Evaluación de herramientas de software libre, para el sistema operativo Windows, en la adquisición de evidencias de la memoria RAM

Evaluation of free software tools, for the Windows operating system, in the acquisition of RAM memory evidences

Henry Gutiérrez-Oquendo

Universidad Nacional Abierta y a Distancia —UNAD—.

Recibido: 15/12/2021 Aprobado: 10/02/2022

Resumen

El objetivo de este artículo, es evaluar herramientas de software libre del sistema operativo Windows, para la adquisición de evidencias de la memoria RAM, mediante la norma ISO/IEC 25010 que define características y medidas de calidad de uso de un producto. Lo anterior toma en consideración la forma técnica para el análisis del volcado de memoria RAM y el empleo de las herramientas específicas DumpIt, FTK Imager, Windows Forensic Toolchest (WFT), OS Forensic y RamCapturer. Con el fin de garantizar la utilidad de las herramientas seleccionadas, se contempla el definir, clasificar, identificar, obtener, analizar e interpretar resultados obtenidos con la herramienta Volatility, y así poder detectar que instrumentos recupera más, el más eficiente que afecte menos la evidencia. Esto último es de suma importancia, ya que una alteración muy sutil podría cambiar el HASH obteniendo problemas de gran escala en un juicio.

Palabras clave: adquisición de evidencias, evaluación de herramientas, evidencias de la memoria RAM.

Abstract

The objective of this article, is to evaluate free software tools of the Windows operating system, for the acquisition of evidence of RAM memory, using the ISO/IEC 25010 standard that defines characteristics and measures of quality of use of a product. The above takes into consideration the technical form for RAM dump analysis and the use of the specific tools DumpIt, FTK Imager, Windows Forensic Toolchest (WFT), OS Forensic and RamCapturer. In order to guarantee the usefulness of the selected tools, it is contemplated to define, classify, identify, obtain, analyze and interpret results obtained with the Volatility tool, and thus be able to detect which instrument recovers more, the most efficient one that affects the evidence less. The latter is of utmost importance, since a very subtle alteration could change the HASH obtaining large scale problems in a trial.

Key words: : Evidence acquisition, evaluation tools, RAM evidence.

Citación: Gutiérrez Oquendo, H. (2022). Evaluación de herramientas de software libre, para el sistema operativo Windows, en la adquisición de evidencias de la memoria RAM. Publicaciones E Investigación, 16(1). https://doi.org/10.22490/25394088.5567

[1] Escuela de Ciencias Básicas Tecnología e Ingeniería —ECBTI—. Santiago de Chile. https://orcid.org/0000-0002-8300-2014 / Bafim1420@gmail.com

https://doi.10.22490/25394088.5567

1. Introducción

La informática forense investiga delitos relacionados con el cómputo, desde sabotaje, fraude a través de computadoras, estafa electrónica, entre otras. Esto hace dispensable para el investigador forense digital, hacer referencia a un conjunto de procedimientos de recopilación y análisis de evidencias, que se realizan con el fin de responder a un incidente relacionado con la seguridad informática y que, deben de servir como pruebas ante un tribunal: "La fuerza probatoria no se manifiesta hasta que intervienen las personas que hallaron la evidencia o aquellas que han de explicarlas en relación con los hechos a juzgar" (Lázaro Domínguez, 2014, p. 44).

Para este fin, definimos y clasificamos herramientas de software libre, del sistema operativo Windows; igualmente relacionamos técnicas y estrategias de recolección de la información mediante las etapas de investigación forense, (Lázaro Domínguez, 2014, pp. 37-40). Siguiendo el orden, y en relación con el tratamiento de evidencia digital, es bueno hacer énfasis en la ISO/IEC 27037, 2012, (Rafael_L_R, 2019), que indica sobre la aplicación de métodos para adquirir la evidencia digital, procesos reproducibles y defendibles de la evidencia (identificación, recolección y/o adquisición, la conservación/preservación). Con el fin de establecer un ambiente óptimo para la adquisición, se modeló una escena de crimen, en la que cada proceso de volcado de memoria sea eficaz. También, adaptamos la familia de normas (ISO 25000, 2021), que establecen las bases de medidas (métricas de calidad de uso y calidad del producto, [2011]) con el propósito de establecer un juicio de orden que permite dar probatoria de evaluación de las herramientas escogidas para la adquisición de la memoria RAM. Por último, describimos los resultados de forma específica para cada herramienta seleccionada, y para este fin utilizamos el software de análisis forense Volatility; todo esto con el único propósito de establecer nuestra verdad de la evaluación de herramientas de software libre, para el sistema operativo Windows, en la adquisición de evidencias de la memoria RAM, mediante la ISO/IEC 25010.

2. Método2.1 Contexto

2.1.1. Dominio de aplicación de la informática forense digital

El crecimiento en las últimas décadas de la informática forense, hace uso extendido por diversos campos como lo resalta (Incibe, 2021), con el único fin de abordar temas de seguridad como lo son: ingeniería social, phishing, ransomware, actualizaciones, entre otras. En efecto, aborda dos finalidades, como lo son, la probatoria y la auditoría; la primera permite adquirir evidencias y la segunda, conlleva a tomar medidas correctivas frente a hechos vulnerados, dando sentido a la investigación, análisis e interpretaciones de hechos relacionados con dispositivos electrónicos, que posiblemente un juez requiera en su hecho probatorio de juicio (Incibe, 2015, párr. 18).

Un claro ejemplo del uso extendido de la informática forense digital es la agencia federal, como líder en la investigación de ciberataques e intrusiones, "La actividad cibernética maliciosa amenaza la seguridad del público y nuestra seguridad nacional y económica. La estrategia cibernética del FBI es imponer riesgos y consecuencias a los adversarios cibernéticos" (Oficina Federal de Investigaciones [FBI], 2021, párr. 1).

En la probatoria, se establecen unas fases para el tratamiento de la evidencia, que si bien en muchos libros las describen en diferente orden, ya que no son rígidas, es importante precisar una interacción entre ellas, como bien lo indica el Incibe "Respecto al conjunto de fases hay que tener presente que no son secuenciales sino, que están entrelazadas entre sí" (2015); para atender actos delictivos que conllevan al análisis de exactitud de las evidencias para contribuir a un proceso de tipificación de delito.

Frente a estas dos finalidades de la informática forense digital, se crea una necesidad imperante, del experto en su labor, saber que software considera a través de su investigación de pericia, como bien lo señalan Granados & Buitrago, "Por lo tanto, es importante seleccionar la herramienta correcta y hacer buen uso de ella, con el fin de lograr mejores evidencias para el

análisis forense" (2013, p. 32) y es donde pretendemos aportar con esta investigación, para que el perito informático tenga una herramienta de software libre y del sistema operativo Windows, definida en su kit de investigación que le garantice la autenticación, credibilidad, confiabilidad y admisibilidad a la evidencia adquirida.

En suma, es brindar una capacitación a la problemática del crecimiento exponencial de la tecnología de la información que problematizan la falta de procesos que guíen al experto en la aplicación de técnicas, métodos y buenas prácticas, como bien lo indican Lima & Cajamarca (2017). En resumen, el perito informático debe actualizarse día a día, estar a la par de los avances tecnológicos (herramientas), para detectar vectores de ataque y poder establecer controles de análisis y seguridad en los procesos de investigación.

2.1.2. Problemas que enfrenta la informática forense digital.

Los avances tecnológicos marcan pauta en esta sociedad de consumo, como lo dirían Granados & Buitrago "el avance tecnológico se ha incrementado drásticamente, lo cual ha provocado una migración acelerada de información física a digital en la mayoría de las organizaciones o empresas del mundo" (2013, p. 32). Esta migración requiere conocimientos específicos y problematiza la labor de experto a la hora de adquirir evidencias en la nube con entornos remotos y virtualizados, que por lo general son alojados y administrados por terceros, "el uso de la computación en la nube presenta desafíos significativos para los usuarios de las nubes (tanto individuos como organizaciones), así como para las autoridades reguladoras y de aplicación de la ley" (Grispos et al., 2012, párr. 4).

2.2. Descripción del experimento.

Con respecto a la evaluación de herramientas de software libre, para el sistema operativo Windows en la adquisición de evidencia de la memoria RAM; conviene subrayar, que NAXHACK5 (2016) publicó, como adquirir evidencias de la memoria RAM con las herramientas DumpIt y FTK Imager y empleó la herramienta Volatility para su posterior análisis; importante resaltar que no aplicó métricas de evaluación para declinar u/o elegir por una de las dos herramientas evaluadas, caso contrario a esta investigación que se elaboran métricas de calidad de uso y calidad del producto.

Por otra parte, Quintana & Medina (2018), en su TFM, evaluaron herramientas de extracción de información, solo de malware por medio de un ordenador de escritorio del sistema operativo Windows 7, de 64 bits y memoria RAM de 4 GB; obviando tiempo de almacenamiento, complejidad de uso, métrica, control de calidad, métrica de desempeño, métrica de eficiencia; que nosotros abordamos en esta investigación.

2.2.1. Definición y clasificación de herramientas.

Es importante resaltar, que la elección de las herramientas se llevó a cabo mediante la designación de los siguientes conceptos:

- Fácil acceder a la descarga: el portal de descarga de la herramienta es accesible.
- Capacidad de descarga mínima: esto significa que no se requiere de gran capacidad de disco para almacenarla.
- No requiere registro en la página: varias herramientas de la lista anterior, exigen registrase en la página de descarga.
- No requiere validar el correo electrónico: varias herramientas enlistadas, requieren registras el correo electrónico para recibir la aprobación de descarga.
- Efectividad de descarga: algunas herramientas como WindowsScope, Memoryze winPEM, no cumplieron con la efectividad de la descarga.
- Herramientas solo de análisis de memoria RAM.
- Herramientas solo de sistema operativo Windows.

Así mismo, se valoraron 49 programas de código abierto que garantizaban el objetivo por parte del sitio web; de estos, se evidencia en la Figura 1, que el 61,2% son del sistema operativo Windows, para un total de 30 software seleccionados; 14,2% para Mac OS, con un total de siete herramientas y aproximadamente 25% del sistema operativo Linux con un total de 12 programas.

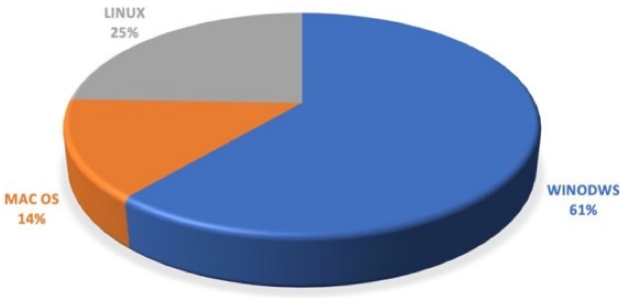

Fig. 1. Herramientas de análisis forense digital.

En la Tabla 1, se muestra las herramientas que se validaron para esta profundización.

Tabla 1.
Herramientas de software libre solo para el sistema operativo Windows

Herramienta validada	Sitio web
DumpIt	(Soft32, 2022)
FTL Imager	(ACCESSDATA, 2022)
Windows Forensic Toolchest (WFT)	(McDougal, 2017)
OSForensic	(Software PASSMARK, 2021)
RamCapturer	(Belkasoft, 2022)

2.2.2. Escena del crimen

Con el fin de establecer un ambiente óptimo para la adquisición, se modeló una escena de crimen, en la que cada proceso de volcado de memoria sea eficaz; lo anterior indica, que se abrieron los mismos archivos, se conectó el mismo pendrive, se ejecutaron los dos navegadores y se navegó por las mismas páginas web en cada volcado de memoria. Conviene subrayar, que se verificaron con anterioridad las características del computador de la escena del crimen, estas son:

- Sistema operativo: Windows 7 Profesional.
- Service Pack 1.
- Fabricante: Luffi.
- Procesador: Intel(R) Core (TM)2 Duo CPU E7500 ©2,93GHz 2,94GHz.
- Memoria instalada (RAM): 4GH (3,47 GB utilizable).
- Tipo de sistema: Sistema operativo 64 bits.
- Nombre de equipo: WIN-CI4GDFQS59B.
- Grupo de trabajo: WORKGROUP.

En este orden de ideas, seguimos las directrices de Brezinski & Killallea, (2002) para el proceso de toma de evidencia volátil, como se indica en la Figura 2.

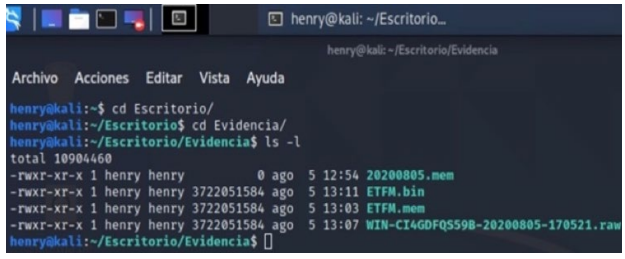

Fig. 2. Dump de memoria RAM.

2.2.3. Diseño de métricas de evaluación herramientas de software libre para la adquisición de evidencia digital

En este punto, queremos resaltar que no es sencillo medir la calidad de una herramienta de extracción de la memoria RAM, tampoco se encuentran muchos documentos que faciliten este proceso de comparación de medida; uno de los pocos contenidos encontrados de métricas en el análisis forense, es en Granados & Buitrago (2013), que realizaron una comparación de las herramientas workMiner y Wireshark y establecieron las métricas de eficiencia, facilidad de uso y relación costo-efectividad, en la conducción del análisis forense en redes de forma particular.

En particular, tuvimos en cuenta las medidas de las normas (ISO-IEC 9126-2 "Métricas Externas" - Instituto Politécnico Nacional, 2003, pp. 30-33), (ISO/CEI TR 9126-3, 2003) e (ISO/IEC TR 9126-4, 2004) (normas de la serie ISO 9000, 2015)) que fueron canceladas y remplazadas por la primera edición (ISO/CEI 25022, 2016), que es parte de la serie de normas SQuaRE (System and Software Quality Requirements and Evaluation), También conocida como la (ISO 25000, 2021), que más que una métrica de medida, es una norma vigente para evaluar la calidad de un producto, como resaltan Echavarría-Flórez & Restrepo-Calle (2020).

Conviene subrayar tres puntos importantes en esta investigación. El primero, no es fácil establecer una medida para la extracción de contenido en la memoria RAM; segundo, no es solo aplicar esta norma a los resultados obtenidos que depende de la naturaleza de las operaciones establecidas para cuantificar el atributo, subjetivo u objetivo del investigador y tercero, las métricas diseñadas, para casos específicos son directas (su medida no depende de ningún otro atributo) y para medidas complejas, son indirectas (su atributo se deriva de una o más métricas de medida).

En relación con esto, nos enfocamos en la normas ISO 25000, 2021 que hace referencia a la medición de calidad del producto, atendiendo a las medidas de calidad (interna, externa y en uso) y guías prácticas para su aplicación, (ISO/IEC 25010, 2011) para elaborar métricas de calidad de uso y calidad de producto, siguiendo las pautas mostradas en el diseño de la Tabla 2. Se elaboraron siete métricas que hacen referencia a la efectividad de adquisición; eficacia e integridad funcional; eficiencia y comportamiento de tiempo; flexibilidad y adecuación funcional; capacidad de uso y estética de la interfaz de usuario; protección contra errores del usuario e integridad y satisfacción y confianza.

Tabla 2.
Métricas de calidad de uso y calidad del producto

Criterio: relaciona el criterio de la medida seleccionada.	
Métrica: se especifica la métrica a medir, bien sea de calidad de uso, calidad del producto o calidad de uso y producto.	
Objetivo: son las acciones que se llevan a cabo en la aplicación de la métrica.	
Método de medida	Método utilizado en la medida cualitativa, cuantitativa o semi-cuantitativa.
Valor	Define la cantidad de medida.
Tipo	Hace relación al tipo de control que se establecen en la métrica, puede ser calidad del producto o calidad de uso del producto.
Escala	Se define el tipo de escala; binomial, intervalos, ordinal o ratio.
Procedimiento	Establece el método de recolección de datos en la métrica.

3. Resultados

3.1. Presentación de los resultados.

Los resultados para cada herramienta seleccionada fueron analizados por plugins relevantes del software Volatility, ya que es una de las mejores herramientas en el mercado para el análisis de las evidencias como lo establece, (NAXHACK5, 2016), esta afirmación surge de la realización de evaluación de adquisición de la memoria RAM con las herramientas DumpIt y FTK Imager.

Porqué Volatility, es una respuesta que la proporciona bytemind (2020) al decir que "Volatility es una herramienta forense de código abierto para la respuesta a incidentes y el análisis de malware". Añade que está escrito en Python y es compatible con Microsoft Windows, Mac OS X y Linux. No obstante, Volatility es una herramienta utilizada en muchos casos para comprender y analizar información de malware como lo indican Quintana & Medina (2018), agregó, diciendo que el análisis de una evidencia era eficaz después de utilizar un buen software de extracción de evidencia.

3.1.1. Medida de calidad de uso y calidad del producto. Para especificar esta medida, son muy importantes las direcciones de búsqueda de información de la herramienta Volatility, su estructura es:

root@kali: Escritorio/Evidencia#Volatility
-f (nombre de la imagen) --dtb=(información)
--kpcr=(información) --profile=(información)
Direcciones específicas

Se observa que esta medida implica, establecer relación de medida con otras métricas como lo son las direcciones especificas; procesos que estaban corriendo en la máquina; conexiones de redes en la máquina analizada en el momento del volcado de memoria; extraer el contenido de portapapeles de Windows; módulos descargados; identificador de usuario, entre otros.

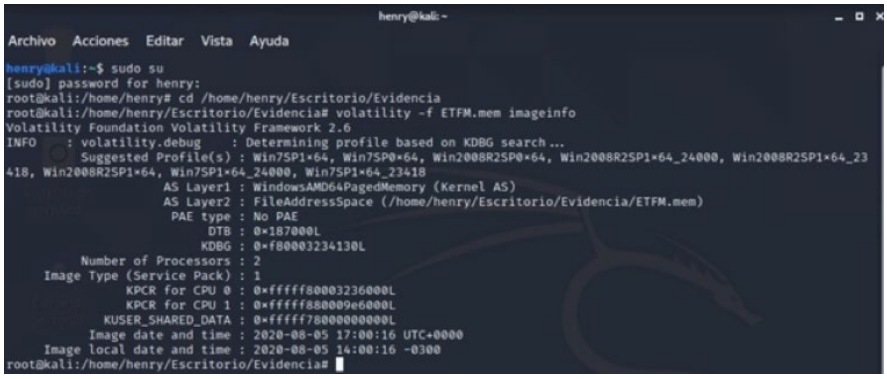

Fig. 3 Información relevante para el análisis de la evidencia digital.

En este punto, hacemos referencia a la efectividad de adquisición, como se muestra en Figura 3, para establecer información relevante como es: DTB, KDBG, KPCR y profiles.

Las herramientas que no ejecutaron el volcado de memoria, fueron: Windows Forensic Toolchest; aclaramos, que es reconocida en varios sitios web como uno de los mejores software libre para este fin, (McDougal, 2017), pero a nuestro juicio, no cumple con las condiciones mínimas para el dump de memoria RAM. Por otra parte, RamCapturer que a pesar de que ejecutó el volcado, no recolecto información, por lo que dificulta la etapa del análisis, como se muestra en la Figura 4.

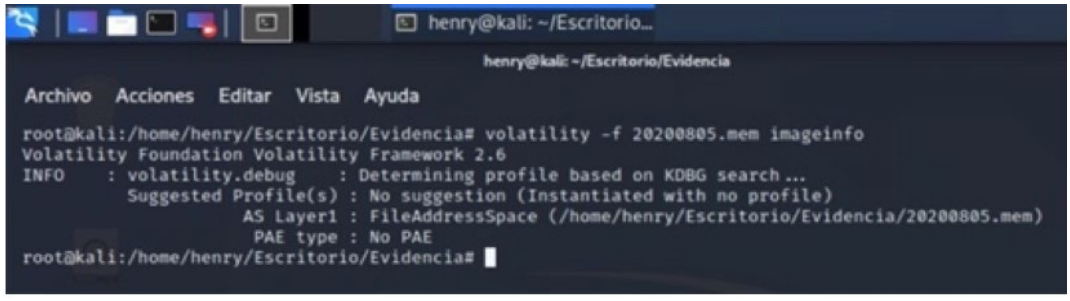

Fig. 4 Herramientas que no ejecutan volcado de memoria.

Es decir que a pesar de que RamCapturer, ejecutó el dump de memoria RAM, con un tiempo de adquisición de 00:11,57, en la etapa del análisis, nos dimos cuenta de que no recolectó evidencia alguna, produciendo un falso negativo de obtención de evidencia digital, a la vez modificando el contenido probatorio, produciendo un impacto a gran escala en la veracidad de verdad en un juicio probatorio. Esto, ya que el perito informático se confía de dump realizado, siendo un falso de adquisición.

Tabla 3.
Métricas, efectividad de adquisición: aciertos y desaciertos

Muestra/ Herramienta	DTB	KDBG	KPCR	profiles	Medida
DumpIt	1	1	1	1	4
FTL Imager	1	1	1	1	4
(WFT)	1	1	1	1	4
OSForensic	0	0	0	0	0
RamCapturer	0	0	0	0	0

Nota: La herramienta Windows Foresic Toolchest (WFT) no ejecutó el volcado de memoria RAM y RamCapturer no recuperó esa información por lo que las medidas para esta métrica es cero.

La Tabla 3 especifica aciertos (1) y desaciertos (0) para esta métrica de medida, de las herramientas seleccionadas.

3.1.2. Eficacia e integridad funcional

Se indica a continuación los plugins ejecutados para cada herramienta (pslits, pstree, netscan, clipboard, modules, unloaded, gahti, hivelist, psxview, console y malfind), iniciando con DumpIt, luego FTK Imager, OS Forensic, RamCapturer y Windows Forensic Toolchest.

En esta métrica, se brindó la relación de medida que tiene el software para adquirir contenido, que altere en lo más mínimo la evidencia y que brinde la satisfacción y seguridad al perito judicial a la hora de actuar en una escena del crimen.

4. Discusión

4.1. Interpretación de los resultados.

La Figura 5 muestra los resultados de la medida eficacia, integridad y funcionalidad. DumpIt y FTK Imager por ejemplo, mostraron 20 procesos padres enlistados y 61 procesos hijos (FTK Imager uno menos). OS Forensic, recolecto 22 procesos padre (dos más que las otras herramientas) y 48 procesos hijos, dejando en evidencia que no captura tantos procesos hijos enlistados como si lo hacen DumpIt y FTK Imager.

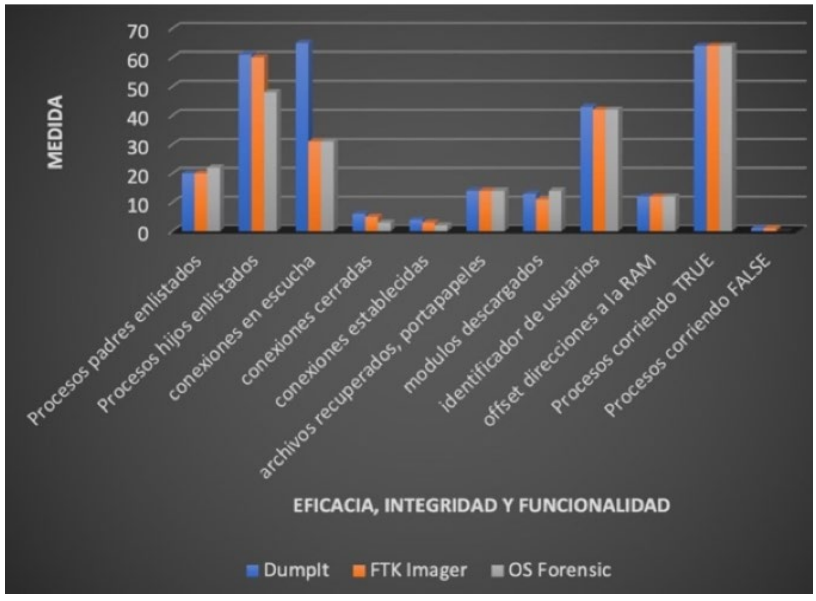

Fig. 5 Relación de eficacia, e integridad funcional

Se deduce, que la herramienta OS Forensic, no brinda seguridad al recolectar la información de procesos ocultos en el sistema, porque dejan sin adquirir más de la mitad de la información, caso contrario, DumplIt y FTK Imager, que son eficientes y eficaces para adquirir procesos ocultos que estaban enlistados en la máquina vulnerada. Estos resultados se evidenciaron cuando se aplica el comando pstree de Volatility.

Igualmente, se verifican las conexiones de redes. DumplIt, muestra 65 conexiones en escucha, 6 cerradas y 4 conexiones establecidas. Por otra parte, FTK Imager, deja al descubierto 31 conexiones en escucha, 5 cerradas y 2 conexiones establecidas. Y OS Forensic, evidencia 31 conexiones en escucha, 3 cerradas y 2 establecidas. Lo anterior indica que, para realizar un análisis de memoria RAM en conexiones de redes, la mejor herramienta es DumpIt, seguida de FTK Imager.

En lo relacionado con extraer información del portapapeles de Windows, las tres herramientas (DumpIt,

FTK Imager y OS Forensic), cumplen la misma función de forma eficiente, ya que se recuperaron 9 archivos y 5 que están sobrescritos.

En lo referente a los módulos descargados por el usuario; la herramienta DumpIt mostró 13, FTK Imager 11 y OS Forensic 14. Siendo una medida muy pareja, por lo que las tres herramientas son recomendados para esta labor en particular. De igual forma, las tres herramientas (DumpIt, FTK Imager y OS Forensin) cotejan por igual la información del usuario del equipo vulnerado.

Para ejecutar los análisis más profundos de la evidencia adquirida, se hace necesario saber las áreas físicas y virtuales (offset); frente a esto, se aplicó el comando gathi de Volatility que es de gran ayuda en la informática forense. En esta medida, los software DumpIt, Ftk Imager y OSForensic, arrojaron por igual, un resultado de 12 direcciones virtuales y físicas de offset directas a la RAM.

Con respecto al indicador de medida con procesos ocultos, DumpIt y FTK Imager, arrojaron 64 resultados enlistados como verdaderos y un proceso enlistado falso, ósea oculto, mientras que OS Forensic, muestra los mismos 64 procesos enlistados, pero no el que está oculto y que aparece con los otros mencionados. Los comandos escaneados solo son mostrados por la herramienta DumpIt que se ejecuta por consola, a diferencia FTK Imager y OS Forensic.

Por último, DumpIt y FTK Imager muestran un malware en ejecución, mientras que OS Forensic, no muestran malware ejecutándose en el sistema.

La Figura 6, evidencia que las herramientas DumpIt, FTK Imager y OS Forensic, recolectaron por igual, la información del sistema operativo y datos necesarios para el análisis de la imagen.

Así mismo, la medida eficacia integridad y funcionalidad, es observada en la misma figura, siendo DumpIt en nuestra investigación la más eficiente a la hora de realizar el volcado de memoria RAM; recolectar más procesos enlistados y más conexiones en red.

En lo referente a la métrica de eficiencia y comportamiento. FTK Imager se tomó un tiempo de 03:47,36 y OS Forensic 01:17,93. DumpIt con una medida de cronómetro de 01:29,22. Si bien, OS Forensic, gasta menos tiempo que DumpIt y FTK Imager en la adquisición, no adquiere tanta información como las ya mencionadas. Dicho de otra manera, DumpIt obtiene una medida objetiva (Alta), por ser el software que más evidencia recolecta gastando más tiempo que OS Forensic y FTK Imager, pero es más recomendada por ser eficiente en el proceso de pericia.

Por otra parte, RamCapturer, se muestra como una de las herramientas más eficiente en el volcado de memoria RAM, por gastar menos recursos en menos tiempo, pero dicho inicialmente, este software no garantiza la adquisición de la evidencia.

Con respecto a DumpIt, no deja modificar la ruta ni tampoco renombrar la imagen, pero, si se ejecuta desde un pendrive que es lo más recomendado, automáticamente guarda la imagen en el dispositivo (USB) y asigna el nombre de la máquina vulnerada. Caso contrario, es FTK Imager y OS Forensic, que permiten realizar cambios de nombre y guardado en la imagen.

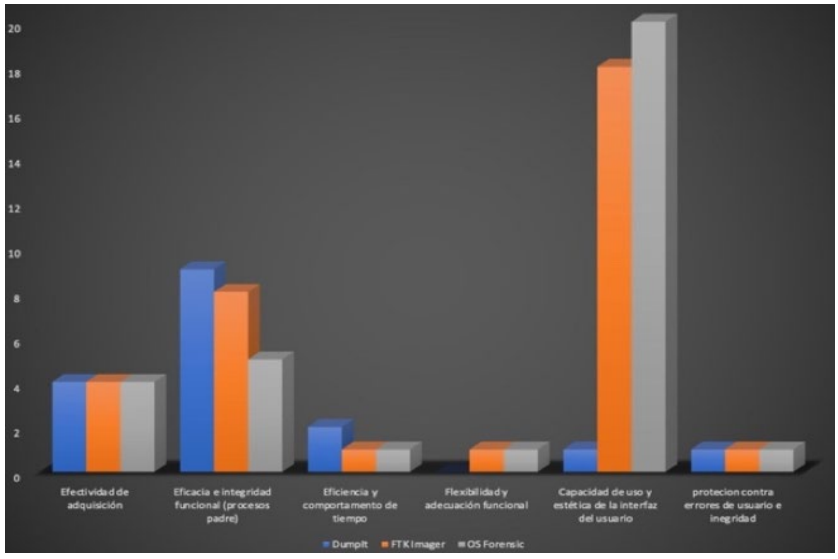

Fig. 6. Resultado de métricas evaluadas.

En lo referente a la capacidad de uso y estética de la interfaz de usuario, FTK Imager y OS Forensic, brindan más funciones para ejecutar en su interfaz que la herramienta DumpIt, que solo está diseñada para la adquisición de evidencias de la memoria RAM.

El último dato a tener en cuenta de la Figura 6, es la protección contra errores de usuario e integridad. Para este punto en particular, las tres herramientas (DumpIt, FTK Imager, OS Forensic) son fiables para el perito informático, ya que arroja un mensaje antes de ejecutar la acción.

4.2. Trabajos futuros

La realización de este artículo destaca las líneas de investigación futuras en la ciencia forense digital, además brinda al perito judicial, la satisfacción y confianza de elegir herramientas de software libre, para el volcado de la memoria RAM. En efecto, en el ámbito forense digital, existen suficientes pruebas para el análisis de recolección de información de disco duro, de interconexiones de redes, hasta del análisis del comportamiento de un malware, pero son pocos los trabajos que se enfocan en el volcado de la memoria RAM.

Ahora bien, para ampliar esta investigación se recomiendan los siguientes trabajos a futuro y así poder completar esta evaluación, esto es:

Las técnicas anti-forenses amplian esta investigación, y es que analizar y conocer estas actividades, le permite al perito auditar de forma más especifica la adquisición de evidencias en el análisis forense digital.

La computación en la nube con entornos virtuales abre posibilidades de investigación, ya que la memoria RAM no es única de una máquina sino de un sistema informático, con lo cual se puede modificar y duplicar la naturaleza de la evidencia.

Captura de código malicioso (malware) en la memoria RAM. A futuro, es más útil realizar una recolección de malware en la memoria RAM que en el disco duro, por el hecho de que el código esta al descubierto y no empaquetado o cifrado, por lo que el análisis será más claro para observar su comportamiento y vector de ataque.

Adquisición de evidencias en la nube con entornos virtuales; como se dijo inicialmente, la memoria RAM es de un sistema informático y no de un solo dispositivo, lo que facilita las técnicas anti-forenses y dificulta la adquisición del contenido probatorio.

Efectuar una evaluación de herramientas de software libre para la adquisición de la memoria RAM, en sistemas operativos Linux y Mac OS, puede ser individual o en forma conjunta.

Extender este análisis a herramientas de pago, para la adquisición de la memoria RAM, para todos los sistemas operativos.

Hacer comparación de herramientas de adquisición de evidencia digital, tanto de pago como software libre en los diferentes sistemas operativos.

Lo anterior beneficia no solo a la ciencia forense sino también a auditores de sistemas, analistas de redes, analistas de código malicioso, unidades de delitos informáticos, unidades del cibercrimen, entre otros.

5. Conclusiones

Para dar respuesta a la pregunta que motivó esta investigación ¿Cuál es la mejor herramienta a la hora de adquirir una evidencia digital?, pasamos a la conclusión en lo referente a la satisfacción y confianza que brinda la herramienta a la hora de adquirir la evidencia de la memoria RAM y afirmamos que DumpIt y FTK Imager; a nuestro juicio, son las mejores herramientas de libre uso para el sistema operativo Windows a la hora de adquirir la evidencia digital, y que el perito informático debe tener en su kit de investigación.

No obstante, esta afirmación surge de la acumulación de resultados observados y cuantificados, de las diferentes medidas aplicadas y evidenciadas en las Figuras 5 y 6, para las que la ISO /IEC 25010 brindó las medidas de calidad de uso y calidad de producto.

Referencias

ACCESSDATA. (2022). FTK Imager version 4.2.1. AccessData. https://accessdata.com/product-download/ftk-imager-version-4-2-1

Belkasoft. (2022). Belkasoft RAM Capturer: Volatile Memory Acquisition Tool. https://belkasoft.com/es/ram-capturer

Brezinski, D. & Killallea, T. (2002). Directrices para la recopilación y el archivo de pruebas. https://www.ietf.org/rfc/rfc3227.txt

bytemind. (27de febrero de 2020). Análisis forense con volatility. Byte Mind. https://byte-mind.net/analisis-forense-con-volatility/

Echavarría-Flórez, I. S. & Restrepo-Calle, F. (2020). Métricas de legibilidad del código fuente: revisión sistemática de literatura. Revista Facultad de Ingeniería, 29(54), e11756-e11756. https://doi.org/10.19053/01211129.v29.n54.2020.11756

Granados, Á. C. M. & Buitrago, F. A. S. (2013). Evaluación y comparación de herramientas para el análisis forense en redes. Cuaderno Activa, 5, 31-37. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/128

Grispos, G., Storer, T. & Glisson, W. B. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics (IJDCF), 4(2), 28-48. https://doi.org/10.4018/jdcf.2012040103

ICIBE-Cert. (12 de noviembre de 2015). Introducción al análisis forense en móviles. INCIBE-CERT. https://www.incibe-cert.es/blog/introduccion-analisis-forense-en-moviles

Instituto Nacional de Ciberseguridad. (2021). Incibe. https://www.incibe.es/

ISO 25000. (2021). ISO/IEC 2502n – División de Medición de Calidad. https://iso25000.com/index.php/normas-iso-25000/8-iso-iec-2502n

ISO 25000. (2021). Normas ISO 25000. https://iso25000.com/index.php/normas-iso-25000?limit=4&limitstart=0

ISO/CEI 25022. (2016). ISO/IEC 25022:2016. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/57/35746.html

ISO 9000. (2015). ISO 9000:2015(es), Sistemas de gestión de la calidad—fundamentos y vocabulario. https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:es

ISO/CEI TR 9126-3. (2003). ISO/IEC TR 9126-3:2003. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/02/28/22891.html

ISO-IEC 9126-2 "Métricas Externas"—Instituto Politécnico Nacional. (2003). https://1library.co/article/iso-iec-m%C3%A9tricas-externas-instituto-politecnico-nacional.z3d0458e

ISO/IEC 25010. (2011). ISO/IEC 25010:2011(en), Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models. https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en

ISO/IEC 27037. (2012). ISO/IEC 27037 Directrices para identificación, recopilación, adquisición y preservación de evidencia digital. Ciberseguridad. https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital/

ISO/IEC TR 9126-4. (2004). ISO/IEC TR 9126-4:2004. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/97/39752.html

Lázaro Domínguez, F. (2014). E Libro. https://bv.unir.net:2769/es/ereader/unir/106250?page=97

Lima, J. S. G. & Cajamarca, B. L. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica, 6(3), 89-95. https://dialnet.unirioja.es/servlet/articulo?codigo=6163708

McDougal, M. (2017). Software y seguridad de Fool Moon. http://www.foolmoon.net/security/

NAXHACK5. (2016). Análisis Forense II – Adquisición de memoria RAM – Follow The White Rabbit. https://fwhibbit.es/analisis-forense-ii-adquisicion-de-memoria-ram

Oficina Federal de Investigaciones. (2021). Cyber Crime [Folder]. Federal Bureau of Investigation. https://www.fbi.gov/investigate/cyber

Quintana, L. B. & Medina, C. R. (2018). Herramienta de extracción de información de malware. 95.

Rafael_L_R. (2019). Perito informático y tecnológico - PeritoIT. http://peritoit.com

Soft32. (2022). Descargar DumpIt 1.3.2. https://dumpit.soft32.com/

Software PASSMARK. (2021). OSForensics—Download. https://www.osforensics.com/download.html