EXTRACCIÓN DE IMAGEN FORENSE A MERORIA RAM, PARA APLICAR MECANISMOS DE PASSWORD CRACKING

Lisbeth Carolina Mendoza Varela, ingeniera en sistemas Informáticos, Técnico en Tecnologías de la Información del concejo de la judicatura Consejo de la Judicatura
Caro-mend@espam.edu.ec

Cesar Moreira Zambrano, Ingeniero en Sistemas Informáticos, Administrador del Centro de Datos de la ESPAM MFL. Escuela Superior Politécnica Agropecuarias de Manabí
cmoreira@espam.edu.ec

RESUMEN

Con los avances y necesidades actuales se necesitan dispositivos digitales con más capacidad de procesamiento de información y almacenamiento de datos. Haciendo de los dispositivos una mina de información potencial que puede caer bajo ataques de personas que operan fraudulentamente en crímenes cibernéticos, los cuales acceden a información de los usuarios cometiendo actos ilícitos digitales, divulgación de información privada y un sinnúmero de ciberdelitos.

La aplicabilidad de mecanismos de Informática Forense se encarga de la adquisición, el análisis y la valoración de elementos de evidencia digital hallados en ordenadores, soportes de datos e infraestructuras de red, que pudieran aportar luz en el esclarecimiento de actividades ilegales perpetradas en relación con instalaciones de proceso de datos, independientemente de dichas instalaciones sean el objetivo de la actividad criminal para cometerla.

El presente trabajo se enfoca en la utilización de técnicas forense aplicada a dispositivos de almacenamiento temporal como memoria RAM que se encuentran incorporados en todos los equipos electrónicos digitales con el fin de almacenar información de manera temporal; y posterior a esto aplicar técnicas de ethical hacking con mecanismos de password cracking, se analizan las capacidades, potencialidades y/o deficiencias de las herramienta dando a conocer sus resultados técnicos en cuanto a efectividad, tiempo de proceso y recuperación de datos; tomando en consideración que la información se puede almacenar, borrar y recuperar con base científica, haciendo de la investigación algo curiosamente interesante con carácter científico.

Palabras claves: password cracking, Memoria RAM, Imagen Forense, Ciberseguridad, Informática Forense.

INTRODUCCIÒN

Actualmente las tecnologías de la información y comunicación constituyen la columna vertebral para el funcionamiento de organizaciones y empresas de todo tipo. La ubicuidad de medios informáticos, combinada con el crecimiento acelerado de Internet y los despliegues de redes durante los últimos años, abre un escenario de oportunidades para actos ilícitos, sin embargo, esta creciente popularidad tecnológica hace que la misma se vea sumergida en actividades ilegales o delictivas, donde operaciones como el narcotráfico, sicariato, pornografía infantil, fraudes financieros entre otros (DOMINGUEZ, 2019), sin duda han elevado sus índices de criminalidad, siendo el crimen cibernético uno de los más escurridizos en la escala del crimen organizado de alto nivel, es aquí donde la cyberseguridad ha generado interés en los últimos años pero no es menos cierto que los estados no adoptan políticas plenamente establecidas para mitigar el impacto generado por los medio digitales (Pinto, 2016).

Las tareas de análisis forense en dispositivos de almacenamiento como las memorias RAM pueden volverse en muchas ocasiones una ardua labor, y bajo ciertas circunstancias como: condiciones internas de la organización, falta de conocimiento o inexistencia de estándares o buenas prácticas; y condiciones como: el desconocimiento o falta de leyes, hacen que el estudio se pueda volver incluso imposible, pero mediante la utilización de herramientas tecnológicas podemos realizar la extracción de imágenes forense en caliente como o aplicando mediante mecanismo de post-mortem.

En otras ocasiones las dificultades sí están causadas por aspectos técnicos, ya que para conservar adecuadamente una prueba esta debe ser previamente recolectada con éxito, es decir efectuar la recolección de evidencias bajo parámetros legales, así como en la forma de proceder para su recolección, lo que garantiza la integridad de las evidencias; teniendo como principal inconveniente la inexistencia de un estándar mundial que rija este tipo de tareas. Otro aspecto a

considerar es la multiplicidad de marcas y sistemas operativos de los equipos de cómputo. Esto lleva a dejar insubsistente la evidencia recopilada sea por vacíos normativos o por la pérdida de integridad de la información por la inadecuada manipulación de la misma (Cajo, 2019).

Esta imposibilidad no siempre viene determinada por la capacidad técnica sino por los requisitos legales exigibles a las evidencias que procedan de este tipo de equipos de cómputo. Por ejemplo, una de las condiciones clave en la recolección de evidencias es la asepsia, práctica que asegura que las pruebas recogidas no estén contaminadas, que por tanto sean válidas.

Cuando un computador está involucrado en un delito o en un incidente se debe analizar y tomar en cuenta que el dispositivo contiene información personal, laboral, e incluso puede reflejar costumbres o hábitos de la persona, convirtiéndose así en información muy sensible para ser tomada para una investigación.

Existen diferentes tipos de herramientas forenses de extracción de imagen de memoria RAM. FTK Imagen es una herramienta para la creación de imágenes de disco y extracción de imágenes digitales de toda índole hablado de informática forense, guarda una imagen de un disco duro en un archivo o en segmentos que pueden ser posteriormente reconstruidos y analizados. Se calcula los valores de hash MD5 y confirma la integridad de los datos antes de cerrar los archivos. El resultado es un archivo de imágenes que se pueden guardar en varios formatos, incluyendo, DD raw. (Rivera, 2016)

METODOLOGIA Y MATERIALES

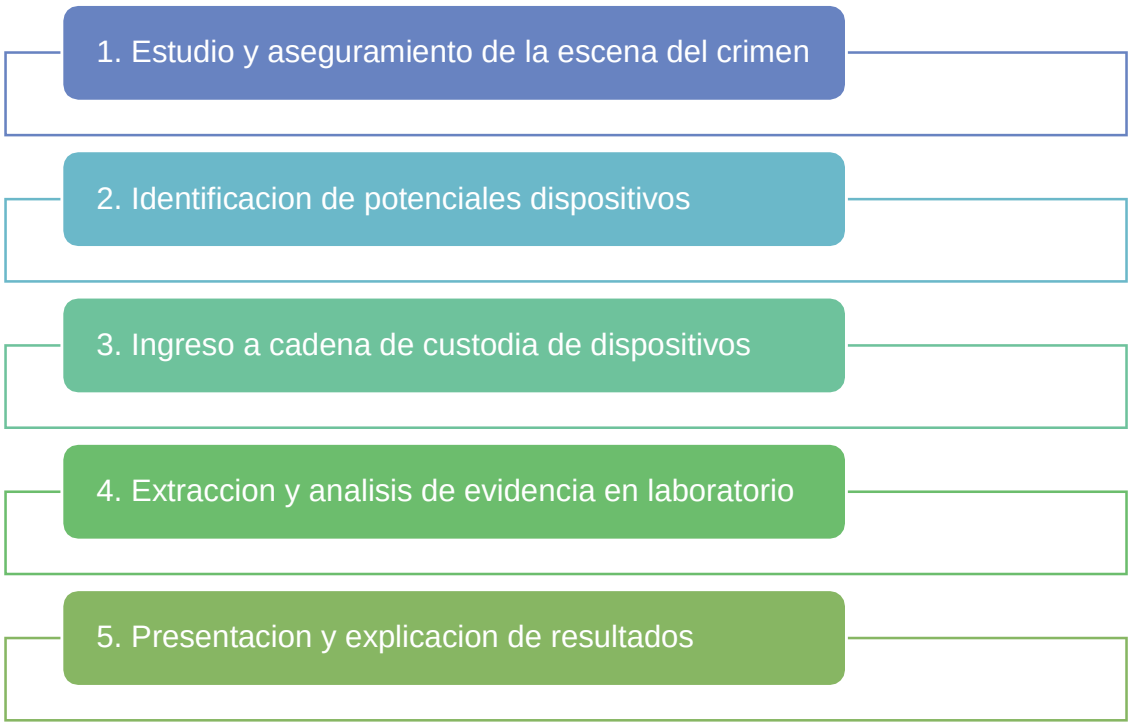
En los últimos años se han desarrollado distintas metodologías para el análisis forense digital, todo acorde a los casos que se le presentan al equipo forense, sin embargo, algunas empresas o instituciones de seguridad digital han expuesto las suyas mismas que han servido de base en el presente trabajo. En la tabla 1 se muestran las metodologías revisadas.

Tabla 1. Metodologías revidas

Metodología de MaTTica (MaTTica, 2017)	Identificar Preservar Analizar Presentar
Metodología de ragonJar (DragonJAr, 2014)	Acceso Adquisición Análisis Reporte

La metodología propuesta se encuentra sustentada en la experiencia profesional en el campo de la informática forense aplicada en las pericias dentro del país, la metodología se acopla al sistema de justicia e investigación vigente en el Estado Ecuatoriano..

La metodología propuesta en el presente trabajo consta de cinco fases.



Estudio y aseguramiento de la escena del crimen

Para este efecto el investigador forense digital forma parte del operativo y del primer equipo para realizar el aseguramiento in situ, asegurando los equipos electrónicos donde almacena información digital, encendido o apagados

Identificación de potenciales dispositivos

Identificar los dispositivos activos y pasivos, dispositivos conectados a redes cableadas o inalámbricas, etiquetar y asegurar técnicamente los equipos pasivos, verificar los equipos activos de los cuales se pueda extraer evidencia digital en caliente, extraer evidencia digital de los equipos activos identificados anteriormente, apagar, etiquetar y asegurar los equipos activos.

Ingreso a cadena de custodia de dispositivos

La cadena de custodia es una exigencia legal y fundamental en un proceso de investigación, el experto forense debe estar al tanto de la legislación, normativa y procesos de cadena de custodia para aplicar las siguientes acciones:

1. Identificar y registrar todas las características de los dispositivos previamente etiquetados.
2. Registrar la información con fecha y hora en los formatos de cadena de custodia.
3. Ingresar todo el hardware etiquetado a cadena de custodia con el respectivo acuse de recibo del custodio.
4. Trasladar bajo cadena de custodia todos los dispositivos a bodega o laboratorio forense para la extracción de la información.

Extracción y análisis de evidencia en laboratorio

Una vez obtenida la evidencia y cumpliendo con la cadena de custodia, siguiendo los parámetros legales, se procedió con la extracción de evidencia digital utilizando herramientas forenses de software, dependiendo del caso el forense decide qué herramienta usar y cómo analizar la evidencia extraída; sin embargo en la primera fase que es la apertura de dispositivos y extracción de evidencia, analizaremos tres herramientas forenses de alta tecnología como son Access Data

FTK Imager, OSForensics y L0phtCrack (Tabla 2)

Herramienta	Características	Tiempo de extracción en minutos	Tiempo de extracción en segundos	Capacidad de imagen gigabytes	Herramienta Booteable
Access Data FTK Imager	Propietario y versión free limitada	11.00	32	6.49	Si
OSForensics	Propietario y versión free limitada	3.0	0.1	6.49	Si
L0phtCrack	Propietario	9.00	54	6.49	SI

Tabla 1. Herramientas de análisis forense Autores (2020).

FTK Imager y OSForensics poseen mecanismo de análisis forense digital, comenzando por el bloqueo de escritura del dispositivo, a diferencia de los bloqueadores de hardware que nos permite bloquear la escritura del medio de almacenamiento precautelando la veracidad y autenticidad de la evidencia a extraer.

La metodología permite realizar la adquisición mediante un proceso de clonado bit a bit también conocido como bajo nivel, bajo este procedimiento se obtiene una imagen exacta de los datos contenidos del dispositivo de almacenamiento, este proceso se encuentra documentado a detalle en el RFC 3227. La norma indica que no se debe trabajar con la evidencia original del medio de almacenamiento de datos, sino con una copia a bajo nivel del mismo denominada imagen forense.

Password cracking

Las técnicas de password cracking son utilizadas para recuperar las contraseñas de los sistemas informáticos, los atacantes aplican estas técnicas para obtener acceso no autorizado al sistema vulnerado, en si la mayoría de las técnicas de

password cracking tienen éxito debido a las contraseñas débiles o fácilmente adivinables, como muestra la **tabla 2.**

Información	**Determinación del perfil basado en la búsqueda de KDBG**
	Win7SP1x64
AS Layer1	WindowsAMD64PagedMemory (Kernel AS)
AS Layer2	FileAddressSpace (/root/Desktop/ramimage.mem)
PAE type	No PAE
DTB	0x187000L
KDBG	0xf800046500a0L
Number of Processors	4
Image Type (Service Pack)	1
KPCR for CPU 0	0xfffff80004651d00L
KPCR for CPU 1	0xfffff880009ea000L
KPCR for CPU 2	0xfffff88003165000L
KPCR for CPU 3	0xfffff880031d7000L
KUSER_SHARED_DATA	0xfffff78000000000L
Image date and time	2020-09-11 03:42:34 UTC+0000
Image local date and time	2020-09-10 22:42:34 -0500

Tabla 2. Determinación del perfil de búsqueda KDBG

Para ver todos los hive de memoria de donde están cargados los registros utiliza el comando hivelist, **ver tabla 2.**

Virtual	Physical	Name
0xfffff8a00009e010	0x00000000004b9010	\REGISTRY\MACHINE\HARDWARE
0xfffff8a0002f6010	0x00000001589be010	\Device\HarddiskVolume2\Boot\BCD
0xfffff8a00036b01	0x00000001589b3010	\SystemRoot\System32\Config\SOFTWARE
0xfffff8a00320c010	0x00000001491ae010	\SystemRoot\System32\Config\DEFAULT
0xfffff8a0034c5010	0x00000001461a2010	\SystemRoot\System32\Config\SECURITY
0xfffff8a00352e2b0	0x00000001458af2b0	\SystemRoot\System32\Config\SAM
0xfffff8a0035d7010	0x00000001446f3010	\??\C:\windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a003755010	0x0000000143d7d010	\??\C:\Users\Laptops\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a003861410	0x00000001450a7410	\??\C:\windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a003962010	0x000000014004c010	\??\C:\Users\Laptops\ntuser.dat
0xfffff8a007a4d410	0x00000000a64b1410	\??\C:\System Volume Information\Syscache.hve
0xfffff8a00000d010	0x00000000002e2010	[no name]
0xfffff8a0000241f0	0x00000000004291f0	\REGISTRY\MACHINE\SYSTEM

Tabla 3. Extracción de los hive de memoria

Presentación y explicación de resultados

Como se puede apreciar en la tabla 3, los datos que nos interesan son las espacios de memoria SAM y SYSTEM, el comando para extraer el contenido completo de SAM es el siguiente hashdump, -y registro del archivo SYSTEM –s y ahora si el Offset donde está el SAM para identificar donde está el hive en la memoria –s tal como se muestra a continuación en la tabla 4.

USUARIO	HASH
Administrator	:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest	:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Laptops	:1000:aad3b435b51404eeaad3b435b51404ee:3f1d9cdd90f1a484cf99eca3a4e29865:::

Tabla 4. Hash de memoria extraída de SYSTEM Y SAM

Como podemos apreciar en la tabla 4 ya extrajo el contenido de la memoria SAM del registro, donde podemos visualizar los diferentes usuarios del sistema operativo, Administrator, Guest, Laptops con sus respectivos hash

Luego de haber guardado el contenido dentro de un archivo plano con el nombre de sam.txt podemos utilizar una herramienta de tipo John de ripper para reventar esa clave y poder conocer el password mediante técnicas de password cracking ver imagen 1.

Imagen 1. Aplicabilidad de John ripper para extraer la clave del sistema operativo

2%35, 4! $/ 3 9 $)3#53)s .

Como resultado de los análisis comparativos y de los indicadores, se presenta el análisis correspondiente a la extracción de la imagen forense de la memoria RAM, la cual consta de 5 fases.

Estudio y aseguramiento de la escena del crimen: se formó parte del equipo primario en visitar y manipular el equipo considerando varias acciones basadas en la experticia que se tiene.

Identificación de potenciales dispositivos: para preservar la evidencia digital se aplicó la cadena de custodia correspondiente para evitar que la información perdiera validez lo cual es una exigencia legal y fundamental en un proceso de investigación de cualquier tipo, la misma no está exenta en la investigación digital, es más, en forense digital se vuelve transcendental, considerando que la información contenida en medios digitales es altamente volátil y de fácil alteración.

Extracción y análisis de evidencia en laboratorio: Una vez extraída la evidencia forense bajo cadena de custodia, siguiendo los parámetros legales, el experto procede a la extracción de evidencia digital con herramientas forenses de hardware y software, para este efecto se aplicó la herramienta de kali Linux 19.0 con los componentes integrados de volatility y John ripper.

Presentación y explicación de resultados:

De manera experimental se efectuó el procedimiento de extracción de una imagen forense de memoria RAM en un ambiente controlado de un equipo de cómputo, identificando toda la información almacenada en el dispositivo. Para llevar a cabo

el proceso se utilizaron instrumentos como: solicitud del incidente, revisión de legislación, cadena de custodia, reportes detallados e informe final. Se validaron los resultados usando diferentes herramientas tanto de software libre como de software propietario.

Este procedimiento permitió manejar y analizar evidencias digitales almacenadas en la memoria RAM del equipo de cómputo mediante una extracción en tiempo real, garantizando el proceso forense. Para llevar a cabo el proceso se identificaron varias herramientas, sin embargo, ninguna de ellas resulta ser mejor que otra. Por lo tanto, es importante utilizar la herramienta OSForensics para la extracción de la imagen forense y para la manipulación y extracción de la información mediante la herramienta de kali Linux en si versión 19.0 con su componente integrado en la función de volatility, la misma que permite realizar el proceso de preservación, y posterior aplicar técnicas de ethical hacking con la herramienta de jonh ripper. La utilización de estas herramientas nos permitió obtener un rendimiento promedio del 90% durante todo el proceso forense, sobre otras herramientas analizadas.

CONCLUSIONES

El análisis forense digital de memoria RAM, permite analizar a profundidad si el equipo está infectado mediante malware, o si el existen conexiones remotas existentes, y mediante herramientas se logra reventar las claves de acceso al sistema operativo mediante password cracking, pero el mismo análisis forense permite reconstruir un evento ilícito, como la copia no autorizada de archivos o documentos confidenciales, intrusión en bases de datos, clonación de identidad

electrónica, ataques a servidores o equipos conectados a redes y muchos otros ilícitos que se han convertido en el escenario del crimen moderno.

Para realizar el proceso de extracción de una imagen forense de memoria RAM. Se debe tener conocimientos sólidos en ciberseguridad, tener amplio conocimiento de tecnología digital, electrónica y de telecomunicaciones pasando por la programación, los sistemas operativos y las bases de datos.

La aplicabilidad de mecanismos de ethical hacking basado en herramientas como John the Ripper son de mucha seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de los usuarios son suficientemente buenas. John the Ripper es capaz de autodetectar el tipo de cifrado de entre muchos disponibles, y se puede personalizar su algoritmo de prueba de contraseñas.

BIBLIOGRAFIA

Cajo, I. M. (2019). *Evidencias Digitales en la Investigación Forense Informática.* Riobamba, Ecuador: Editorial Politécnica ESPOCH.

Dominguez, f. L. (2019). *Introduccion a la informática forense.* Cali: casa del libro.

Pinto, D. (2016). Metodología de análisis forense orientada a incidentes en dispositivos móviles. *Revista Cientifica MASKANA*, 1-11.

Rivera, A. (10 de 04 de 2016). *Backtrack Academy.* Obtenido de https://backtrackacademy.com/articulo/creacion-y-analisis-basico-de-una-imagen-forense-en-windows-7-con-ftk-imager-y-volatility