LOG DE EVENTOS COMO FUENTES DE EVIDENCIA DIGITAL Y SU TRATAMIENTO EN NETWORK FORENSICS

Andrés Casanova MSc, CFC

Auditor de Sistemas Deposito Central de Valores (Deceval)

Jcasanova@deceval.com.co

Las opiniones aquí expresadas son responsabilidad exclusiva del autor y no comprometen al Deceval S.A..

LA EVIDENCIA DIGITAL

Se puede decir que el término “Evidencia Digital” abarca cualquier información en formato digital sujeta a intervención humana que pueda establecer una relación entre un delito y su autor, otros autores la describen como “cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado en un proceso legal”. Desde el punto de vista del derecho probatorio, puede ser comparable con un documento como prueba legal, que sirve para llevar a convencimiento a un juez o fiscal.

EL NETWORK FORENSICS

El network forensics, cubre un escenario más profundo y complejo que el cómputo forense , ya que igualmente que en el cómputo forense busca identificar evidencia legal, pero en este escenario se requiere el uso de técnicas científicamente probadas y orientadas hacia elementos de conexión en redes y telecomunicaciones, lo que implica protocolos de conexión (fundamentado en la familia de protocolos TCP/IP para redes en Internet), configuraciones de elementos de red y correlación de eventos para equipos particulares. Por lo tanto, el network forensics se constituye como una rama importante en ciencias forenses que complementa y fortalece toda investigación de evidencia digital, puesto que exige que el peritaje contemple la comprensión de operaciones de redes, siguiendo protocolos y la formación criminalística que permita establecer rastros y/o movimientos de posibles intrusos o atacantes

FUENTES DE DATOS DE LA EVIDENCIA

Se considera que parte de la evidencia puede quedar registrada en las trazas en los elementos intermedios en la comunicación entre los dos puntas (lado atacante – lado victima).

De los lados del atacante o la victima	Log de Auditorias del sistema operativo
	Log de eventos del sistema operativo
	Log de eventos de aplicaciones
	File MAC
	File Swap (registros en memoria virtual)
De los elementos intermediarios en la comunicación	Paquetes y trafico TCP
	Logs de firewall
	Logs de IDS
	Logs de routers

LOS LOGS COMO MATERIA PRIMA

Los logs se constituyen en trazas que registran todas las actividades sobre un determinado elemento de cómputo. Estas trazas permiten detectar intentos hostiles que pueden comprometer la seguridad de un sistema. La configuración, recolección y custodia de los logs [4] se constituyen en elementos fundamentales de evidencia digital.

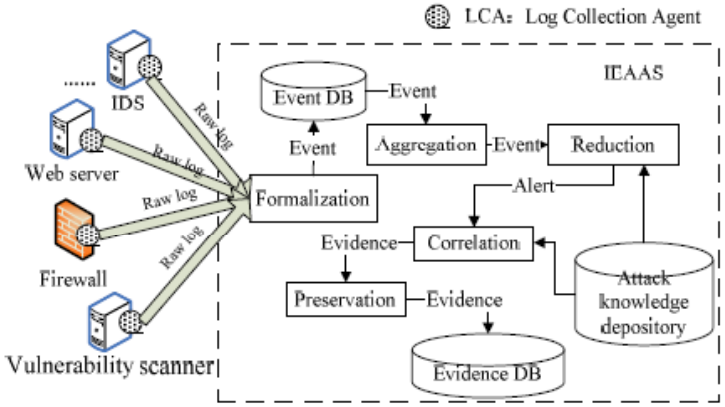
Todos logs de auditoría de los diferentes componentes de una red contienen información suficiente que conduzca a resultados puntuales luego de un riguroso análisis; sin embargo, los logs por su naturaleza y volumen pueden llegar a ser dispendiosos en su tratamiento y/o análisis, dependiendo de la cantidad, calidad y seguridad

De la manera como se centralicen, normalicen, sincronicen, custodien, transporten y aseguren las trazas de auditoría registradas en los logs, dependerá la validad de la evidencia Digital

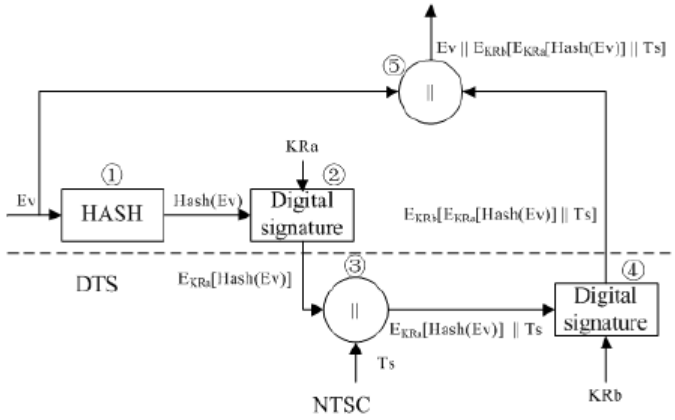
LINEAMIENTOS DE CONFIGURACION DE LOGS

- Sincronizar los elementos de cómputo con horario centralizado u horario local. Para Colombia es el horario de la SIC (Superintendencia de Industria y Comercio)
- Identificar fechas y horas de activación de los logs
- Verificar opciones de no sobreescritura de los archivos de log
- Verificar que los registros armen una traza completa y legible (que se pueda interpretar)
- Verificar que las trazas no sean alterables desde un aplicativo externo
- Verificar los niveles adecuados de seguridad del almacenamiento de la base de trazas
- Verificar los niveles de encripción adecuados de los registros
- Verificar la inclusión de los niveles de seguridad necesarios en el almacenamiento seguro de los archivos tipo log tales como firmas digitales y timestamp

GARANTIZANDO LA SEGURIDAD EN EL TRANSPORTE Y LA CONSOLIDACION



Framework of IEAAS

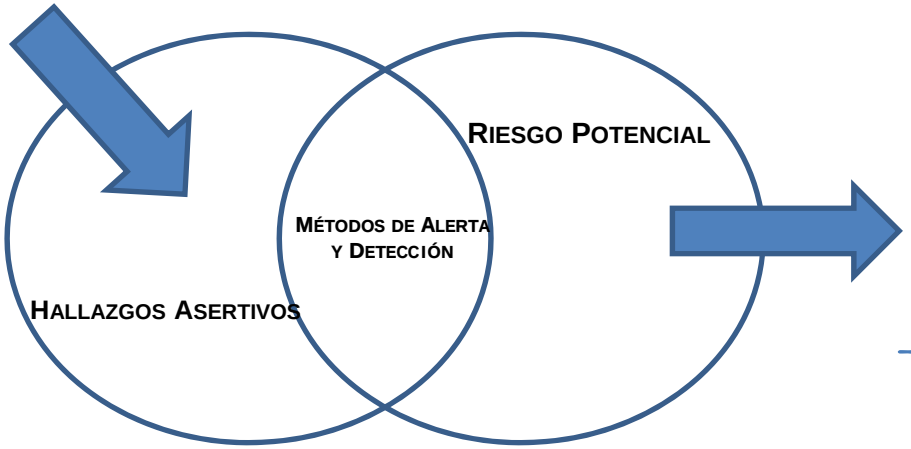


Preservation of intrusion evidence

CORRELACIÓN DE REGISTROS DE EVENTOS

La correlación de eventos es el proceso mediante el cual se busca asociar los eventos para encontrar información útil con el fin de llegar a una conclusión asertiva sobre un hecho en particular. Se emplean técnicas matemáticas tales como:

- Algoritmos de Reducción
- Minería de Datos
- Redes Neuronales

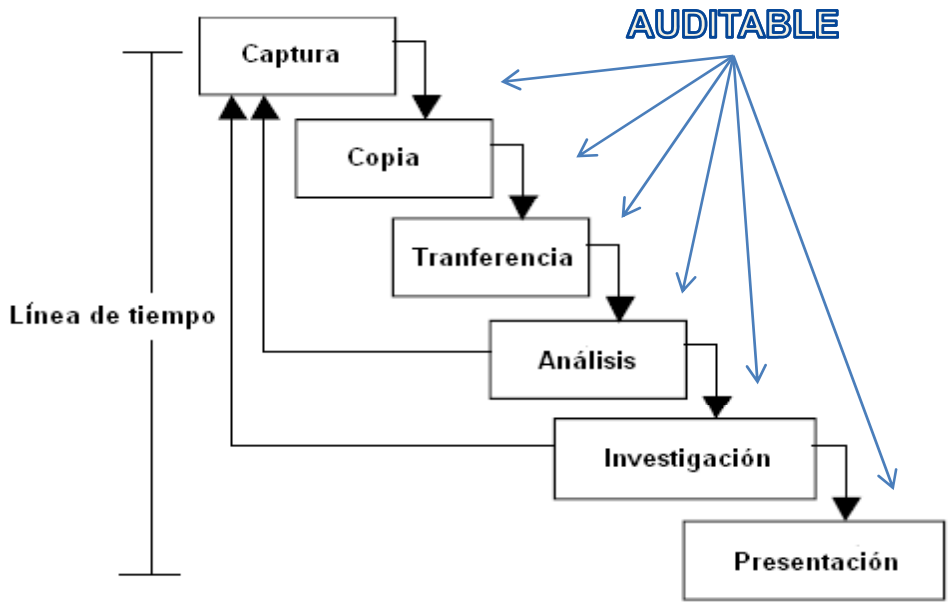


PREDICCIÓN DE RIESGO

- **ANÁLISIS DE FRECUENCIAS**
- **REDES BAYESIANAS**
- **DIAGRAMAS DE INFLUENCIAS**

FORMALIZACION DEL PROCESO EN NETWORK FORENSICS

En general el proceso de Network Forensics incluye 5 pasos, los cuales se describen a continuación:



Todos los pasos deben cumplir con una rigurosa documentación por parte del perito informático, conservando una estricta línea de tiempo. La línea de tiempo permite ver la evolución de los eventos y de los hechos en un paso a paso con fechas precisas.

CONCLUSIONES

- Cada país cuenta con sus propios conceptos y/o legislaciones jurídicas las cuales reglamentan la validez y suficiencia de la evidencia digital, en consecuencia, todos los equipos y/o grupos de investigación a nivel nacional en materia de peritaje informático deben estar alineados a la legislación
- De la rigurosidad con que se capture, recolecte, custodie, evalué y presente la evidencia digital en un proceso legal, dependerá la emisión asertiva de un fallo por parte de un juez. Esta rigurosidad, está específicamente ligada a la metodología, los procedimientos y a la evaluación de la evidencia
- Los logs de los diferentes componentes de una red, deben ser configurados con ciertas características que permitan ser recolectados con prácticas seguras, las cuales incluyen rutas seguras y algoritmos de encripción de registros así como el uso de firmas digitales y de timestamp que garanticen la inalterabilidad de la evidencia
- Todas la técnicas empleadas por el perito experto informático, deben cumplir con los requerimientos necesarios para mantener el carácter de evidencia digital de los registros de eventos en los diferentes elementos que componen una red

REFERENCIAS

[1] Chen Lin, Li Zhitang, Gao Cuixia, Automated Analysis of Multi-source Logs for Network Forensics. 978-0-7695-3557-9/09 © 2009 IEEE

[2] Jorge Herrerías, Roberto Gómez. Log Analysis towards an Automated Forensic Diagnosis System. 978-0-7695-3965-2/10 © 2010 IEEE. 2010.

[3] Jeimy Cano M. Computación Forensics. Ed Alfaomega 2009. ISBN 978-958-682-767-6

[4] Jeimy Cano M. Peritaje informático y la evidencia digital en Colombia. Editorial Universidad de los Andes 2010. ISBN 978-958-695-492-1

[5] Nattn Nisimblat. El manejo de la prueba electrónica en el proceso civil colombiano. Universidad de los Andes 2010. ISS 1909-7786

[6] Lin Chen, Zhitang Li, Cuixia Gao. Dynamic Forensics based on Intrusion Tolerance. 978-0-7695-3747-4/09 © 2009 IEEE

[7] Wei Ren, Hai Jin. Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design. 1550-445X/05 © 2005 IEEE

[8] Grant Osborne, Benjamin Turnbull. Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation. 978-0-7695-3564-7/09 © 2009 IEEE

[9] Lin Chen, Zhitang Li, Cuixia Gao, Yingshu Liu. Modeling and Analyzing Dynamic Forensics System based on Intrusion Tolerance. 978-0-7695-3836-5/09 © 2009 IEEE

[10] Wei Ren, Hai Jin. Modeling the Network Forensics Behaviors. 0-7803-9469-0/05/ ©2005 IEEE

[11] Ahmad Almulhem. Network Forensics: Notions and Challenges. 978-1-4244-5950-6/09/ ©2009 IEEE

[12] Grant Osborne, Benjamin Turnbull, Jill Slay. The 'Explore, Investigate and Correlate' (EIC) conceptual framework for digital forensics Information Visualisation. 978-0-7695-3965-2/10 © 2010 IEEE

[13] Guidance, "EnCase forensic." [Online]. Available: http://www.guidancesoftware.com

[14] AccessData, "FTK forensic toolkit." [Online]. Available: http://www.accessdata.com

[15] Niksun, "NetDetector." [Online]. Available: http://www.niksun.com

[16] CA, "etrust." [Online]. Available: http://www.ca.com