Análisis Comparativo De Herramientas Forenses Informáticas Para La Realización De Peritajes En Medios Digitales

Iván Mesias Hidalgo-Cajo
Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes
Docente Escuela Superior Politécnica de Chimborazo, Ecuador
Saul Yasaca-Pucuna
Magíster en Informática Educativa
Técnico Docente Escuela Superior Politécnica de Chimborazo, Ecuador
Byron Geovanny Hidalgo-Cajo
Máster Universitario en Ingeniería Computacional y Matemática
Docente Universidad Nacional de Chimborazo
Docente Escuela Superior Politécnica de Chimborazo, Ecuador
Keylee Alexandra Cevallos-Paredes
Máster Universitario Europeo en Alimentación, Nutrición y Metabolismo
Docente Escuela Superior Politécnica de Chimborazo, Ecuador
Diego Patricio Hidalgo-Cajo
Magíster en Educación Matemática
Docente Ministerio de Educación, Ecuador
Víctor Manuel Oquendo-Coronado
Ingeniero en Sistemas Informáticos
Docente Ministerio de Educación, Ecuador

Doi:10.19044/esj.2018.v14n34p80 URL:http://dx.doi.org/10.19044/esj.2018.v14n34p80

Abstract

This paper focuses on making a comparison of the different computer forensic tools used in the performance of data surveys in digital media. The research was developed based on the method of weighting by criteria (scientific and descriptive study). In this study, specifically four computer forensic tools were used and evaluated by six criteria for the selection of them, and they were chosen based on ISO 9126:1998. Based on the comparison, the results of the four computer forensic tools were analyzed. It was determined that for the different criteria (Case study: Clone of 500 Gb hard disk in off mode), the HD Clone and XWay Forensics tools obtained 84.62% of acceptability, compared to Norton Ghost that obtained a contribution of

69.23% and the tool EnCase with a score of 58.46% to obtain the cloning of the disks. In addition, with the use of ISO 9126: 1998, greater portability, reliability of the results, acquisition cost of the tool, ease of use and application, greater operational capacity and support for the tool was achieved in the cloning of digital media. This is attributed to the fact that it is composed of six evaluation criteria as mentioned above.

Keywords: Forensic tools, surveys, digital media

Resumen

El objetivo de la investigación es comparar las diferentes herramientas forenses informáticas utilizadas en la realización de peritajes de datos en medios digitales. La investigación se desarrolló basándose en el método de ponderación por criterios, científico y descriptivo, donde se utilizaron específicamente cuatro herramientas forenses informáticas evaluadas por seis criterios para la selección de estas, criterios escogidos en base a la Norma ISO 9126:1998. Entre los resultados de comparación de las cuatro herramientas forenses informáticas analizadas se determinó que, para los diferentes criterios (Caso práctico: Clonación de disco duro de 500 Gb en modo apagado), las herramientas *HD Clone* y *XWay Forensics* obtuvieron un 84,62% de aceptabilidad, frente a *Norton Ghost* que obtuvo un aporte de 69,23% y la herramienta *EnCase* con un puntaje de 58,46% para la obtención de la clonación de discos. Además, con la aplicación de la Norma ISO 9126:1998, se logró tener mayor portabilidad, confiabilidad de los resultados, costo de adquisición de la herramienta, facilidad de uso y aplicación, mayor capacidad operativa y soporte para la herramienta en la clonación de medios digitales, ya que está compuesta de seis criterios de evaluación como se menciona anteriormente.

Palabras Clave: Herramientas forenses, peritajes, medios digitales

INTRODUCCIÓN

El rápido avance registrado en el área de las tecnologías de información y comunicación ha permitido un desarrollo en las diferentes actividades realizadas por los distintos sectores que conforman la sociedad, pero al mismo tiempo se puede acceder a las puertas del uso fraudulento de las computadoras con el fin de la realización de actividades ilícitas. De esta forma la informática se ha convertido en el objeto o medio para cometer delitos (Ayala Vásquez, Cortez Argueta, Guidos Juárez, & Ruiz Sánchez, 2010).

En la adquisición de la evidencia se debe garantizar la autenticidad y la originalidad de la misma, además de evitar que sufra alteraciones o daños. En esta fase de análisis es muyimportante el proceso legal de la informática

forense, debido a que se mantiene la integridad de la evidencia obtenida que se establece en la cadena de custodia (Hidalgo Cajo, 2014).

En vista de lo expuesto anteriormente, este trabajo busca determinar las diferentes herramientas y equipos necesarios para llevar a cabo la investigación forense en un entorno de trabajo adecuado.

1.1 Justificación/Problema

Las herramientas de análisis forense informático que se utilizan en la Informática Forense pueden ser diversas e independientes del sistema operativo donde se desarrollan las diferentes actividades que realizarán los investigadores informáticos forenses. Así se tiene que la evidencia digital necesita ser recolectada por herramientas forenses informáticas especializadas, y su calidad depende de la contundencia de esta en un proceso legal. Por tal motivo, es necesario que las herramientas sean las correctas y que su aplicación sea la adecuada. Con este estudio, pretendemos conocer el nivel de uso que se les da a las herramientas de informática forense para poder hacer propuestas que permitan que la evidencia digital recolectada sea altamente confiable y que esto permita resolver casos de delitos informáticos más ágil y eficientemente.

1.2 Revisión de la literatura

La adquisición de información de discos significa copiar de una manera especial el contenido en bruto de la información del sistema en observación. Luego se trabajará sobre esta copia dejando intacta la información original (Gervilla Rivas, 2014).

La adquisición se realiza no arrancando la computadora por los medios convencionales sino accediendo a los volúmenes en modo de solo lectura para que ni un byte sea alterado desde el momento en que empieza nuestra intervención. Hay que tener en cuenta que el simple booteo (arranque) de una computadora altera por lo menos algunos archivos en sus contenidos y fechas, varía la cantidad total de archivos, etc. Lo mismo ocurre cuando abrimos un archivo aunque más no sea para leerlo o imprimirlo. Se puede rastrear todo este tipo de actividad en una computadora. La adquisición puede involucrar desde un disquette o un disco rígido de una computadora hasta un conjunto de discos de un servidor, un juego de cintas, o varias computadoras de una organización (CompExcell, 2010).

1. Dispositivo Modo Encendido o modo "*live*"

En esta situación se aplicará el siguiente axioma "Si esta encendido no apagarlo y si está apagado no encenderlo" (Cornejo, 2015). Una vez clarificada esta acción, se procederá a tomar las siguientes evidencias (a grandes rasgos y no importa el orden).

- Volcado de la memoria RAM
- Obtención del archivo pagefile.sys
- Obtención del NTUSER.DAT
- Prefetch
- Procesos, sesiones, conexiones, tareas, políticas, configuración de red, protocolos...
- Ficheros del registro (SAM, SECURITY, SOFTWARE...)
- Ficheros de logs de windows, etc.

Las herramientas que se utilizarán no podrán ser intrusivas ni llevar instalación (es preferible que sean portables) y normalmente se dispondrá de un disco duro externo con dos particiones, una de ellas con los programas y la otra para volcar los resultados.

Una vez obtenida la información se hala del cable de alimentación apagando el equipo de forma abrupta y nunca se hará de forma ordenada ya que puede haber algún programa o proceso que elimine información precisa y necesaria. Si se trata de un portátil sólo se retirará la batería.

2. Equipo Modo Apagado

Esto se entiende como equipo muerto o modo *"sleep*". Extraer el disco duro y clonarlo resulta el modo más recomendado. Aunque de esta forma se pierde todo lo que contenía la memoria RAM, en el fichero de paginación. Sin embargo, se puede lograr el acceso a todo lo que estaba en el disco (López-Delgado, 2007).

3. Virtualización

Es el modo más recomendable. Actualmente muchas empresas tienen todo virtualizado vía web porque les resulta más cómodo, por lo tanto, se puede clonar la máquina y la memoria RAM. De esta forma se admiten los modos encendido y apagado (Arzola Rodríguez, 2015).

4. Equipo Modo "NUBE"

Es conocido como modo *Cloud* es el más complicado y difícil, porque para acceder a una información de una empresa que está en la nube se tiene que hacer con orden judicial. Si se tiene un incidente con una empresa se le pide a Google que retire los datos y se le entrega la información sobre por qué y en dónde está la orden judicial. Por ejemplo, Amazon cuenta con una herramienta para hacer clonados en dependencia de la compañía o institución que lo requiera. A veces, como en el caso de Google, sólo se proporcionan datos específicos y no el clonado exacto porque es imposible implementar un servidor dedicado a cada persona o empresa. Una base de datos distribuida en cien mil ordenadores ayuda a proporcionar los datos necesarios, pero no a

clonar las máquinas. Como consecuencia, se pierde mucha información. Para Microsoft, por orden judicial, normalmente se proporciona una herramienta pagada con anterioridad en función de ejecutar el clonado. Por lo tanto, se infiere que Google es el más afectado porque en otros casos como Amazon y Microsoft, pueden usar herramientas que no son baratas, pero al menos pueden contar con ellas (Sánchez Cordero, 2014).

La clonación de discos es el proceso de copiar los contenidos de un disco duro de una computadora a otro disco o a un archivo imagen (Pato Rodríguez, 2006). A menudo, los contenidos del primer disco se escriben en un archivo imagen como un paso intermedio y, como paso posterior, el disco de destino es cargado con el contenido de la imagen. El procedimiento también es útil para cambiar a un disco diferente o para restaurar el disco a un estado previo (Sánchez Cordero, Análisis Forense Informático, 2015).

1.3 Propósito

1. Comparar las diferentes herramientas forenses informáticas utilizadas para la copia de medios digitales.

2. MÉTODO

Tipos de investigación

Investigación documental: Consultas en diversas fuentes de investigación como son: bases de datos digitales, libros, revistas, manuales, internet, entre otros**.**

Método

Criterios Ponderados: Sirven para realizar un análisis cuantitativo o cualitativo en el que se compararán entre sí las diferentes alternativas. El método permite ponderar factores de preferencia para el investigador al tomar la decisión. Se sugiere aplicar el siguiente procedimiento para jerarquizar los factores cualitativos.

Científico: Es un estudio sistemático, lógico y organizado de la proposición hipotética planteada para adquirir conocimientos y brindar una solución.

Descriptivo: Se realizó un estudio descriptivo que consiste en llevar a conocer situaciones relevantes a través de la descripción de las variables de investigación para exponer de manera cuidadosa los resultados a fin de extraer generalizaciones significativas.

2.1 Instrumentos y materiales

2. Microsoft Office Excel 2016
3. Sistema Operativo (Windows)
4. Herramientas Forense Informático

5. Computador
6. Norma ISO 9126:1998

2.2 Procedimiento

El primer paso fue la selección de las herramientas de software a ser estudiadas. Para la realización de la selección de herramientas, se estudió el libro *Herramientas para copias de datos bit a bit,* en el cual se indica que el copiado bit a bit consiste en realizar una copia íntegra de un medio o dispositivo completamente para trabajar sobre una copia que posee las mismas características que la original.

Posteriormente, para estas cuatro herramientas se realizó la selección final para tener como objetivo identificar las que serían estudiadas en la presente investigación. Para la realización de la selección se tomaron en cuenta los siguientes criterios presentados en la Tabla 1.:

Tabla 1. *Criterios de selección de herramientas para informática forense*

No.	NOMBRE	DESCRIPCIÓN
1	Utilidad	Fin con el que se utiliza la herramienta en la Informática Forense.
2	Adaptabilidad	No necesita complementos para instalarse o utilizarse en los equipos.
3	Mantenimiento	Se estudiarán herramientas que cuenten con actualizaciones permanentes, ya que la evolución de la informática es constante.
4	Portabilidad	No es necesaria su instalación sobre el sistema operativo o puede ejecutarse en diferentes plataformas de hardware.
5	Accesibilidad	Que esté disponible su obtención para el respectivo estudio.
6	Documentación	Se estudiarán herramientas de las que exista documentación suficiente para obtener la información necesaria.
7	Estabilidad	Robustez de la aplicación en cuanto a operatividad en la plataforma que vaya a ser utilizada.

En base a la matriz de los criterios procedemos a la siguiente selección de herramientas forenses informáticas a selecionar:

Las herramientas para copias de datos bit a bit seleccionadas son:

- HD Clone
- EnCase
- Norton Ghost
- XWay Forensics

3. Resultados

La propuesta de herramientas forenses informáticas se basará en la jerarquización de las herramientas estudiadas y analizadas de la siguiente manera:

1. Definir con qué criterios se medirán las herramientas que necesitamos comparar.

2. Para todas las herramientas forenses informáticas seleccionadas, medir el nivel de desempeño de cada criterio.
3. Realizar la compararación de cada herramienta forense para determinar cuáles son las que obtienen mejores puntuaciones en los criterios definidos anteriormente, para lo cual se utilizará la tabla de criterios (Tabla 1). Las puntuaciones se obtendrán de acuerdo al criterio seleccionado.
4. Establecer la jerarquía de propuestas ordenadas descendentemente.

3.1. Los criterios a tomar en cuenta para la comparación de las herramientas serán:

1. **Portabilidad:** Capacidad de la herramienta para ser utilizada tanto en un entorno de hardware y software determinado como en otro, conservando la funcionalidad de esta. Se refiere al nivel en que la misma herramienta puede ser utilizada en los diferentes entornos (combinaciones de hardware y software) donde se pueda encontrar la evidencia. Este criterio también incluye la facilidad de instalación con que las herramientas puedan instalarse en los entornos en los que puede funcionar.
2. **Confiabilidad de los resultados:** Para que una herramienta sea confiable en los resultados que proporciona, es necesario comparar el resultado de ésta con el de las otras herramientas del mismo tipo y, si son similares, se podrá tomar como confiable, pero si no, se considerará no confiable. Por ejemplo, con las herramientas Hash, el resultado de cálculo del mismo tipo de hash al mismo archivo debe dar igual para todas las herramientas.
3. **Costo de adquisición de la herramienta:** Algunas de las herramientas seleccionadas pueden tener un costo que puede ser significativo. Por supuesto, sí existen herramientas que realicen la misma funcionalidad, pero el costo de adquisición es menor o nulo. Esta sería una alternativa viable comparada con la de costo mayor.
4. **Facilidad de uso y aplicación:** Facilidad con que la herramienta puede ser aplicada para obtener el fin de esta. Esta facilidad de uso está relacionada al nivel de entendimiento del programa y su funcionabilidad, la facilidad de control y uso por parte del usuario y el esfuerzo necesario para aprender a utilizarla. En esto intervienen criterios como la interfaz del programa y la forma en que esta va guiando al usuario a través del proceso de ejecución de las operaciones para que las que las herramientas fueron diseñadas y la ayuda en pantalla.
5. **Mayor capacidad operativa:** Este criterio se refiere a que, si dos herramientas realizan la misma función, se debe seleccionar la

herramienta que tenga mayor capacidad para realizar dicha función. Por ejemplo, seleccionar la herramienta que haga copias de bit a bit pero que pueda trabajar con discos de mayor tamaño.

6. **Soporte para la herramienta:** Es necesario que las herramientas seleccionadas tengan soporte para solventar problemas que puedan surgir con esta y las actualizaciones que los fabricantes ponen a disposición para asegurar el correcto funcionamiento de la herramienta.

Las características a evaluar en el método utilizado para ponderar las herramientas forenses informáticas está basado en el método de criterios ponderados. Mediante este método, se definen los criterios que las herramientas deben cumplir y se le asigna un puntaje de acuerdo al peso del factor. El peso del factor depende de la importancia del mismo.

Los criterios y subcriterios tomados en cuenta y su respectiva ponderación son:

1. Adaptabilidad al entorno: (15pts)

A. No requiere de sistema operativo (10pts).

B. Requiere de sistema operativo, pero funciona sobre más de uno (5pts).

C. Soporta más de una arquitectura de computadora (5pts).

El primero y el segundo criterio son excluyentes, si una herramienta cumple con el primero, no puede cumplir con el segundo y viceversa.

2. Confiabilidad de resultados: (15pts).

A. Los resultados son iguales a los anteriores (15pts).

3. Costo de adquisición de la herramienta: (5pts).

A. No existe costo para la herramienta (5pts).

4. Facilidad de uso y aplicación (10pts).

A. Tiene interfaz gráfica amigable (5pts).

B. Presenta ayuda en pantalla (5pts).

5. Capacidad operativa (15pts).

A. Soporta lo más común del hardware en el mercado (8pts).

B. Tiene soporte para elementos de hardware especiales o puede operar sobre ellos (7pts).

6. Soporte para la herramienta (5pts).

A. Tiene desarrollo y actualizaciones constantes de las herramientas (5pts).

Los criterios de comparación fueron elegidos en base a la Norma ISO 9126:1998, la cual define los criterios y subcriterios que debe tener un software para ser considerado de calidad. La norma está orientada al desarrollo de software, para lo cual se considerará en la jerarquización de las herramientas de informática forense analizadas (Tabla 2).

Tabla 2. *Comparación de herramientas para copia de medios*

HERRAMIENTAS PARA COPIA DE MEDIOS										
HERRAMIENTAS	**CRITERIO 1**			**CRITERIO 2**	**CRITERIO 3**	**CRITERIO 4**		**CRITERIO 5**		**CRITERIO 6**
	A	**B**	**C**	**A**	**A**	**A**	**B**	**A**	**B**	**A**
HD Clone	Si	No	No	Si	Si	Si	Si	Si	Si	Si
EnCase	No	No	No	Si	Si	Si	Si	Si	No	Si
Norton Ghost	No	No	No	Si	Si	Si	Si	Si	Si	Si
XWay Forensics	Si	No	No	Si	No	Si	No	Si	Si	Si

Las ponderaciones dadas a cada uno de los criterios y subcriterios fueron definidas por el grupo de investigación, basados en las investigaciones realizadas por profesionales que utilizan las herramientas forenses informáticas. El máximo puntaje que una herramienta puede alcanzar será de 65, que es la sumatoria total (Tabla 3).

Tabla 3. *Puntuaciones de herramientas para copia de medios*

HERRAMIENTAS PARA COPIA DE MEDIOS (PUNTAJES)								
HERRAMIENTA	**CRITERIOS**						**TOTAL**	
	1	**2**	**3**	**4**	**5**	**6**	**Cant. / 65**	**%**
HD Clone	10	15	0	10	15	5	55	84,62
EnCase	0	15	0	10	8	5	38	58,46
Norton Ghost	0	15	0	10	15	5	45	69,23
XWay Forensics	10	15	5	5	15	5	55	84,62

Las puntuaciones de herramientas según ponderaciones de criterios presentan los puntajes obtenidos para cada herramienta, recordando que el criterio de puntuación está basado en el método de los factores ponderados (Figura 1).

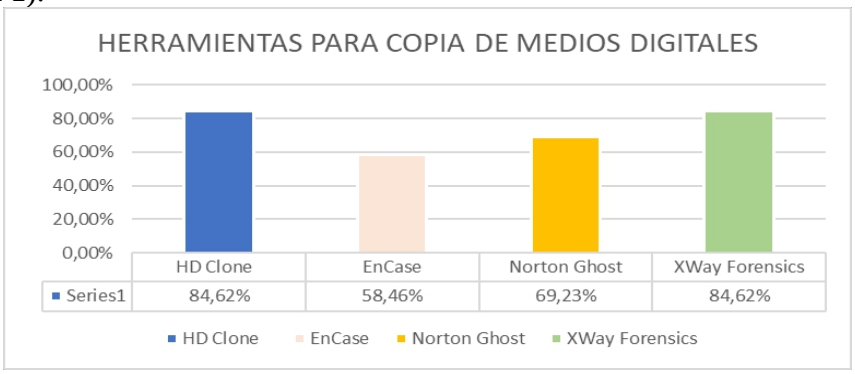

Figura 1. *Representación gráfica de las ponderaciones de herramientas forenses informáticas para copia de medios digitales.*

Conclusión

- En Ecuador no existe un marco legal que tipifique los delitos informáticos y apoye su persecución por parte de las autoridades y que a su vez soporte la validez de la evidencia digital en este tipo de casos.
- Al usar las diferentes herramientas forenses se añade al proceso de copia de medios digitales un alto grado de eficiencia, confiabilidad y seguridad que contribuye a dar una mayor veracidad a los resultados obtenidos en un peritaje informático.
- En la comparación de las diferentes herramientas forenses informáticas analizadas se determinó que, para los diferentes criterios de ponderación, las herramientas HD Clone y XWay Forensics alcanzaron un 84,62% de aceptabilidad, frente a Norton Ghost que obtuvo un aporte de 69,23% y la herramienta EnCase un puntaje de 58,46% para la obtención de la clonación de discos.
- Gracias a la aplicación de la Norma ISO 9126:1998, se definieron los seis criterios de evaluación de las herramientas: tener mayor portabilidad, confiabilidad de los resultados, costo de adquisición de la herramienta, facilidad de uso y aplicación, mejora la capacidad operativa y soporte para la herramienta en la clonación de medios digitales.

References:

1. Arzola Rodríguez, O. (2015). *Virtualización de la Red UCLV.* Santa Clara.
2. Ayala Vásquez, R. E., Cortez Argueta, E. A., Guidos Juárez, J. C., & Ruiz Sánchez, C. D. (2010). *INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE.* Universitaria.
3. CompExcell. (2010). *Informática Forense*. Obtenido de http://www.informaticaforense.com.ar/procedimientos.htm
4. Cornejo, M. A. (2015). *Seguridad Informática 365*. Obtenido de http://bellapadula.blogspot.com/2015/05/adquisicion-de-evidencias.html
5. Gervilla Rivas, C. (2014). *Metodología para un Análisis Forense.* Barcelona.
6. Hidalgo Cajo, I.M. (2014). *Análisis preliminar y Diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Forense Informático.* Tarragona.
7. López-Delgado, M. (Junio de 2007). *Análisis Forense Digital*. Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

8. Pato Rodríguez, A. (2006). *Metodología para realizar el manejo de incidentes de seguridad de TI mediante actividades de forénsica digital*. Caracas.
9. Sánchez Cordero, P. (Enero de 2014). *Conexión Inversa*. Obtenido de http://conexioninversa.blogspot.com/2014/01/artefactos-forenses-ii-prefetch-y.html
10. Sánchez Cordero, P. (2015). *Análisis Forense Informático.* Barcelona.