proceso escalable y semiautomatizado para transferir datos desde soportes físicos a un sistema de almacenaje de preservación digital". Esto se interpreta como el resultado de la aplicación correcta del proceso planteado. los datos incautados de una forma exhaustiva, mediante métodos especializados y herramientas forenses, con el fin de obtener resultados completos y confiables para ser presentados en un juicio formal y así alcanzar el desarrollo del concepto de justicia cuando el juez dicte sentencia. Si se obtiene una íntegra cadena de custodia, y un almacenamiento adecuado para analizar la información, se obtendran resultados congruentes para interponer la pena al delito cometido. Según (Del-Pozo; Elford; Pearson, 2009), el producto deseado consiste en "un proceso escalable y semiautomatizado para transferir datos desde soportes físicos a un sistema de almacenaje de preservación digital". Este se interpreta como el resultado de la aplicación correcta del proceso planteado. Se estudian los requerimientos a nivel técnico, en esta investigación, para la implementación de un almacén digital forense en Costa Rica, gestionando el apoyo al sistema judicial, el cual vela por la seguridad de los datos incautados para resolver casos relacionados con delítos informáticos.

Es importante entender el estado actual del repositorio digital forense en Costa Rica, y establecer una línea base para saber cuáles aspectos deberá abarcar la propuesta. Esta investigación inicia con el analisis de la metodología en la cual se recopilan y procesan las evidencias digitales en Costa Rica, para adaptar los procesos actuales a un entorno de repositorio digital forense, compartido por las autoridades judiciales, manteniendo una base de información que permita una mejor gestión en los casos de investigación a nivel nacional con mínimo tiempo de respuesta.

También se deben analizar los requerimientos técnicos de un repositorio digital forense de otros países tratando de buscar mejores prácticas y los métodos

más utilizados, con el fin de identificar avances que se adapten al entorno nacional.

Una vez recopilada toda esta información se brindará una propuesta de un repositorio digital forense para la comunidad judicial de Costa Rica, aportando las bases para la implementación de un sistema que permita gestionar de forma segura, la evidencia digital forense.

2. Metodología

Para este proyecto se van a realizar investigaciones en distintas bibliografías supervisadas con el fin de obtener información de otras situaciones similares que actualmente se presentan en otros países del mundo, esto nos permitirá entender cómo actualmente otras naciones se enfrentan ante la situación de almacenes digitales forenses.

Adicionalmente se harán entrevistas personales a colaboradores de distintas instituciones de Costa Rica quienes están involucrados directamente con el tema a desarrollar, Una de las instituciones donde se acudió fue el Poder Judicial y sus dependencias, ya que el Organismo de Investigación Judicial es el organismo quien alberga la mayoria de evidencias digitales, debido a que es el autorizado a recopilar información forense digital.Este trabajo investigativo permite conocer sobre la situación actual del país con respecto al manejo que se da en materia de delítos informáticos. Permitirá tener una escena clara de cómo se realizan los procedimientos, proponer sugerencias y mejoras con respecto al Almacén digital forense.

2.1. ¿Qué es el delito Informático?

Los delitos informáticos son todas aquellas acciones fraudulentas realizadas con la utilización de medios electrónicos e informáticos. Para que exista este tipo de delíto, debe haber una víctima y un atacante o amenaza, en donde surja un motivo ya sea económico, diversión o por egocentrismo, que influya para que el atacante realice tal acción. Entre los delítos o acciones fraudulentas se puede mencionar: robo de información confidencial contenida en bases de datos, modificación o alteración de sitios web, robo y clonación de tarjetas de crédito y débito, daño a sistemas informáticos de manera intencional, extorsión a personas por medios cibernéticos, robo de la propiedad intelectual, entre otros.

Una vez que da lugar una acción delictiva, profesionales en la materia llamados Informáticos Forenses, se basan en procedimientos específicos para obtener las evidencias en la escena del incidente. La primera acción que se debe tomar es asegurar el lugar para evitar la contaminación de evidencias, únicamente los especialistas pueden estar en el área del incidente,no es conveniente la presencia de muchas personas trabajando en el mismo lugar porque pueden afectar o alterar evidencias importantes.

2.2. Cadena de Custodia

Una vez que las evidencias hayan sido identificadas y obtenidas con ayuda de herramientas forenses, inicia lo que se conoce como la cadena de custodia, en donde se debe asegurar que la evidencia no sea alterada y mantenga su integridad desde el momento que se obtiene hasta que es presentada en una corte de justicia, pasando luego ya sea a su dueño o a un almacén de evidencias forenses.

2.3. Necesidad de un almacén digital en Costa Rica

La necesidad de implementar un almacén digital el cual aloje específicamente información forense y datos incautados por el Poder Judicial, es inminente, pero surge del problema que poseen las entidades costarricenses en analizar la información recolectada de manera exhaustiva, con el fin de presentar pruebas de peso legal en juicios, que se generan por los delítos informáticos cometidos.

2.4. Definición de almacén (cómo se guarda y maneja esa información y cómo se audita)

El almacén digital consiste en un repositorio de información que centralizará el conjunto de evidencias recolectadas a través del tiempo por el Poder Judicial, estas evidencias están relacionadas con investigaciones de delítos informáticos que ocurren en Costa Rica. La información alojada en el almacén digital debe almacenarse en sectores aislados uno del otro. A esta práctica se le llama utilización de “Sandboxes”, de esta manera se maneja la información y se experimenta con herramientas especializadas de recuperación de datos, lectura de datos, identificación de esteganografía, entre otras técnicas forenses. Las transacciones realizadas en el servidor y almacén dedicado se auditan mediante logs, teniendo detalle de lo que se transfiere y se obtiene en los sectores aislados “Sandboxes”. Por el gran volumen de transacciones en los análisis se implementaran syslogs, en conjunto con log servers.

2.5. Herramientas

Se utilizarán Herramientas que nos permitan desarrollar un almacén digital forense pero a un nivel más básico, sin tener que incurrir en gastos. Se podrían utilizar herramientas gratuitas como generadores de valores Checksum MD5summer para la verificación y comprobación de archivos a la hora de cifrarlos. Es posible inclusive contar con la ayuda de software diseñado con el objetivo de preservar la información o suites de análisis forense.

Como ejemplos se tiene:

- TCT (The Coroner’s ToolKit) Herramienta de IBM gratuita creada por Dan Farmer orientada a UNIX-LINUX creada para asistirnos en análisis forenses y recuperación de datos.

- Autopsy y Sleuth Kit Para Windows y Unix, creado por Brian Carrier. Esta es otra herramienta de análisis forense open source. Utiliza varios métodos de TCT y en conjunto con Autops, logra brindar visualizaciones sobre análisis de archivos, búsquedas por palabras clave y tipos de archivo, ademas de listar MetaData.
- Soluciones técnicas de alto nivel como FTK (Forensics ToolKit). Es creado por AccesData en un esfuerzo por construir una herramienta capaz de abarcar la mayoría de los procesos requeridos en el análisis digital forense, como por ejemplo escaneo de discos duros, también es capaz de descencriptar contraseñas. Trabaja con su propio duplicador de imágenes llamado FTK Imager y calcula su integridad con los valores del hash MD5.
  http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk

En la parte de Hardware existen servidores dedicados que son diseñados con facilidades para la adquisición de información como la duplicación de modo seguro de las imágenes y discos proporcionados. Un ejemplo es FRED, el cual tiene arranque dual de sistemas operativos, software de creación de imágenes de disco como el FTK Imager y Software de análisis forense.

http://www.digitalintelligence.com/products/fred/

3. Marco Legal

Al reflexionar en una propuesta como un almacén digital forense no se puede dejar de lado el marco legal y lo que implicaría el desarrollo de un proyecto así en el futuro. Parte de las entrevistas realizadas nos han permitido saber que no hay ninguna ley determinada que cubra aspectos específicos de un almacén digital forense. Sin embargo habría que revisar las leyes actuales como Ley 9048, Delitos Informáticos y Conexos y la Ley número 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales para poder ir incluyendo nuevos artículos que permitan refundirlos en un almacén digital forense. Es inusual el que no exista nada pertinente a los almacenes, es más bien común que luego de que se implementa tecnología nueva, luego comparezca la parte legal que competa con dichas implementaciones. Nuevamente nos hicieron saber que una herramienta de ese tipo debería ser obtenida por el Organismo de Investigación Judicial, ser la única propietaria y siempre que se necesitase evidencia para su posterior análisis debería de ser obtenida por el Organismo de Investigación Judicial o si es para los fiscales entonces bajo estricta supervisión de O.I.J sería empleada. Por estas razones se incluirá dos requisitos a la hora de presentar la propuesta.

4. Conclusiones

Los requerimientos para la implementación de un almacén forense es un asunto del cual no es fácil obtener información, esto debido a la ausencia de almacenes forenses no solo en Costa Rica sino en otros países. Al ser un tema nuevo

de investigación, se ha tenido que abordar artículos similares en donde se estudiaron necesidades que mantienen una misma orientación. De igual forma se han aplicado conocimientos propios en el área, de acuerdo con casos de estudio anteriores, adicionando elementos esenciales para poder cubrir el objetivo y generar una propuesta razonable y completa. Se ha identificado que el apoyo que se le brindará al sistema judicial con el desarrollo de este proyecto, permitirá una mejora considerable en el estudio de datos incautados, y disminuirá los tiempos procesales de los casos en cuestión.

En cuanto al alcance de la propuesta es importante aclarar que esta va orientada a la sección de delitos informáticos. Debido a que las evidencias digitales no solo provienen de este departamento, es posible gestionar el ambiente del almacén digital para seccionarlo en repositorios y así permitir que cada departamento pueda cargar, mantener, y obtener la evidencia digital, bajo los mismos modelos de seguridad.

Dentro del proceso de entendimiento se logró contactar a varios especialistas e investigadores sobre delitos informáticos ocurridos dentro del país, quienes nos brindaron información importante para entender la posición en la que se encuentra dicha situación y el norte que se debe seguir para alcanzar los objetivos. En estas sesiones se comunicaron y entendieron los departamentos o secciones existentes, además expusieron las principales tareas que realizan cada uno de estos departamentos. Con toda esta información se asegura orientar la propuesta en concordancia con lo que se requiere.

Otro aspecto importante por considerar es la seguridad aplicada a la transferencia de este tipo de archivos, ya que los datos se pueden clasificar como información altamente sensible, la cual debe mantenerse exacta, íntegra y tiene que ser manipulada únicamente por personas autorizadas y profesionales en la materia. Para lograr este objetivo esta investigación se ha enfocado en dos factores, uno es el cifrado del medio, lo que asegura que los datos van protegidos y no podrán ser vistos por personas ajenas, y la otra es la implementación de controles de acceso, los cuales por medio de autenticación, permitirán el ingreso al sistema y el acceso se restringirá a los datos por medio de roles y privilegios.

5. Recomendaciones

Se recomienda, como parte del proceso de aseguramiento de la información y de la seguridad lógica que se debe establecer para lograr la implementación de un repositorio digital de información forense, brindando un nivel adecuado de protección a los datos, y de acceso a los mismos, se recomienda alinearse a los siguientes puntos técnicos para que se logre la satisfactoria implementación de la solución propuesta.

Para facilidad de acceso a los datos almacenados en el repositorio, se recomienda la integración de los servicios por medio de una nube privada, de esta forma, los usuarios podrán acceder a la información cuando se requiera. El concepto de nube privada se enfoca en que los datos se encuentran alojados en un almacén central, este almacén será propiedad de la entidad que regula los pro-

cesos judiciales de Costa Rica, y se conecta con las oficinas descentralizadas a lo largo del territorio nacional.

Si se desea acceder a la información almacenada en la nube, se deberá conectar por medio de una terminal de la Institución, esto se puede llevar a cabo por medio de la implementación de VLANs en la infraestructura de red. Como medida de seguridad, será obligación, asegurar el método utilizado para realizar la conexión al repositorio digital, aplicando cifrado, con ayuda de certificados digitales de confianza, emitidos por entidades certificadoras a nivel mundial, además de proteger la conexión por medio de comunicación tunelizada, es decir, aplicación de VPNs. Este equipo deberá estar bajo vigilancia constante, es decir, monitoreado las 24 horas del día, por medio de un circuito cerrado de televisión y un oficial de seguridad. Para entrar y salir del recinto donde se encuentra el equipo, se deberá firmar una bitácora.

El hardware que se implemente para albergar la información proveniente de las investigaciones criminales, debe ser dedicado, única y exclusivamente, para cumplir con el objetivo de mantener y resguardar los datos, así como permitir el acceso a los mismos por medio de mecanismos [1] seguros, anteriormente descritos.

Referencias

Adam Bates Kevin Butler, M. S. W. Z., Andreas Haeberlen. (2004, feb). Let sdn be your eyes: Secure forensics in data center networks. *Internet Society*(ISBN 1-891562-36-3), 1-7. pages 8

A. Patrascu, V. P. (2015, apr). Logging for cloud computing forensic systems. *International Journal of Computer Communications & Control*, *ISSN 1841-9836*(10(2):222-229), 1-9. pages 8

Barbara Kitchenham a, O. P. B. a. D. B. b. M. T. a. J. B. b. S. L. a., *. (2009, jul). Systematic literature reviews in software engineering – a systematic literature review. *Information and Software Technology*, *51*(7–15), 1-9. pages 8

Farid Daryabar, N. I. U. N. F. b. M. S. S. b. S. F. N., Ali Dehghantanha. (2013, aug). A survey on cloud computing and digital forensics. *Journal of Next Generation Information Technology(JNIT)*, *Volume4,*(Number6,), 1-13. pages 8

G. Sibiya, T. F., H. Venter. (2012). Digital forensic framework for a cloud environment. *Proceedings of the 2012 Africa Conference*, 1-8. pages 8

Marty, R. (2011). Cloud application logging for forensics. *Proceedings of the 2011 ACM Symposium on Applied Computing*, 178-184. pages 8

Pascale, M. (2007). Manual de peritaje informatico. *Fundación de Cultura Universitaria.*. pages 8

Pino, D. S. A. D. (2009). Introducción a la informática forense. *Direccion Nacional de Tecnologías de la Información de la Fiscalía General del Estado.*. pages 8

[1] Situacion tecnica para hacer algo

Roberto Hernandez Sampieri, P. B. L., Carlos Fernandez Collado. (2010). Metodologia de la investigacion. *McGrawHill*, *quinta Edicion*(ISBN: 978-607-15-0291-9), Cap 4. pages 8

S. Zawoad, A. D., y Hasan, R. (2013). Seclaas: Secure logging-as-a-service for cloud forensics. *ACM Symposium on Information, Computer and Communications Security*, *DOI: 10.1145*(2484313.2484342), 219-230. pages 8

(Farid Daryabar, 2013) (Pino, 2009) (Adam Bates Kevin Butler, 2004) (A. Patrascu, 2015) (Pascale, 2007) (Roberto Hernandez Sampieri, 2010) (Barbara Kitchenham a, 2009) (Marty, 2011) (G. Sibiya, 2012) (S. Zawoad y Hasan, 2013)

Glosario

almacén digital Es la utilización de componentes digitales como memorias, discos duros, entre otros, para almacenar información intangible. 1

almacén forense Lugar donde se guardan pruebas relacionadas con delítos. 1

ataques cibernéticos Es un intento intencionado utilizando tecnologías para causar daños a un sistema informático o red. 1

bases de datos Ees un "almacén" que nos permite guardar información de forma organizada para que luego podamos encontrar y utilizar fácilmente. 3

cadena de custodia Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. 2

certificados digitales de confianza Es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. 7

cifrado Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos. 7

datos incautados Datos tomado en posesión por la autoridad competente. 2

delitos informáticos Son acciones fraudulentas realizadas por medios electrónicos e informáticos. 1

esteganografía Es una técnica que permite entregar mensajes camuflados dentro de un objeto (contenedor), de forma que no se detecte su presencia y pasen inadvertidos. 4

información forense Información que está asociada a un hecho delictivo. 1

nube privada Es un tipo de modelo de implementación para el cómputo en la nube donde los recursos de TI (aplicaciones, cómputo, almacenamiento y redes) los proporciona como servicio el mismo departamento de TI de la organización. 6

repositorio Es equivalete a un almacén. 2

VLANs Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. 7