Cloud Forensics Research

Fecha : 12/02/2025

Asignatura: Análisis Forense

Curso: 2024/25

Grupo: 3

Integrantes: Israel Valderrama, Alejandro Seoane, Victor Jímenez, Alejandro Díaz y Nicolás Ruiz.

Índice

1. Resumen Ejecutivo

El análisis forense digital en entornos cloud presenta desafíos específicos debido a la naturaleza distribuida, la elasticidad y la volatilidad de los datos en la nube. Este informe investiga las metodologías aplicadas a la adquisición y preservación de evidencias digitales en la nube, las dificultades técnicas y normativas involucradas, y las mejores prácticas identificadas en la literatura y en estudios de caso.

2. Introducción

En los últimos años, el análisis forense en la nube ha ganado popularidad debido al crecimiento exponencial de los servicios cloud, los cuales ofrecen mayor flexibilidad y escalabilidad, pero también introducen nuevos riesgos de seguridad. La nube ha transformado la forma en que se crean, acceden y gestionan los servicios tecnológicos, lo que hace necesario investigar incidentes en estos entornos para identificar, recopilar y preservar evidencias (Khan et al., 2023).

El análisis forense en la nube emplea diversas técnicas para examinar brechas de seguridad en estos entornos, como filtraciones de datos o robos de identidad. Su objetivo es investigar las circunstancias del ataque, fortalecer la seguridad y proteger los activos de la organización.

Este informe explora las metodologías forenses aplicadas a la nube, haciendo énfasis en la recolección de evidencias. Además, se analizan las diferencias con el análisis forense tradicional, las herramientas más eficaces y el impacto de características como la elasticidad y ubicuidad de la nube en el proceso forense (Khan et al., 2023).

3. Análisis forense en cloud

Revisión de literatura

El análisis forense en la nube ha evolucionado como una extensión de la informática forense, adaptándose al nuevo mundo de los entornos cloud. Según (VPN Unlimited, 2024), describen el análisis como la identificación, preservación, recopilación y análisis de pruebas digitales provenientes de servicios como IaaS, PaaS y SaaS entre otros. Este enfoque es esencial para investigar incidentes como brechas de seguridad o accesos no autorizados. Por su parte, (Patau, 2023) destaca que el análisis forense en la nube sigue una metodología bastante parecida a la criminalística, donde se reconstruyen eventos y detectan ciberataques mediante herramientas avanzadas.

El documento (ISMS Forum, 2018) destaca la gran importancia que tienen estas estrategias de supervisión continua en entornos cloud para poder garantizar la integridad de todas las evidencias. Se mencionan herramientas como CloudTrail o Azure Monitor Log las cuales son esenciales para capturar registros críticos. (Microsoft, 2025) también insiste en

el uso de snapshots en Windows 365 para preservar datos volátiles sin comprometer el entorno original.

De manera técnica, (Oxygen Forensics, 2024) presenta técnicas como Cloud Extractor, que permite acceder a más de 100 servicios en la nube, incluyendo redes sociales y plataformas de almacenamiento. Han sido diseñadas para superar los desafíos específicos al acceso limitado y conocimiento volátil de la nube. (Patau, 2023) y (Almacenamiento IT, 2020) analizan las oportunidades y complicaciones del análisis forense en la nube, destacando problemas como los costos asociados con el almacenamiento y las diferencias jurisdiccionales.

Análisis crítico

Los desafíos que tienen para el análisis forense en la nube específicamente la naturaleza de los datos, es decir, la distribuida y dinámica de los datos. Según (VPN Unlimited, 2024) y (Patau, 2023), mencionan que la volatilidad de los datos es una de los principales problemas, ya que los registros desaparecen fácilmente debido a la elasticidad de la nube. Mientras FTK Imager o EnCase pueden ser utilizados para capturar imágenes forenses en infraestructuras IaaS, tenemos Cloud Extractor (Oxygen Forensics, 2024) (permiten acceder a plataformas SaaS con autenticación avanzada).

Desde un enfoque de vista normativo, (ISMS Forum, 2018) y (Patau, 2023) destacan que el cumplimiento del RGPD y otras regulaciones son bastantes necesarias para garantizar investigaciones legales. Las diferencias jurisdiccionales pueden dificultar el manejo de evidencias digitales, sobre todo en los datos que están distribuidos globalmente (Almacenamiento IT, 2020). (Microsoft, 2025) señala la importancia de usar logs hasheados para documentar la cadena de custodia y preservar la integridad de las evidencias.

A pesar de todas estas limitaciones, el progreso de las herramientas automatizadas ha mejorado la mitigación de algunos de los desafíos técnicos mencionados anteriormente. Por ejemplo, por un lado, aplicaciones como Splunk o Elastic Stack (Patau, 2023) facilitan la captura continua de registros antes de que estos se eliminen. Aún así destacamos la falta general de estandarización en los procedimientos forenses utilizados en entornos en la nube.

Propuestas de mejora

Existen varias tácticas fundamentadas en diferentes estudios, ayudarían a abordar algunos de los problemas anteriores. (VPN Unlimited, 2024) sugiere la forma de acuerdos entre clientes y proveedores para determinar el acceso a registros y capturas de pantalla. Específicamente, en los modelos SaaS y PaaS, el cliente tiene el menor control posible sobre sus datos.

Desde la parte técnica, (Oxygen Forensics, 2024) propone herramientas sofisticadas como Cloud Extractor para tener acceso a servicios cloud con una autenticación sólida.

(Microsoft, 2025) destaca la importancia de utilizar snapshots junto con hash logs para garantizar la preservación crítica y la verificación de la evidencia digital.

(ISMS Forum, 2018) favorece el establecimiento de marcos internos en concordancia con las normativas internacionales (como RGPD y NIS2). Además, sería beneficioso desarrollar alianzas entre compañías de nube y entidades reguladoras para establecer procedimientos forenses a nivel mundial (Patau, 2023).

Aconsejamos destinar recursos en formación técnica especializada para los equipos de investigación forense. De acuerdo con (Patau, 2023) y (Almacenamiento IT, 2020), la capacitación de profesionales en herramientas concretas como AWS CloudTrail o Azure Security Center puede mejorar notablemente las investigaciones forenses en ambientes cloud.

4. Características de la nube

4.1. Elasticidad y volatilidad

La elasticidad y volatilidad son características fundamentales de la computación en la nube que presentan desafíos significativos para el análisis forense digital. La elasticidad hace referencia a la capacidad de la nube para escalar recursos dinámicamente, lo que provoca cambios en la ubicación y el estado de los datos. Por otro lado, la volatilidad implica lo rápido que pueden modificarse o borrarse los datos en la nube (Gaviria Alvarez, 2025).

Estas características tienen una gran importancia en la preservación de evidencias digitales en entornos cloud. Los investigadores forenses deben adaptar sus técnicas y procedimientos para hacer frente a los cambios de los datos en la nube. Esto incluye el desarrollo de métodos para capturar rápidamente evidencias volátiles, implementar estrategias de preservación que tengan en cuenta la elasticidad de los recursos, y establecer procedimientos robustos para mantener la integridad de la evidencia (Gaviria Alvarez, 2025).

4.2. Ubicuidad y compartición

Según los artículos recopilados, la trazabilidad de la evidencia digital plantea un gran desafío debido a la posibilidad de almacenar grandes cantidades de información de forma remota y la capacidad de acceder a ella desde cualquier lugar. Presenta una serie de desafíos en la identificación y adquisición de datos electrónicos esenciales para un procedimiento penal cuando un perpetrador de un acto delictivo "se esconde en la nube" (Karagiannis & Vergidis, 2021).

4.3. Abstracción

La abstracción introduce grandes limitaciones en el acceso a datos y herramientas forenses. La arquitectura distribuida y virtualizada de la nube complica la identificación y adquisición de evidencia, ya que los investigadores deben coordinarse con proveedores de

servicios en la nube, administradores de envíos y propietarios de la infraestructura para adquirir los artefactos relevantes (AllahRakha, 2024).

Además, la ambigüedad legal en torno a las fronteras jurisdiccionales a menudo restringe este proceso. La naturaleza virtualizada de las plataformas en la nube también dificulta la ubicación de registros y logs necesarios para reconstruir líneas de tiempo de ataques. Rastrear ataques se vuelve aún más complicado debido a la distribución geográfica y la federación de activos en la nube entre diferentes proveedores (AllahRakha, 2024). En consecuencia, es necesario establecer estándares forenses internacionales adaptados al ecosistema de la nube que abarquen acuerdos legales, requisitos tecnológicos y pautas metodológicas para permitir investigaciones con resultados íntegros.

5. Análisis de normativas y su impacto

El análisis forense en entornos de computación en la nube enfrenta retos únicos debido a la naturaleza distribuida, dinámica y de terceros de estos servicios. Según el artículo de (Malik et al., 2024), las principales complicaciones técnicas incluyen:

Ubicación y volatilidad de los datos: La computación en la nube permite que los datos se almacenen en múltiples centros de datos geográficamente dispersos. Esto dificulta la identificación y recuperación de evidencia, ya que los datos pueden moverse dinámicamente entre servidores y jurisdicciones sin notificación previa.

Falta de control sobre la infraestructura: Los investigadores dependen de los proveedores de servicios en la nube (CSPs, por sus siglas en inglés) para acceder a la evidencia. Sin acceso físico a los servidores, el proceso de adquisición forense se vuelve complejo y puede requerir la cooperación del CSP, que no siempre está garantizada o puede ser limitada por regulaciones de privacidad.

Integridad y autenticidad de la evidencia: En la computación en la nube, múltiples usuarios pueden compartir la misma infraestructura, lo que plantea desafíos para garantizar que la evidencia no haya sido alterada. El artículo menciona que los investigadores deben desarrollar técnicas especializadas para demostrar la autenticidad y cadena de custodia de la evidencia digital.

5.1 Implicaciones legales

Desde un punto de vista legal, el artículo destaca varios desafíos clave:

Jurisdicción y soberanía de los datos: Dado que los CSPs pueden almacenar datos en servidores ubicados en diferentes países, determinar qué leyes se aplican a una investigación es un problema complejo. Por ejemplo, si una empresa europea usa un servicio en la nube con servidores en EE.UU., las autoridades de diferentes países pueden reclamar derechos sobre esos datos, lo que puede generar conflictos legales.

Acceso y derechos de los investigadores: En muchos casos, los investigadores pueden necesitar órdenes judiciales para obtener acceso a datos almacenados en la nube. Sin embargo, las leyes varían según la región, y algunos países tienen normativas más estrictas sobre la privacidad de los datos en la nube, lo que puede impedir la recolección de evidencia.

Retención y eliminación de datos: Muchos CSPs tienen políticas de retención de datos que pueden llevar a la eliminación automática de información después de cierto tiempo. Esto complica la recuperación de evidencia si no se actúa rápidamente.

Responsabilidad y privacidad: El artículo también menciona que la relación contractual entre el usuario y el CSP juega un papel fundamental en la protección de los datos. Dependiendo de los términos de servicio, un usuario puede no tener el control total sobre su información, lo que afecta la disponibilidad de la evidencia en una investigación.

6. Recomendaciones

Como se indica en el quinto documento de la bibliografía (Practical Considerations, n.d.), es esencial adoptar procedimientos estandarizados como la ISO/IEC 27037, que aseguren la integridad y autenticidad de la evidencia digital. Estos estándares nos garantizan que la información recolectada sea válida y confiable en procesos legales, auditorías y revisiones internas.

La incorporación de tecnologías como la inteligencia artificial, el blockchain y la criptografía cuántica representa un avance significativo en la precisión y seguridad del manejo de la información digital. La inteligencia artificial facilita la automatización de procesos de análisis de grandes volúmenes de datos, el blockchain asegura la inmutabilidad y trazabilidad de la cadena de custodia, y la criptografía cuántica refuerza la protección de la confidencialidad frente a amenazas sofisticadas.

Finalmente, es importante realizar revisiones periódicas de estos procedimientos para ajustarlos a los avances tecnológicos. Las amenazas evolucionan constantemente, por lo que la capacidad de adaptación es fundamental para garantizar que las metodologías utilizadas sigan siendo efectivas y cumplan con las regulaciones vigentes. La revisión continua permite identificar áreas de mejora y adoptar rápidamente nuevas herramientas que refuercen la seguridad y fiabilidad de la evidencia digital.

7. Bibliografía

- (Gaviria Alvarez, 2025)
  Gaviria Alvarez, W. (2025). Propuesta de buenas prácticas en la recolección y garantía de integridad de la evidencia digital en el cloud computing. https://repository.unad.edu.co/handle/10596/65824

- (Karagiannis & Vergidis, 2021)
  Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the Power of Disposal. Information (Basel), 12(5), 181. https://doi.org/10.3390/info12050181

- (Khan et al., 2023)
  Khan, A. A., Shaikh, A. A., Laghari, A. A., & Rind, M. M. (2023). Cloud forensics and digital ledger investigation: a new era of forensics investigation. International Journal of Electronic Security and Digital Forensics, 15(1), 1. https://doi.org/10.1504/ijesdf.2023.127745

- (Malik et al., 2024)
  Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. Sensors (Basel, Switzerland), 24(2), 433. https://doi.org/10.3390/s24020433

- (AllahRakha, 2024)
  AllahRakha, N. (2024). Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations. Pakistan Journal of Criminology, 16(2).
  https://www.pjcriminology.com/wp-content/uploads/2024/04/9-Demystifying-the-Network-and-Cloud-1.pdf

- (VPN Unlimited , 2024)

  (N.d.). Vpnunlimited.com. Retrieved February 12, 2025, from
  https://www.vpnunlimited.com/es/help/cybersecurity/cloud-forensics

- (Patau, 2023)

  Patau, M. (2023, July 26). Todo lo que necesitas saber sobre el análisis forense en la nube. Ackcent.
  https://ackcent.com/es/todo-lo-que-necesitas-saber-sobre-el-analisis-forense-en-la-nube/.

- (Isms Forum, 2025)

  (N.d.). Ismsforum.Es. Retrieved February 12, 2025, from
  https://www.ismsforum.es/ficheros/descargas/cloudauditforensics2018v41544463021.pdf.

- (Microsoft, 2025)

  (N.d.). Microsoft.com. Retrieved February 12, 2025, from
  https://learn.microsoft.com/es-es/windows-365/enterprise/digital-forensics.

- (Oxygen Forensic, 2024)

  Cloud Extractor: 10 años del mejor análisis forense de la nube de la industria. (2024, October 21). Digitoforense.
  https://www.digitoforense.cl/noticias/oxygen-forensics/translating-digital-data-has-never-been-easier/.

- (Arsys, 2023)

  Análisis forense en cloud: ¿qué es y en qué consiste? (n.d.). Arsys. Retrieved February 12, 2025, from
  https://www.arsys.es/blog/analisis-forense-cloud.

- (Almacenamiento IT, 2020)

  (N.d.). Ituser.Es. Retrieved February 12, 2025, from
  https://almacenamientoit.ituser.es/noticias-y-actualidad/2020/07/dificultades-y-oportunidades-del-analisis-forense-en-el-almacenamiento-en-la-nube.