Análisis forense de memoria RAM como evidencia digital en delitos comunes: simulación de peculado en Ecuador

Vaca Belalcázar Henry Santiago[1]✉,

[1]Especialización en Informática Forense, Universidad Fraternidad de Agrupaciones Santo Tomás de Aquino (FASTA), Gascón 3145, (B7600FNK) Mar del Plata. Buenos Aires, Argentina.

✉ santyv_01@hotmail.com

Datos del artículo
Cita
Vaca Belalcázar H.S. Análisis forense de memoria RAM como evidencia digital en delitos comunes: simulación de peculado en Ecuador. ReCiF. 2026;(1):1–14.

Editor
Julio César Martínez Sánchez

Revisión por pares
Dos

Recibido
4/julio/2025

Aceptado
25/noviembre/2026

Publicado
30/abril/2026

Resumen

En Ecuador, entre 2020 y 2024 se registraron 8.724 denuncias por ciberdelitos, de las cuales únicamente se reportan 82 detenciones, lo que representa una tasa de efectividad del 0.94%. Esta cifra genera preocupación social y plantea serios cuestionamientos en torno a la capacidad investigativa del estado. En este contexto, se presenta el análisis forense de memoria RAM como una técnica ampliamente utilizada para la investigación de delitos informáticos, pero subutilizada en la pericia de delitos comunes con componentes tecnológicos. El objetivo de este artículo es precisamente determinar la importancia de dicho análisis en la investigación criminal, a partir de una simulación del delito de peculado en un entorno controlado. Para lo cual, se aplicó una metodología cualitativa-exploratoria basada en tres volcados de memoria con distinto nivel de sobreescritura, tiempo de acción y estado de aplicaciones. Los resultados evidencian la recuperación de mensajes, archivos, datos de navegación, así como la construcción de una línea de tiempo que vincula evidencias digitales con usuarios. Estos hallazgos demuestran que el análisis forense de memoria RAM aporta evidencias útiles en este tipo de delitos, lo que podría contribuir a mejorar la eficacia de la justicia penal ecuatoriana.

Palabras clave: informática forense, análisis forense, memoria RAM, peculado, *volatility*, admisibilidad legal.

Abstract

In Ecuador, between 2020 and 2024, 8.724 cybercrime reports were filed, of which only 82 arrests were reported, representing a 0.94% effectiveness rate. This figure generates social concern and raises serious questions about the state's investigative capacity. In this context, forensic RAM analysis is presented as a widely used technique for investigating cybercrimes, but underutilized in common crimes with technological components. The objective of this article is precisely to determine the importance of such analysis in criminal investigations, based on a simulation of the crime of embezzlement in a controlled environment. To this end, a qualitative-exploratory methodology was applied based on three memory dumps with different levels of overwriting, duration of action, and application status. The results show the recovery of messages, files, browsing data, as well as the construction of a timeline linking digital evidence to users. These findings demonstrate that forensic analysis of RAM provides useful evidence in these kinds of crimes, which could contribute to improving the effectiveness of Ecuadorian criminal justice.

Key words: digital forensics, forensic analysis, RAM memory, embezzlement, Volatility, legal admissibility

Introducción

La digitalización ha transformado las dinámicas sociales, económicas y gubernamentales, aportando eficacia, automatización y desarrollo. No obstante, este avance ha traído consigo también importantes desafíos: el acceso remoto, el anonimato y la sofisticación de estrategias criminales han expandido no solo los ciberdelitos, sino también la planificación y ejecución de delitos comunes apoyados por tecnologías de la información y comunicación (TIC).

En el Ecuador, según el boletín de análisis de ciberdelincuencia del Ministerio del Interior de la nación, entre 2020 y 2024 se reportaron 8.724 ciberdelitos de los cuales solo se han efectivizado 82 detenciones, es decir una tasa de eficacia del 0.94%. Esta cifra visibiliza la limitada capacidad del estado para investigar delitos tecnológicos (1). Por otra parte, según datos internos oficiales de la Dirección Nacional de Investigación Técnico Científico Policial (DINITEC)[1], las pericias informáticas se incrementaron de 1.956 en 2019 a 6.617 en 2024. Estas pericias en su mayoría se concentran en delitos comunes como: tráfico de drogas (2.267), peculado (1.303) y asesinato (1.148), lo que evidencia que actualmente los delitos comunes requieren cada vez más de análisis digital. No obstante, estas experticias se enfocan casi exclusivamente en la evidencia digital no volátil como dispositivos de almacenamiento externo, relegando el análisis de evidencia volátil como la contenida en la memoria RAM.

En este escenario, la informática forense se consolida como una disciplina clave para el sistema judicial, al aplicar una metodología científica destinada a la identificación, adquisición, análisis y preservación de evidencia digital que podría resultar clave en procesos judiciales (2). Dentro de sus múltiples técnicas, la memoria RAM constituye una fuente única de evidencia: almacena procesos activos, claves de sesión, archivos temporales y conexiones de red que desaparecen al apagar el sistema, haciendo su análisis esencial para reconstruir eventos en tiempo real (3).

A nivel internacional, el análisis forense de memoria RAM ha demostrado ser fundamental en fraudes financieros, phishing y secuestro de códigos 2FA, herramientas como Volatility2 y FTK Imager3 (Forensics Toolkit Imager) permitieron recuperar credenciales robadas, sesiones activas y registros efímeros que demostraron el flujo del delito (4–6). En extorsiones digitales y ataques con ransomware como Conti, la RAM fue clave para obtener claves de cifrado eliminadas y reconstruir conversaciones volátiles en plataformas como WhatsApp Web (7,8). Incluso llamadas VoIP han sido analizadas con éxito al recuperar paquetes de voz e identificadores de sesión no almacenados en servidores (9).

Las redes sociales también han sido utilizadas como escenario del delito, y la memoria RAM permitió acceder a pruebas que de otro modo habrían sido irrecuperables. En Twitter, se recuperaron publicaciones eliminadas y credenciales activas vinculadas a discursos de odio (10), mientras que en Facebook se identificaron anuncios borrados relacionados con tráfico ilegal de órganos (11,12). A su vez, en accesos no autorizados a dispositivos y cuentas digitales —como WhatsApp Desktop, correos electrónicos y teléfonos móviles— se logró extraer desde la RAM archivos cifrados, claves de sesión y credenciales temporales, fortaleciendo la imputación penal (13–15).

[1] Los datos citados de DINITEC corresponden a estadísticas internas oficiales de gestión pericial, entregadas al autor —miembro activo de la Policía Nacional del Ecuador— mediante comunicación institucional autorizada. Estos registros no se encuentran publicados en medios de acceso abierto por su naturaleza operativa.

[2] Herramienta de análisis forense de memoria RAM, utilizada para extraer procesos activos, conexiones y artefactos digitales volátiles.

[3] Software que permite capturar imágenes forenses de discos y memoria RAM, preservando la integridad digital mediante funciones hash.

Incluso en delitos de alta complejidad tecnológica, como sabotajes industriales o evasión de localización en smartphones con GPS desactivado, el análisis de memoria RAM ha resultado decisivo. En sistemas robotizados, se identificaron comandos maliciosos en ejecución mediante LIME[4] *(Linux Memory Extractor)* y Volatility, y en móviles se reconstruyeron ubicaciones a partir de datos Wi-Fi temporales, aportando evidencia fundamental en casos de crimen organizado (16,17).

En el Ecuador, el trabajo de Montesinos Abad (18) constituye el único antecedente encontrado sobre el uso de memoria volátil con fines investigativos. En este estudio se aplicaron herramientas como Volatility, FTK Imager y Autopsy[5] en un caso simulado de delito informático, específicamente relacionado con la filtración de bases de datos empresariales. El autor demostró que el análisis forense de memoria RAM permitió acceder a procesos activos, claves temporales y conexiones de red que no se registran de forma persistente. Estos resultados evidencian el valor de esta técnica en contextos investigativos nacionales, incluso tratándose de un entorno simulado.

A partir de la literatura revisada, se revelan al menos dos limitaciones importantes: en primer lugar, los estudios se centran en escenarios puramente digitales, sin extender su aplicación a delitos del derecho penal común, como lo es el peculado. En segundo lugar, privilegian el componente técnico sobre los aspectos jurídicos, dejando de lado desafíos como la integridad de la evidencia, la cadena de custodia y su admisibilidad en juicio.

Frente a esta brecha, el presente estudio, de enfoque cualitativo, exploratorio y aplicado, no solo busca replicar procedimientos técnicos ya conocidos, sino abrir un campo de aplicación innovador: demostrar, mediante una simulación controlada de delito penal común (peculado), que el análisis de memoria RAM puede expandir el potencial probatorio de las investigaciones criminales en entornos donde, hasta ahora, no ha sido considerado como son los delitos comunes con componentes tecnológicos.

Metodología

Diseño del estudio y enfoque metodológico

El estudio se desarrolló mediante un enfoque cualitativo, exploratorio y aplicado, enfocado en evaluar el análisis forense de memoria RAM como técnica útil para la investigación de delitos del derecho penal común, específicamente el peculado[6]. Ante lo cual, se aplicó el método de simulación controlada, una técnica validada en disciplinas como la informática forense y ciberseguridad (19), que permite replicar escenarios delictivos de manera segura, consistente y técnicamente verificable.

El objetivo central de esta metodología fue observar la persistencia y recuperabilidad de trazas digitales volátiles en contextos simulados de comisión de delito, incluso después de intentos deliberados de eliminación superficial de evidencias.

[4] Módulo de kernel que permite la adquisición forense de memoria RAM en sistemas Linux, generando volcados en formato raw o ELF sin alterar significativamente el sistema analizado.
[5] Herramienta forense digital de código abierto que permite analizar discos duros y dispositivos extraíbles, facilitando la recuperación de archivos, metadatos y rastros de actividad en investigaciones criminales.
[6] El peculado, tipificado en el artículo 278 del COIP, consiste en que un servidor público sustrae o utiliza indebidamente fondos o bienes que administra por razón de su cargo, en beneficio propio o de terceros.

Caso simulado: peculado con uso de TIC

La elección del delito de peculado responde a su alta prevalencia en el contexto ecuatoriano, según datos internos oficiales de la DINITEC, donde figura como la segunda tipología delictiva más periciada entre 2020 y 2024. Aunque este tipo de delitos han ido en aumento, no se han encontrado antecedentes que denoten el uso del análisis forense de memoria volátil como prueba en investigaciones de esta naturaleza. Esto pone en evidencia una brecha, tanto en el ámbito metodológico como en el legal.

Para explorar esta posibilidad, el estudio desarrolló una simulación basada en un caso de peculado, que busca replicar las acciones digitales fraudulentas de un funcionario público. La intención fue comprobar si, incluso luego de intentos por borrar rastros, la memoria RAM puede conservar información clave para una investigación penal.

Diseño del escenario simulado

La simulación se desarrolló en un entorno virtual creado en *VirtualBox*, configurado con Windows 10 x64, 8 GB de RAM, y un disco duro virtual de 50 GB. Se instalaron y utilizaron aplicaciones que por sus características técnicas facilitan la configuración de escenarios realistas de ocultamiento de evidencia: WhatsApp Desktop (no guarda mensajes en el disco local), Telegram (permite mensajes autodestructivos), Signal (ofrece mensajes temporales), WordPad, Microsoft Edge y Gmail.

Durante la jornada simulada, un funcionario ficticio implicado en actos de peculado ejecutó una serie de acciones diseñadas para reflejar una conducta delictiva típica con apoyo digital. Entre ellas:

Envío de mensajes incriminatorios:

- WhatsApp Web: “Hola loco”, “te paso el documento”, “ya sabes qué hacer”, “justificar de cualquier forma” (adjuntando *gastos_presentados.rtf*).
- Signal: “Hola”, “te mandé el archivo por whata”, “ya sabes qué hacer”; respuesta: “lo hago de inmediato” (incluyendo un audio).
- Telegram: “borra todo”, “de los otros también” (junto a dos imágenes *.jpg*).
- Gmail: “Pilas”, con el documento *gastos_presentados.rtf* como adjunto.

Navegación web en sitios asociados a actividades sospechosas:

- Guías sobre como enviar mensajes temporales en Signal.
- Manuales para gestión de transacciones fraudulentas (Stripe).
- Página oficial del Ministerio de Finanzas del Ecuador.

Modificación de documentos:

- Edición del archivo *gastos_presentados.rtf* en WordPad.

Captura de memoria RAM y escenarios temporales

Para evaluar la persistencia de artefactos en distintos contextos de sobrescritura digital, se realizaron tres volcados de memoria RAM en diferentes momentos:

Escenario	Estado aplicaciones	Tiempo desde la acción	Nivel de sobrescritura	Objetivo forense
Volcado 1	Todas las apps abiertas y en uso	Inmediato	Nulo	Capturar la máxima densidad de evidencia en RAM
Volcado 2	Eliminados mensajes y documentos, apps aún abiertas	10 minutos	Bajo	Evaluar persistencia tras intento superficial de borrado
Volcado 3	Todo cerrado, usuario ejecuta nuevas tareas	30 minutos	Moderado	Simular ocultamiento con sobrescritura activa y ver recuperación residual

Tabla 1. Caracterización técnica de los escenarios de volcado de memoria

Metodología de análisis forense

Figura 1. *Proceso de análisis forense de memoria RAM*

Resultados

Se realizaron tres volcados de memoria RAM en distintos momentos del ciclo de uso del sistema, simulando variaciones en el grado de sobrescritura y persistencia de evidencia digital. A continuación, se sintetizan los resultados obtenidos.

Escenario 1: captura con todas las aplicaciones abiertas

Este volcado se realizó con todas las aplicaciones activas y sin procedimientos previos de cierre o eliminación. Fue el entorno más fértil para la recuperación de evidencia volátil.

Tipo de Evidencia	¿Recuperada?	Fragmentos recuperados	Observación técnica breve
WhatsApp Web (Edge) – Mensajes	Completa	"ya sabes que hacer", "Hola loco", "justificar de cualquier forma", "te paso el documento,	Mensajes completos recuperados de *buffers*[7] y caché del navegador.
WhatsApp Web (Edge) – Archivo .rtf adjunto	No recuperado	–	No se hallaron rutas de archivo ni buffers activos en RAM
Signal – Mensajes	Parcial	"ya sabes que hacer", "lo hago de inmediato", "Hola"	Fragmentación del *heap*[8] o cifrado en memoria impidieron recuperar el texto completo.
Signal - Audio enviado	No recuperado	–	No se halló ni el buffer de reproducción ni el archivo temporal en heap.
Telegram – Imágenes	No recuperadas	–	Referencias visualizadas con *filescan*, pero los *dump*[9] fallaron.
Telegram – Mensajes	Completo	"borra todo", "De los otros tambien", "Si de una", "ya se la vuelta"	Persistencia completa en heap por sesión activa.
WordPad	Completo	Contenido RTF completo, encabezado + cuerpo: "gastos presentados"	Documento abierto, sin cierre ni modificación posterior.
Documento enviado	Completo	"gastos presentados.rtf"	Recuperado con estructura íntegra.
Actividad en navegador	Completa	"www.finanzas.gob.ec", www.stripe.com", "www.support.signal.org"	Actividad visible en RAM y estructura *HTTP/WebSocket* intacta.

Tabla 2 *Resultados del volcado 1*

Este escenario representa la condición óptima para una pericia digital basada en memoria RAM. La integridad de los mensajes y del documento .rtf, sumada a la recuperación completa de la actividad

[7] Zonas temporales de almacenamiento utilizadas por el sistema para gestionar datos en tránsito.
[8] Segmento dinámico de la memoria RAM utilizado por los programas para almacenar datos temporales en tiempo de ejecución.
[9] Volcado de memoria.

de navegación, demuestra que una captura inmediata posibilita reconstrucciones completas y robustas de los eventos. Esto justifica la inclusión del análisis RAM en protocolos iniciales de intervención en delitos con componentes digitales.

Escenario 2: cierre de aplicaciones y eliminación superficial

Tras el cierre de sesiones y la eliminación manual de mensajes, se realizó la segunda captura sin reinicio del sistema ni herramientas de limpieza. El volumen y calidad de la evidencia disminuyeron sensiblemente:

Tipo de Evidencia	¿Recuperada?	Fragmentos recuperados	Observación técnica breve
WhatsApp Web (Edge)	Parcial	"Hola loco", "justificar de cualquier"	Algunos mensajes persistieron en buffers cerrados, aunque incompletos.
Signal – Mensajes	Parcial	“Hola” y "lo hago de inmediato"	Fragmentación en heap o cifrado de sesión impidieron recuperación completa."
Signal – Audio	No recuperado	–	La ausencia total de buffers sugiere que el archivo de audio fue cargado brevemente y liberado antes del volcado.
Telegram – Imágenes	No recuperadas	–	Direcciones virtuales inservibles o sobreescritas.
Telegram - Mensajes	Parcial	“Borra todo” y “Si de una”	Persistencia mínima en *strings*[10], sin respaldo binario.
WordPad	Incompleto	Solo encabezado: "gastos presentados.rtf"	El documento cerrado genera fragmentación, pérdida del cuerpo del texto.
Actividad en navegador	Fragmentaria	"web.whatsapp.com" (sin más contexto)	Pérdida de conexiones activas y tokens de sesión.

Tabla 3. *Resultados del volcado 2*

Aunque se observaron pérdidas sustanciales de evidencia, la permanencia de fragmentos textuales revela que eliminar archivos o cerrar sesiones no garantiza el borrado de datos volátiles. En este escenario la memoria RAM ha probado ser un recurso útil para reconstruir, aunque sea de manera limitada, el comportamiento digital del usuario. Este tipo de resultados adquieren especial importancia en estudios que buscan mostrar comportamientos de ocultación o consolidar pistas ya existentes a través de señales residuales.

[10] Comando de análisis forense que permite localizar y extraer cadenas de texto legibles dentro de archivos binarios o volcados de memoria, facilitando la recuperación de datos ocultos o fragmentarios.

Escenario 3: sobrescritura inducida por uso posterior

En este escenario, se representó una circunstancia donde el usuario intentó eliminar toda evidencia: se cerraron las aplicaciones empleadas, se eliminaron archivos y se empezó a usar el equipo con otras herramientas antes de efectuar el volcado de memoria. Esta disposición facilitó la observación de los efectos de la sobreescritura provocada por el uso subsiguiente y su influencia en la conservación de los datos originales.

Tipo de Evidencia	¿Recuperada?	Ejemplos de fragmentos recuperados / Estado	Observación técnica breve
WhatsApp Web (Edge)	Fragmentaria	"documento", "Hola loco", sin orden ni sesión activa	Persisten cadenas Unicode aisladas. No hay estructura de conversación o trazas web intactas.
Signal – Mensajes	Parcial	"Ya sabes que hacer", "Hola", sin metadatos visibles	Fragmentos dispersos sin procesos o buffers identificables. Memoria parcialmente sobrescrita.
Signal – Audio	No recuperado	–	Archivo no se detectó ni en filescan ni con extracción dirigida. Posible sobrescritura total.
Telegram – Imágenes	No recuperadas	–	Ninguna imagen visible por binwalk, strings ni file. Probable liberación de memoria.
Telegram – mensajes	Parcial	“borra”	Persistencia residual en heap; sin respaldo estructural ni metadatos
WordPad	No recuperado	–	Documento completamente ausente. Fragmentación extensa. No hay encabezado.
Documento enviado por Gmail	No recuperado	–	Ningún rastro del envío ni del archivo, pese a haberse enviado por navegador.
Actividad en navegador	Mínima	"finanzas.gob.ec", sin estructura de navegación	Fragmentos aislados de cadenas, sin cookies, historial ni buffers activos.

Tabla 4. *Resultados del volcado 3*

La sobrescritura operativa —sin herramientas específicas de borrado seguro— fue suficiente para destruir prácticamente toda la evidencia estructurada. Solo restaron fragmentos desconectados de texto sin sentido. Esto demuestra que el tiempo es un elemento crucial en la cadena de custodia digital y que los procesos forenses deben dar prioridad a las intervenciones iniciales para optimizar el potencial de prueba de la RAM.

Línea de tiempo forense

La línea de tiempo se desarrolló a partir del Volcado 1, reconstruyendo de manera cronológica las acciones fundamentales efectuadas por el usuario. Para determinar la secuencia de sucesos, se utilizaron marcas de tiempo recuperadas, fragmentos de mensajes y rutas de archivo.

Fecha	Hora	Plataforma	Contenido extraído	Contacto / Usuario
2025-04-06	—	WhatsApp Web	“Hola loco”	—
2025-04-16	03:05	WhatsApp Web	Sesión activa	+5491140382914
2025-04-25	13:24:14	Signal	“Mensaje de voz” enviado	+541157522791
2025-04-25	13:37:03	WhatsApp Web	“Ya sabes que hacer”	91140382918@c.us / Amor arXXXa
2025-04-25	—	WhatsApp Web	“Te paso el documento”	—
2025-04-25	—	WhatsApp Web	Ruta de archivo: *gastos_presentados.rtf*	Usuario local: santy
—	—	Telegram	“Borra todo”, “Ahorita borro”	—
—	—	Telegram	“Ya se la vuelta”	—

Tabla 5. *Línea de tiempo forense extraída de la memoria RAM*

La reconstrucción de la línea de tiempo desde la memoria RAM permite no solo establecer el orden secuencial de los eventos, sino **vincular directamente a usuarios y contactos específicos mediante identificadores únicos.** La aparición de números telefónicos internacionales (códigos +54, Argentina) y dominios de mensajería encriptada como *c.us* sugiere **una posible red transnacional de apoyo logístico o de complicidad**, abriendo hipótesis investigativas sobre el alcance y coordinación del delito. Así mismo, frases como “ya sabes qué hacer” y “borra todo” refuerzan señales de **dolo, premeditación e intento de ocultación.** Este tipo de evidencia digital de carácter volátil, complicada de seguir tras la clausura de las aplicaciones, constituye un recurso esencial para sustentar líneas de investigación penal complejas, particularmente en crímenes financieros con repercusiones internacionales.

Discusión:

Aspecto técnico: resultados, valor judicial y comparación con estudios previos

Los resultados obtenidos a partir del análisis de los tres volcados de memoria RAM permiten confirmar la utilidad práctica de esta técnica en el contexto de una investigación por peculado, un delito común con componentes digitales. A diferencia de la mayoría de los estudios revisados en el estado del arte, donde el análisis de RAM se ha aplicado predominantemente en delitos informáticos como fraude electrónico, suplantación de identidad o ransomware (3,5,6), esta investigación se enfocó en un escenario no tradicional: un delito económico con intercambio de comunicaciones y documentos a través de mensajería y correo electrónico. Esta aplicación representa una contribución importante al debate técnico y metodológico, al demostrar que el análisis forense de memoria RAM puede superar el ámbito puramente cibernético.

Los hallazgos del volcado 1 mostraron una alta capacidad de recuperación de evidencia digital: se consiguió obtener mensajes íntegros de WhatsApp Web, textos fragmentados de Signal, un documento .rtf totalmente integro y la actividad web del navegador. Este patrón concuerda con lo indicado por Estupiñán Londoño y colaboradores (20), quienes enfatizan que la RAM guarda procesos, archivos y

conexiones activas, facilitando la reconstrucción de eventos relevantes. Sin embargo, incluso en estas condiciones óptimas, no se lograron recuperar los archivos binarios de audio ni las imágenes enviadas por Telegram. Este comportamiento técnico coincide con lo observado en varios casos del estado del arte (7,8), donde elementos como medios multimedia presentan una volatilidad más alta o sufren liberación rápida de memoria al cerrarse la aplicación o tras el envío.

En los volcados 2 y 3, tras el cierre de las aplicaciones y el uso continuado del sistema, se observó una pérdida progresiva de evidencia: mensajes incompletos, ausencia de archivos, fragmentación de strings y desaparición de estructuras clave. Este comportamiento confirma lo planteado por Osborne (2) sobre los desafíos técnicos que implica la gestión dinámica de la RAM, particularmente cuando interviene sobrescritura por uso prolongado. La fragmentación o ausencia de buffers en estos escenarios revela también los límites de la técnica, y deja claro que el éxito del análisis forense depende de una captura oportuna y de un entorno técnico controlado, como lo exigía la simulación.

Por otro lado, la construcción de la línea de tiempo a partir del volcado 1 constituye una herramienta de valor estratégico. Este recurso permitió vincular frases clave, fechas, usuarios, teléfonos y nombres de archivos, creando una narrativa cronológica de las acciones del usuario simulando el delito. En contraste con estudios como el de Rido y Fachri (4), que se enfocan en evidencias puntuales, esta investigación demuestra que la RAM puede ser utilizada no solo para extraer fragmentos, sino para generar una base sólida de reconstrucción fáctica, útil en el desarrollo de hipótesis investigativas, órdenes de allanamiento, o interrogatorios. Su valor como guía para judicialización es, por tanto, concluyente y metodológicamente sustentado.

Finalmente, es necesario señalar que este estudio presenta ciertas limitaciones. En primer lugar, el tiempo de captura de la memoria RAM se restringió a una ventana de treinta minutos, lo cual, permitió observar cómo la recuperación de información se volvía cada vez más escasa, especialmente en el tercer volcado; en un escenario real, esta limitación temporal podría ser de horas o hasta días, lo que afectaría totalmente la eficacia de esta técnica forense. Además, que la investigación se desarrolló en un entorno controlado y simulado, lo que implica que no se enfrentaron todas las condiciones e imprevistos propios de una intervención judicial real. Finalmente, el número de escenarios de prueba (3) fue acotado, lo que, si bien permitió una exploración valiosa, deja pendiente la necesidad de ampliar la variedad de contextos y configuraciones para robustecer los resultados.

Aspecto legal: admisibilidad, protocolos y vacíos regulatorios en evidencia volátil

Cuando analizamos la posibilidad de realizar un volcado de memoria RAM en un caso judicial, lo primero que surge es cuestionar en qué contexto se lo podría autorizar y realizar. La simulación mostró que solo es viable si el equipo está encendido y no ha pasado demasiado tiempo, porque una vez apagado la información se pierde por completo. En la práctica real esto implicaría que la captura se realice en un allanamiento o en un caso flagrante, justo en el momento en que los equipos están en funcionamiento.

También se abre la discusión sobre quién puede y debe autorizar este procedimiento. La ausencia de normas específicas genera incertidumbre, porque en escenarios urgentes el fiscal podría generar la orden, pero en otros casos se esperaría una autorización del juez. En la simulación realizada, se asumió que el procedimiento se ejecutaba de forma controlada y sin contratiempos, pero en el ámbito real esa falta de precisión legal podría volverse un punto débil en la admisibilidad de la prueba. Esto deja ver que no basta con la técnica, sino que se necesita claridad en la norma para blindar jurídicamente el proceso.

Otro tema clave es el de la autenticidad e integridad de la evidencia. La memoria RAM es volátil y cualquier intervención puede alterar su contenido. En la simulación, se utilizó el cálculo de hash y un registro detallado del proceso como una manera transparente de mostrar que lo obtenido no fue manipulado (21). Estas prácticas son fundamentales si se quiere que la prueba sea considerada en un juicio, porque sin esa garantía mínima siempre habrá la posibilidad de que la defensa cuestione su validez. La experiencia práctica mostró que es posible preservar la cadena de custodia y eso marca la ruta de lo que debería hacerse en el contexto real.

Finalmente, no se puede olvidar la brecha con los estándares internacionales. Normas como la ISO/IEC 27037 presentan criterios claros sobre cómo actuar en la captura de evidencia digital volátil y sobre el rol del perito en estas intervenciones (22). En Ecuador estas directrices aún no están adoptadas del todo, lo que significa que cada perito actúa a criterio y los jueces terminan valorando las evidencias digitales con un margen de subjetividad. En la simulación se siguieron varias de estas recomendaciones —uso de hash, documentación exhaustiva de los procedimientos, herramientas validadas por la comunidad forense—, pero más por convicción técnica-metodológica que por que existan normativas específicas que obliguen a ello en el Ecuador. Esto refleja una realidad preocupante: aunque la técnica funcione y entregue resultados sólidos, sin un marco alineado a estándares internacionales la carga probatoria de la evidencia digital puede verse reducida en los tribunales.

Consideraciones finales:

Este estudio permitió demostrar que el análisis forense de memoria RAM no solo es útil en delitos informáticos, sino también en delitos comunes con componentes tecnológicos. En el escenario simulado de peculado, se evidenció que la RAM puede contener mensajes, documentos y trazas de navegación que, en un proceso real, podrían convertirse en evidencias clave para vincular hechos y sospechosos. Esto reafirma que su valor trasciende lo puramente digital, abriendo posibilidades de uso en investigaciones criminales de diversa índole.

Los resultados demuestran que esta técnica puede ser una herramienta estratégica para el sistema judicial ecuatoriano si se aplica de forma oportuna. La recuperación de evidencia digital volátil podría contribuir a mejorar la baja tasa de efectividad actual, que apenas alcanza el 0.94% de detenciones frente al total de ciberdelitos. Incrementar esta cifra no solo representa mayor eficiencia en la persecución penal, sino también un beneficio concreto para la sociedad ecuatoriana, que enfrenta riesgos crecientes a medida que la vida cotidiana se digitaliza.

Desde lo técnico, el trabajo con los volcados reveló un patrón claro: el primer volcado, realizado con mayor rapidez, permitió la recuperación íntegra de mensajes y documentos, confirmando la importancia de actuar con inmediatez. El segundo mostró una reducción en la calidad de la información, aunque aún se rescataron datos relevantes que podrían encausar una investigación judicial, mientras que en el tercero la evidencia fue muy escasa y fragmentada. No obstante, incluso estos fragmentos podrían resultar útiles para hacer hipótesis investigativas, lo que reafirma el hecho de que cada minuto cuenta en este tipo de experticias.

En el ámbito legal, la simulación evidenció la necesidad crítica de contar con un marco normativo específico. Actualmente, la falta de reglas claras sobre quién debe autorizar la captura, en qué condiciones puede hacerse y cómo garantizar la integridad de los datos, genera riesgos de impugnación en juicio. Por lo tanto, se vuelve indispensable establecer normativas que eliminen la discrecionalidad y aseguren que estos procedimientos estén respaldados por órdenes válidas, protocolos estandarizados y apego a estándares internacionales como las ISO/IEC.

Otro aporte relevante fue la construcción de la línea de tiempo a partir del primer volcado, que posibilitó organizar los datos de forma cronológica y comprensible. Esta herramienta no solo fortalece el análisis técnico, sino que también facilita la interpretación judicial, al brindar a fiscales y jueces una narrativa sistemática de los hechos. En un juicio real, esta visualización puede marcar la diferencia entre una evidencia aislada y una prueba sólida capaz de sostener la acusación.

Finalmente, aunque el estudio se realizó en un entorno controlado y con un número limitado de escenarios, sus resultados abren la puerta a futuras aplicaciones. La técnica podría ponerse a prueba en investigaciones de delitos como tráfico de sustancias estupefacientes y psicotrópicas o incluso homicidios, donde el componente digital cada vez tiene mayor peso. Explorar nuevos contextos y superar las limitaciones aquí señaladas permitirá consolidar al análisis de RAM como una herramienta indispensable para la justicia en el Ecuador.

Conflicto de intereses

El autor sostiene que no hay conflictos de interés vinculados con esta investigación, ni conexiones comerciales, patentes o desarrollos tecnológicos que puedan influir en los hallazgos presentados.

Declaración de ética

Esta investigación no implicó a participantes humanos ni recolección de información personal. Se realizó una simulación controlada en ambiente virtual, sin la participación de individuos reales. Por lo tanto, no fue requerida la aprobación de un comité de ética institucional. La investigación se llevó a cabo siguiendo los principios de integridad científica y las mejores prácticas en investigación digital.

Referencias

1. Ministerio del Interior del Ecuador, Dirección Nacional de Ciberdelitos. La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial. Boletín de Análisis de la Ciberdelincuencia. 2024 dic. Available from: https://www.ministeriodelinterior.gob.ec/wp-content/uploads/downloads/2025/07/Boletin-La-nueva-era-de-la-ciberdelincuencia-el-lado-oscuro-de-la-Inteligencia-Artificial.pdf.
2. Carrier B. File System Forensic Analysis. Addison-Wesley Professional; 2005.
3. Osborne G. Memory forensics: review of acquisition and analysis techniques. Canberra (AU): Defence Science and Technology Organisation (DSTO); 2013. Report No.: DSTO-GD-0770. Available from: https://scispace.com/papers/memory-forensics-review-of-acquisition-and-analysis-331cklw7z9
4. Vella M, Rudramurthy V. Volatile memory-centric investigation of SMS-hijacked phones: a Pushbullet case study. In: Proceedings of the 2018 Federated Conference on Computer Science and Information Systems (FedCSIS); 2018 Sep 9–12; Poznań, Poland. ACSIS. 2018;15:607–616. doi:10.15439/2018F11

5. Rido AS, Fachri F. Identifikasi bukti digital WhatsApp pada sistem operasi proprietary menggunakan live forensics. J Ilm Penelit Pembelajar Informatika (JIPI).2024;9(2):1043–1051. doi:10.29100/jipi.v9i2.5238
6. Shukla S, Misra M, Varshney G. Identification of spoofed emails by applying email forensics and memory forensics. In: Proceedings of the 10th International Conference on Communication and Network Security (ICCNS 2020); 2020 Nov 20–22; Tokyo, Japan. New York: ACM; 2020. p. 109–114. doi:10.1145/3442520.3442527
7. Umar R, Riadi I, Kusuma RS. Analysis of Conti ransomware attack on computer network with live forensic method. Int J Inf Dev. 2021;10(1):53–61. doi:10.14421/ijid.2021.2423
8. Amelia C, Riadi I. Browser forensic of extortion case on WhatsApp Web using National Institute of Justice method. Int J Comput Appl. 2021;183(42):36–42. doi:10.5120/ijca2021921823 Available from: https://ijcaonline.org/archives/volume183/number42/32213-2021921823/
9. Irwin D, Slay J, Dadej A, Shore M. Extraction of electronic evidence from VoIP: forensic analysis of a virtual hard disk vs RAM. J Digit Forensics Secur Law. 2011;6(1):15–36. doi:10.15394/jdfsl.2011.1086 Available from: https://commons.erau.edu/jdfsl/vol6/iss1/2
10. Suryani S, Riadi I. Web forensic for hate speech content on Twitter services using National Institute of Standard Technology method. Int J Comput Appl. 2021;183(40):30–38.Available from:https://www.ijcaonline.org/archives/volume183/number40/suryani-2021-ijca-921798.pdf
11. Bahari PW, Riadi I. Facebook browser investigation on Chrome using National Institute of Standards and Technology method. Int J Comput Appl. 2021;183(44):35–40. doi:10.5120/ijca2021921858 Available from: https://ijcaonline.org/archives/volume183/number44/32229-2021921858/
12. Puri CST, Riadi I. Browser forensic for cyber fraud case on Facebook Messenger services using National Institute of Standard Technology method. Int J Comput Appl. 2021;183(42):22–29. doi:10.5120/ijca2021921818 Available from: https://ijcaonline.org/archives/volume183/number42/32211-2021921818/
13. Cahyanto TA, Rizal MA, Wardoyo AE, Warisaji TT, Daryanto. Live forensics to identify the digital evidence on the desktop-based WhatsApp. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). 2022;6(2):213–219. doi:10.29207/resti.v6i2.3849. Available from: https://jurnal.iaii.or.id/index.php/RESTI/article/view/3849
14. Thing VLL, Ng KY, Chang EC. Live memory forensics of mobile phones. Digit Investig. 2010;7(Suppl 1):S74–S82. doi:10.1016/j.diin.2010.05.010 Available from: https://www.sciencedirect.com/science/article/pii/S174228761000037X
15. Faiz MN, Umar R, Yudhana A. Implementasi live forensics untuk perbandingan browser pada keamanan email. JISKa (J Informatika Sunan Kalijaga). 2017;1(3):108–114. doi:10.14421/jiska.2017.13-02 Available from: https://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/13-02
16. Mayoral Vilches V, Alzola Kirschgens L, Gil-Uriarte E, Hernández A, Dieber B. Volatile memory forensics for the Robot Operating System. arXiv [preprint]. 2018 Dec 22 [cited 2025 Jul 3]. Available from: https://doi.org/10.48550/arXiv.1812.09492
17. Anwar N, Mardhia MM, Ryanto L. Live forensics on GPS inactive smartphone. Mobile Forensics.2021;3(1):32–44. doi:10.12928/mf.v3i1.3847.

Available from:https://journal2.uad.ac.id/index.php/mf/article/view/3847 (journal2.uad.ac.id)
18. Montesinos Abad FM. Informática forense: herramientas open source y análisis de datos para el volcado de memoria "MEMDUMP" y su aplicabilidad en la investigación de delitos informáticos [undergraduate thesis]. Quito (EC): Universidad Internacional del Ecuador; 2022.
19. Casey E. Digital evidence and computer crime: forensic science, computers, and the internet. 3rd ed. Amsterdam: Academic Press; 2011.
20. Estupiñán Londoño TV, Mora Merchán KT, Santiago Cely CP. Importancia de la memoria como evidencia digital en la informática forense. In: Proceedings of the 17th LACCEI International Multi-Conference for Engineering, Education and Technology; 2019 Jul 24–26; Montego Bay, Jamaica. Paper 477. doi:10.18687/LACCEI2019.1.1.477 Available from: https://laccei.org/LACCEI2019-MontegoBay/full_papers/FP477.pdf
21. Selvarajah V, Mailvagnam J. A framework for handling digital forensic evidence and evaluation on cyber resilience. J Appl Technol Innov. 2021;5(4):6.
Available from:
https://dif7uuh3zqcps.cloudfront.net/wpcontent/uploads/sites/11/2021/09/30200408/Volume5_Issue4_Paper2_2021.pdf
22. Hermosa Llanos I, Arcos García LA, Murillo Andrade HX, Recalde Rivera PE. Evaluación del peritaje informático forense en Quito: desafíos, estándares y recomendaciones para mejorar su eficacia. Rev Científica Ciencia Tecnología. 2024;24(44). Available from: https://cienciaytecnologia.uteg.edu.ec/revista/index.php/cienciaytecnologia/article/download/723/836/2456