CienciAmérica (2017) V0l. 6 (3)
ISSN 1390-9592

Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador

Model for the forensic analysis and the legalization of atypical digital evidence in judicial processes in Ecuador

Juan Sebastián Grijalva Lima y By-ron Loarte Cajamarca
Universidad Internacional SEK Ecuador. Correo: sebastian.grijalva@uisek.edu.ec

Fecha de recepción:1 de mayo de 2017
Fecha de aceptación: 12 de agosto de 2017

Resumen

El crecimiento exponencial de las Tecnologías de la Información ha permitido ser una herramienta más para el cometimiento de diversos delitos informáticos.

La información almacenada digitalmente pasa a tener mayor relevancia como evidencia en un procedimiento penal o civil derivando en Pericias Informáticas muy específicas y complicadas en la obtención de la evidencia.

Una de las mayores problemáticas es la falta de un proceso que guie a los Peritos Informáticos en la aplicación de técnicas, métodos y buenas prácticas asegurando que realizaron todas las tareas encomendadas con los mecanismos adecuados enmarcados en la normativa legal vigente.

Palabras clave: Informática Forense, Modelo Forense, Análisis Forense, Investigación Digital.

Abstract

The exponential growth of Information Technology has allowed it to be an additional tool for the commission of various computer crimes.

The digitally stored information becomes more relevant as evidence in a criminal or civil proceeding deriving in very specific and complicated Informative Experiences in obtaining the evidence.

One of the major problems is the lack of a process that guides IT experts in the application of techniques, methods and good practices, ensuring that they performed all tasks in accordance with the appropriate mechanisms within the current legal regulations.

Key words: Computer Forensics, Forensics Model, Forensic Analysis, Digital Research.

1. Introducción

La Pericia Informática en equipos tecnológicos, de procesamiento electrónico o en un medio computacional es uno de los servicios que habitualmente se ofrece en el ámbito de la actividad profesional de un Perito Informático.

El Perito Informático es el responsable de recoger y preservar la evidencia digital, aplicando la normativa legal, técnicas, herramientas, entre otras, que el considere las más apropiadas sustentadas de manera técnica y científica.

Qué sucede cuando la evidencia debe ser recolectada desde dispositivos no habituales es decir desde un computador o un celular y en cambio nos encontramos con interfaces atípicas como lo podrían ser sistemas operativos de drones o evidencia digital de interfaces ápticas o de realidad aumentada.

2. Método

2.1 Tipo de Proyecto

El presente proyecto tiene como principal objetivo el solucionar un problema de la comunidad de investigadores forenses quienes se ven en la necesidad de aplicar su criterio durante el proceso de análisis de evidencia digital y dichos vacíos dan lugar a la confrontación respecto a la validez de la evidencia, así como del proceso de adquisición y preservación de la misma.

Por lo antes expuesto se puede definir al presente como un proyecto de investigación tecnológica.

2.2 Tipo de Estudio Realizado

Según el análisis y alcance de los resultados serán descriptivos, analíticos y experimentales.

Descriptivos: Un estudio descriptivo es un tipo de metodología a aplicar para deducir una circunstancia describiendo todas sus dimensiones, en este caso se describe los componentes del modelo pro-puesto.

Analíticos: Un estudio analítico etiológico es un estudio en el que el análisis del estudio se establecen relaciones entre las variables, de asociación o de causalidad.

Experimentales: La investigación experimental es un tipo de investigación que bien utiliza experimentos y los principios encontrados en el método científico. Los experimentos serán llevados a cabo en el laboratorio que se creará para dicho cometido.

2.3 Universo y Muestra

Se realizará una segmentación del universo de acuerdo a las líneas de estudio forense.

Durante el proceso de experimentación se plantea que se realicen estudios de aplicación en dos peritos acreditados por el Consejo de la Judicatura de Ecuador en el ámbito de la Informática.

2.4 Métodos

Métodos Empíricos

Observación

Se pretende a través de la observación de la utilización del modelo propuesto, identificar las características que los experimentadores reflejan sobre la utilización del mismo.

Medición

Se llevará un estadístico de los hitos encontrados durante los diferentes análisis aplicativos para poder definir o ajustar el modelo con la adhesión de nuevos procesos vinculantes.

Experimentación

Se plantea dividir a las personas objeto de la investigación en dos o más grupos. Los dos grupos reciben tratamientos idénticos, excepto que se le entrega a un grupo y no a los otros el modelo propuesto.

Métodos Teóricos

Análisis y síntesis

Mediante el análisis de los contenidos de las diferentes características que componen los procedimientos se deberá sintetizar los mismos de forma efectiva para prevenir redundancia de información e inclusión de información irrelevante.

Inducción y deducción

A partir de las premisas que se obtengan del análisis legal se deberá concluir el objetivo de cada procedimiento increpando a que el mismo sea considerado, evidente y demostrable durante la documentación del mismo.

Hipotético-deductivo.

Ciertos análisis deberán partir también de teorías de otros autores respecto a los aspectos que no hayan sido planteados en la lógica debido a la falta de premisas.

Análisis histórico y el lógico

Al ser una ciencia evolutiva, se deberá entender que la aplicación de nuevas tecnologías en el análisis y experimentación pueden llevar a que se realice un análisis de cuál es el ciclo en el que se encuentre la tecnología a analizarse sin dejar de lado la parte histórica ya que no se puede definir con claridad si el modelo deberá soportar análisis de tecnología anterior.

2.5 Recursos del proyecto

Recursos humanos: Investigador de tesis Doctoral, Tres tesistas del programa de Maestría en Tecnologías de la Información.

Bienes y equipos: Laboratorio de Investigación Forense

Servicios: Digitado, fotocopiado, inter-net

Fuentes de financiamiento personales.

3. Resultados

En la actualidad con el uso de las Tecnologías de la Información pasamos de un modelo de economía donde la principal riqueza se encontraba en los bienes tangibles, a una economía donde la riqueza está dada por el acceso a la información. Información que es de vital importancia en el desarrollo de la vida cotidiana y laboral.

Hoy en día, más y más personas utilizan computadoras y medios de comunicación por ejemplo (teléfonos móviles, correo electrónico e internet) que inadvertidamente colocan una gran cantidad de información y realizan transacciones en repositorios informáticos y sitios web que fácilmente podrían ser violentados y/o vulnerados con diferentes tipos de ataques como: fraudes financieros en la web, infección con malware, ataques de denegación de servicio (DoS), phishing, entre otros, debido a esto las computadoras y las redes de comunicación se han convertido en la principal herramienta para el cometimiento de un delito informático [1].

Cabe mencionar que las organizaciones sufren frecuentemente ataques de diversos tipos a sus sistemas de información, por ejemplo: Kaspersky Lab, en su portal web Secuelist ofrece información actualizada y completa sobre aquellas amenazas de Internet que están activas, una de sus publicaciones “Desarrollo de las amenazas informáticas en el tercer trimestre de 2016” [2] expone los programas maliciosos en Internet y los principales ataques mediante la web.

Ofreciendo estadísticas trimestrales del año 2016 en base a los incidentes de seguridad de múltiples organizaciones alrededor del mundo. Pero no solo organizaciones como la banca, comercio y entidades del Estado, entre otros sectores, se ven afectados por este tipo de delitos informáticos, si no que un número considerable de ciudadanos comunes también se ven afectos por estos incidentes.

Se han identificado varios Modelos propuestos por distintas organizaciones que están estructurados típicamente sin considerar las resoluciones y legislación de los distintos países.

--Modelo según la Norma UNE 71506:2013, de AENOR .[3]

--Modelo según Francisco Lázaro Domínguez en su libro introducción a la Informática Forense [4]

--Modelo según el NIST , en su Special Publication 800-86 [5]

--Modelo según DFRWS (2001), en su informe técnico que lleva por título A Road Map for Digital Forensic Research [6]

--Modelo según IDIP (2003), propuesto por Carrier y Spafford [7]

Todas estas metodologías tienen sus fases bien diferenciadas reflejando en cada una de ellas los mismos principios básicos. Por ello cualquiera de estas metodologías es aplicable a un análisis forense, sin embargo, se puede escoger entre una de ellas dependiendo de las necesidades que se requiera, ya que algunas tienden a ser muy generales y otras más específicas.

Para el desarrollo del presente marco de trabajo, se aplica la metodología propuesta por la UNE 71506:2013. Ya que es bastante completa para el manejo de evidencia digital, no obstante, será complementado con la particularidad propia del uso de interfaces hápticas y entornos virtuales para garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación del informe.

Según la metodología propuesta se debe realizar en esta fase de adquisición un clonado a bajo nivel de los datos originales del soporte de almacenamiento de datos, para lo cual se tomará de guía el RFC 3227 (Directrices para la recopilación de evidencias y su almacenamiento) [8], son directrices que contienen las mejores prácticas relacionado durante la recolección de evidencia y su almacenamiento.

Por lo mencionado anteriormente se elaboraron sub-fases enmarcadas en la evidencia original.

Se debe garantizar la cadena de custodia, Para la elaboración de estos métodos se tomará de guía estándares para el manejo y almacenamiento de la evidencia digital como son: el RFC 3227[13], ISO 27370[14], Modelo Extendido de Séamus Ó Ciardhuain.

1. Fase de Preservación

a. Sub-fase de reconocimiento

b. Sub-fase de autorización

c. Sub-fase de identificación

1) Llevar indumentaria adecuada para evitar descargas electrostáticas.

2) Evitar contaminarla con software que no garantice un proceso limpio.

3) Alejar a todas las personas no autorizadas de la escena.

4) Mantener el estado de los dispositivos si están encendidos, no apagarlo y viceversa.

5) Identificar los equipos afectados, que pueden ser equipos informáticos o a su vez dispositivos de almacenamiento.

6) Realizar una evaluación de las herramientas de software, hardware y procedimientos que se van a utilizar sobre el equipo afectado a analizar.

7) Asegurar que todo el proceso que se realice en esta sub-fase debe ser claramente documentado.

2. Fase de Adquisición

a. Sub-fase de recopilación

Equipo Apagado

Procedimiento por Software

Procedimiento por Hardware

Equipo encendido

Registros y contenidos de la caché.

Contenidos de la memoria.

Estado de las conexiones de red, tablas de rutas.

Estado de los procesos en ejecución.

Contenido del sistema de archivos y de los discos duros.

Contenido de otros dispositivos de almacenamiento.

Información del sistema en tiempo real como:

Fecha y hora.

Procesos activos.

Conexiones de red.

Puertos TCP/UDP abiertos.

Usuarios conectados remota y localmente.

b. Sub-fase de almacenamiento

La cadena de custodia debe realizarse de la siguiente manera:

Manejo del lugar de los hechos

Fijación del lugar de los hechos

Recolección de la evidencia

Embalaje y rotulado de la evidencias

Transporte de la evidencia

Abrir el embalaje de la evidencia

3. Fase de Análisis

•Realizar la reconstrucción de la línea de tiempo

•Llevar a cabo un examen detallado de los sistemas de archivos

Análisis de una imagen forense

- Recuperación de archivos eliminados
- Firmas características
- Documentos
- Archivos gráficos
- Multimedia
- Archivos ejecutables
- Data carving
- Análisis de sistema operativo
- Fecha y hora del sistema
- Conexiones de red abiertas
- Puertos TCP o UDP abiertos
- Usuarios conectados al sistema
- Tabla de enrutamiento interna
- Procesos en ejecución
- Archivos abiertos
- Papelera de reciclaje
- Historial de Internet
- Correo electrónico
- Búsqueda de caracteres
- Metadatos
- Registro de SO

4. Fase de Presentación

Informes Periciales

Entregables que acompañan al Informe

5. Fase de Defensa

La defensa oral del informe

- Forma de vestir
- Revisar otras experticias en el caso de haberlas.
- Actitud
- Lenguaje
- Preguntas e Interrogatorio
- Conclusiones

4. Discusión

Se ha elaborado un marco de trabajo estandarizado para el análisis forense de la evidencia digital en equipos tecnológicos tomando como puntos importantes las acciones más relevantes de las buenas prácticas, normas y estándares internacionales para que los Peritos Informáticos acreditados tomen en cuenta al momento de realizar una investigación forense.

El contar con un marco de trabajo estandarizado garantizará la admisibilidad de la evidencia de manera contundente en un procedimiento Penal o Civil.

En el Ecuador no todos los delitos informáticos son sancionados por lo que es indispensable desarrollar y establecer mecanismos para el análisis forense, permitiendo que estas se desarrollen dentro de marcos regulados y controlados.

Se espera que este modelo sirva de referencia debido a la creciente demanda de diversos delitos informáticos, el uso y difusión puede ser el punto de partida para que este marco de trabajo siga adquiriendo relevancia y fortaleciéndose.

5. Referencias

[1] Mónica Uyana, Milton Escobar, "PROPUESTA DE DISEÑO DE UN ÁREA INFORMÁTICA FORENSE PARA UN EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD INFORMÁTICOS (CSIRT)". Disponible: http://repositorio.espe.edu.ec:8080/bitstream/21000/8123/1/AC-GSR-ESPE-047639.pdf

[2] SecureList, "Desarrollo de las amenazas informáticas en el tercer trimestre de 2016. Estadística" 2016. Disponible: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/84164/it-threat-evolution-q3-2016-statistics/

[3] Ledy Zúñiga Rocha "Código Orgánico Integral Penal", Ministerio de Justicia, Derechos Humanos y Cultos, vol. 1, ISBN: 978-9942-07-592-5, 2014.

[4] Gustavo Jalkh R. "Código Orgánico General de Procesos" Ministerio de Judicatura, Disponible: http://www.funcionjudicial.gob.ec/index.php/es/normativa/codigo-organico-general-de-procesos.html

[5] Fernando Cordero Cueva "CONSTITUCIÓN DEL ECUADOR" Asamblea Constituyente, 2008, Disponible: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

[6] Gustavo Jalkl Roben "Resolución 067-2016" Ministerio de Judicatura, 2016, Disponible: http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/067-2016.pdf

[7] Gustavo Jalkl Roben "Resolución 040-2014" Ministerio de Judicatura, 2014, Disponible: http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2014cj/040-2014.pdf

[8] AENOR "La Asociación Española de Normalización y Certificación", 2016, Disponible: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.WKHjgDvhAdV

[9] Francisco Lazaro Dominguez, "INTRODUCCION A LA INFORMÁTICA FORENSE", RA-MA, ISBN: 9788499642093, 2015.

[10] Karen Kent, "Guide to Integrating Forensic Techniques into Incident Response", 2006, Disponible:

http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875

[11] Collective work of all DFRWS attendees, “A Road Map for Digital Forensic Research”, 2001, Disponible: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

[12] Carrier y Spafford, “GETTING PHYSICAL WITH THE DIGITAL INVESTIGATION PROCESS”, 2003, Disponible: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf

[13] RFC 3227 “Guidelines for Evidence Collection and Archiving” RFC-Base.org, 2002, Disponible: http://www.rfc-base.org/rfc-3227.html

[14] Azas Marlon, ISO 27370 “Diseño de un Modelo para la cadena de custodia y herramientas para el análisis forense de quipos tecnológicos en procesos judiciales en el Ecuador”, Universidad Internacional SEK, 2015.

[15] Brian Carrier “File System Forensic Analysys”, Adisson Wesley Professional, ISBN: 0-32-126817-2, Disponible: http://www.campus64.com/digital_learning/data/cyber_forensics_essentials/info_file_system_forensic_analysis.pdf

[16] Jonathan Zdziarski “ZDZIARSKI'S BLOG OF THINGS”, 2017, Disponible: https://www.zdziarski.com/blog/?cat=11

[17] Rick Ayers, “Guidelines on Mobile Device Forensics”,2014, Disponible: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[19] Dan Haagman, “Good Practice Guide for Computer-Based Electronic Evidence”,1996, Disponible: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[20] SWGDE Best Practices for Mobile Phone Forensics, “cientific Working Group on Digital Evidence”, versión 2.0, 2013, Disponible: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics

[21] Dan Haagman, “Good Practice Guide for Computer-Based Electronic Evidence”,1996, Disponible: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[22] Juan Miguel Tocados, “Metodologìa para el desarrollo de procedimientos periciales en el ambito de la informtica forense”,Trabajo de Fin de Grado, 2015, Disponible: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/6667/TFG_Juan_Miguel_Tocados.pdf?sequence=1&isAllowed=y

[23] Francisco Lazaro Dominguez, “INFORMÁTICA FORENSE”, RA-MA, ISBN: 978-958-762-113-6, 2013.

[24] Pereyra, Damián; Eterovic, Jorge, “Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto”, Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/43214/Documento_completo.pdf?sequence=1

[25] Leopoldo Sebastián Gómez, “Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados”,2015, Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/55345/Documento_completo.pdf-PDFA.pdf?sequence=1

6. Autores

Juan S. Grijalva Nació en Quito, el 7 de mayo de 1983, actualmente es estudiante de PHD en ciencias Informáticas en la Universidad Nacional de La Plata Argentina, tiene una Maestría en Evaluación y Auditoría de Sistemas Tecnológicos en la Universidad de las Fuerzas Armadas, es Ingeniero en Informática en la Universidad Tecnológica América y es Psicofisiólogo Forense en la Academia Tudor.

Byron Loarte Egresado de la Carrera de Ingeniería en Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional.

Se desempeña como docente en la Facultad de Ciencias de la Escuela Politécnica Nacional.

Sus líneas de interés son: Desarrollo de Software, Seguridad de la Información.