

Técnicas y Herramientas de Análisis Forense en Redes para la Detección y Mitigación de Ataques

Network Forensic Analysis Techniques and Tools for Attack Detection and Mitigation

Leonidas Antonio Inca Portilla ^{1*}, Ronaldo Steven Rosales Espinoza ¹

Ana María Ruíz Alcivar ¹, Nayelhy Marisol Ponce Cabrera ¹

¹ Universidad Técnica de Machala, Ecuador.

* Autor de Correspondencia: linca1@utmachala.edu.ec

Resumen: El análisis forense de redes se ha vuelto una pieza importante para investigar incidentes de ciberseguridad y recopilar evidencia digital en entornos que cada vez son más complejos. En este trabajo se revisaron 22 estudios científicos recientes con el fin de conocer las principales herramientas, métodos y desafíos presentes en esta área, considerando escenarios como IoT, la computación en la nube, las redes SDN y las tecnologías 6G. Los resultados muestran que herramientas conocidas como Wireshark y Autopsy todavía se siguen utilizando bastante, aunque poco a poco están siendo acompañadas por otras que usan aprendizaje automático para ayudar en el análisis. Sin embargo, todavía hay varios problemas por resolver, como el hecho de que no todas las herramientas funcionan bien entre sí, la dificultad para conservar correctamente la evidencia digital y la falta de reglas legales claras que sean comunes para todos los casos. En general, los resultados indican que es necesario seguir mejorando el uso de estas tecnologías en situaciones reales, teniendo en cuenta no solo lo técnico, sino también el trabajo humano y el marco legal que las rodea.

Palabras clave: Análisis forense, redes, ciberseguridad, evidencia digital, herramientas.

Abstract: Network forensics has become a crucial tool for investigating cybersecurity incidents and gathering digital evidence in increasingly complex environments. This paper reviews 22 recent scientific studies to identify the main tools, methods, and challenges in this field, considering scenarios such as IoT, cloud computing, SDN networks, and 6G technologies. The results show that traditional tools like Wireshark and Autopsy continue to play a significant role, although they are gradually being complemented by solutions that incorporate machine learning. Even so, several challenges remain, including compatibility between different tools, proper preservation of digital evidence, and the lack of common legal criteria for its handling. Overall, the findings reflect the need to further strengthen the application of these technologies in real-world situations, taking into account not only the technical aspects but also the human and legal factors involved.

Keywords: Network forensics, cybersecurity, digital evidence, forensic tools, network analysis.

1. Introducción

En los últimos años, la seguridad de las redes ya no es solo un tema técnico, sino algo que preocupa cada vez más a gobiernos, empresas y usuarios. El aumento del tráfico en internet, junto con el uso de tecnologías como el Internet de las Cosas (IoT), las redes 6G y los servicios en la nube, ha hecho que existan más puntos vulnerables que pueden ser aprovechados por atacantes. Hoy en día, las amenazas son más difíciles de detectar y seguir, ya que los ataques han cambiado y se han vuelto más complejos. Frente a este escenario, el análisis forense de redes ha tomado más importancia, porque permite revisar lo que ocurrió durante un ataque y reunir información digital que ayuda a entender cómo pasó todo. Además de ayudar a identificar posibles responsables, también sirve para mejorar la seguridad y preparar mejor a las organizaciones frente a futuros incidentes (Akinbi, 2023; Waseem et al., 2021).

También implica entender cómo se conectan y se comunican los sistemas entre sí, cómo se mueve la información dentro de una red y de qué manera se van guardando los eventos que ocurren en ella. Según Qureshi et al. (2021), el uso de herramientas como la inteligencia artificial y el aprendizaje automático ha ayudado a simplificar varias tareas que antes se hacían manualmente, lo que permite ahorrar tiempo sin afectar la calidad de la información obtenida. Estas tecnologías se utilizan en distintos contextos, desde empresas y organizaciones hasta áreas más sensibles como entidades gubernamentales o sistemas relacionados con la seguridad. No obstante, sigue existiendo una pregunta importante: ¿qué tan efectivas son realmente estas soluciones en redes actuales, donde la información cambia constantemente y seguir el rastro de los eventos puede resultar cada vez más complicado?

En la práctica, herramientas como Autopsy y MobSF se han convertido en alternativas muy utilizadas para analizar discos duros y aplicaciones móviles. Gracias a ellas, ha sido posible recuperar información importante incluso cuando se ha intentado borrar o modificar la evidencia digital para ocultar lo ocurrido (Menahil et al., 2021; Nayak et al., 2023). Por otra parte, Ghabban et al. (2021) indican que muchas herramientas forenses actuales ya no se limitan únicamente a recopilar información después de un incidente. Con el tiempo, han incorporado funciones que ayudan a identificar posibles amenazas y

a responder ante ellas mientras están ocurriendo. Esto permite que los investigadores no solo entiendan lo que ocurrió, sino que también puedan actuar más rápido para reducir el impacto del ataque y mejorar la forma en que se responde ante situaciones similares.

El uso cada vez mayor de técnicas para ocultar información digital ha hecho que muchas formas tradicionales de investigación tengan que replantearse. González Arias et al. (2024) indican que los atacantes utilizan herramientas para esconder, fragmentar o eliminar rastros de sus actividades, lo que complica el trabajo de quienes investigan estos casos. Por eso, los especialistas en análisis forense necesitan actualizarse constantemente para poder reconocer y recuperar estas evidencias de forma más efectiva. A esto se le suma que, en muchos casos, las investigaciones deben hacerse con poco tiempo, recursos limitados y cumpliendo normas legales estrictas para asegurar la cadena de custodia. En este contexto, surge una duda importante: ¿cómo se puede obtener información confiable cuando los escenarios son cada vez más complejos?

Varios autores coinciden en que el problema no se reduce solo a lo técnico, sino que también tiene que ver con la forma en que se organizan y aplican los métodos de trabajo. Akinbi (2023) señala que la aparición de redes 6G y el crecimiento acelerado de los dispositivos IoT demandan enfoques más flexibles y adaptables. De forma complementaria, Ragab et al. (2025) y Egger et al. (2025) resaltan que los modelos de aprendizaje federado pueden ayudar a analizar información desde distintos lugares sin necesidad de compartir directamente los datos originales. Esto es especialmente útil cuando se trabaja con información sensible, como la que proviene de aplicaciones móviles, redes sociales o plataformas en línea, ya que permite aprovechar los datos disponibles sin exponerlos por completo y cuidando mejor la privacidad.

No es sorprendente que, con todos estos cambios digitales, los lugares donde se hace análisis forense de redes sean cada vez más variados y difíciles de manejar. Hoy en día, la información ya no viaja solo por redes físicas tradicionales, sino también por sistemas en la nube, entornos mixtos y dispositivos que se comunican entre sí de forma automática. Este cambio ha hecho que el trabajo forense tenga que adaptarse a nuevas

formas de funcionamiento de las redes, así como a amenazas más avanzadas y difíciles de detectar. En este contexto, ÇiL & DEMİRCİ (2024) estudian cómo los cambios constantes en la forma en que se dirige el tráfico en redes SDN pueden complicar el seguimiento de lo que ocurre dentro de la red. Por su parte, Yaacoub et al. (2022) señalan que observar el tráfico en distintos niveles ayuda a detectar mejor los problemas cuando los escenarios son más complejos.

A estos cambios tecnológicos se suman desafíos operativos presentes en situaciones reales. En muchas organizaciones, la necesidad de responder rápidamente a un incidente obliga a los analistas a equilibrar la rapidez del análisis con el cumplimiento de los procedimientos necesarios para preservar la cadena de custodia (Jarrett & Choo, 2021). Así mismo Soni (2024), señalan que la automatización puede agilizar numerosas tareas, pero no sustituye completamente el criterio humano, especialmente cuando es necesario diferenciar entre actividades legítimas y comportamientos potencialmente maliciosos dentro de una red. De forma similar, Dunsin et al. (2024) sostienen que el uso de inteligencia artificial en procesos forenses debe complementarse con modelos explicables que permitan justificar y auditar cada decisión tomada por el sistema.

Un ejemplo claro de esto se ve en los ataques que afectan a sistemas de energía. En estas situaciones, la información que sirve como evidencia no siempre está en los registros habituales de los sistemas, sino que muchas veces aparece en comportamientos extraños dentro del tráfico de la red, algo que necesita herramientas específicas para poder detectarse Fakiha (2024). Esto lleva a una duda importante: ¿las herramientas que se usan hoy en día realmente están listas para identificar este tipo de ataques con precisión?, ¿cuáles son sus principales limitaciones?, y ¿qué enfoques han demostrado mejores resultados cuando se aplican a infraestructuras críticas o dispositivos con recursos limitados, como los que forman parte del ecosistema IoT?

La investigación reciente muestra un creciente interés por desarrollar marcos de trabajo capaces no solo de recopilar evidencia, sino también de organizarla, correlacionarla y priorizarla de manera eficiente. Algunos estudios, como el de Egger et al. (2025), En algunos estudios recientes también se está viendo el uso de blockchain para asegurar que la evidencia digital no se altere y se mantenga confiable. Por otro lado, Abuowaida et

al. (2025) proponen estructuras que permiten que varios equipos de investigación puedan acceder a la información al mismo tiempo sin poner en riesgo su seguridad. En esa misma línea, Jiménez et al. (2024) plantean una forma de trabajo más colaborativa, donde distintos equipos pueden coordinarse entre diferentes países o regiones mediante sistemas distribuidos, lo que ayuda a responder de manera más organizada ante incidentes complejos.

Con la creciente cantidad de dispositivos conectados y el aumento de posibles puntos vulnerables, se vuelve cada vez más necesario crear formas específicas de detección para el Internet de las Cosas (IoT). En esta línea, Alzakari et al. (2025) presentan una propuesta para identificar ataques de tipo ransomware usando modelos de aprendizaje automático. Un aspecto importante de este trabajo es que está pensado para funcionar en dispositivos con poca capacidad, donde normalmente la seguridad es más limitada. Los resultados muestran que el sistema logra detectar mejor este tipo de ataques, además de aprovechar de forma más eficiente los recursos y responder en tiempos adecuados para este tipo de entornos.

Por otra parte, la llegada de las redes 6G plantea retos distintos para el análisis forense, aunque igualmente importantes. Alqabbani et al. (2023) analizan cómo esta nueva generación de redes obliga a replantear muchas de las herramientas y métodos utilizados tradicionalmente. Hoy en día se genera una cantidad de datos muy grande y a gran velocidad, lo que hace que la información cambie y desaparezca rápidamente. Esto provoca que los métodos tradicionales ya no sean suficientes para analizar lo que ocurre en una red. Además, el uso generalizado del cifrado, la constante modificación de las redes y el hecho de que la información esté repartida en distintos lugares hacen que sea más difícil encontrar y analizar las evidencias digitales. Por eso, es necesario buscar nuevas formas de trabajo que se adapten mejor a esta realidad.

Aunque estos estudios se centran en contextos distintos, ambos llegan a una misma idea importante: la forma en que se hace el análisis forense también tiene que ir cambiando a la par de las tecnologías que intenta proteger.

Las amenazas actuales y los entornos donde se desarrollan demandan enfoques más especializados, adaptables y capaces de mantener su eficacia incluso en condiciones técnicas complejas o cambiantes.

2. Metodología

2.1. Tipo de estudio y enfoque metodológico

Este artículo surge del interés por comprender cómo se están abordando actualmente los procesos de análisis forense en redes frente a un escenario de amenazas cada vez más complejo. Con este propósito, realizamos una revisión bibliográfica de carácter cualitativo y exploratorio centrada en las técnicas y herramientas empleadas para analizar tráfico de red, identificar incidentes de seguridad y apoyar las tareas de detección y mitigación de ciberataques.

La revisión se basó en artículos científicos obtenidos de distintas bases de datos académicas, dando prioridad a trabajos que tratan sobre áreas que han cobrado importancia en los últimos años, como el Internet de las Cosas, las redes 6G, la computación en la nube y los sistemas de redes definidas por software (SDN).

La selección de estos contextos respondió a que concentran buena parte de los retos actuales de la ciberseguridad, debido a factores como la gran cantidad de dispositivos conectados, la distribución de los recursos tecnológicos y la dificultad para preservar y analizar evidencias digitales.

Al revisar y comparar los estudios seleccionados, se trató de entender qué métodos se usan con más frecuencia, qué herramientas aparecen más en la literatura y cuáles son las principales dificultades que han señalado los investigadores. Con esto fue posible tener una idea más clara de cómo está actualmente el análisis forense de redes y qué aspectos todavía se pueden mejorar o seguir desarrollando en este campo.

A diferencia de una revisión sistemática que sigue reglas muy estrictas para incluir o dejar fuera estudios, en este trabajo se eligió un enfoque más flexible. Esto permitió analizar los estudios de una forma más interpretativa, centrándose más en los temas y en lo que aportaba cada uno, en lugar de seguir únicamente criterios rígidos de

selección. Este enfoque ayudó a reconocer patrones comunes, aportes importantes y problemas que se repiten en los estudios revisados. También permitió reunir trabajos con distintos enfoques y escenarios, incluyendo propuestas sobre métodos de detección, formas de analizar incidentes y herramientas pensadas para responder a problemas de seguridad. De esta manera, se buscó obtener una visión más amplia del estado actual del análisis forense en redes y de su aplicación en entornos tecnológicos contemporáneos.

El proceso que se siguió está resumido en la Figura 1, donde se muestran las etapas principales de la revisión bibliográfica. En general, primero se buscaron las fuentes de información, luego se eligieron los estudios que eran más útiles o relevantes para el trabajo y, finalmente, se organizaron por temas. Esta forma de presentarlo en una figura ayuda a entender de manera más clara y sencilla cómo se fue realizando todo el proceso y cómo se estructuró el análisis de la información.

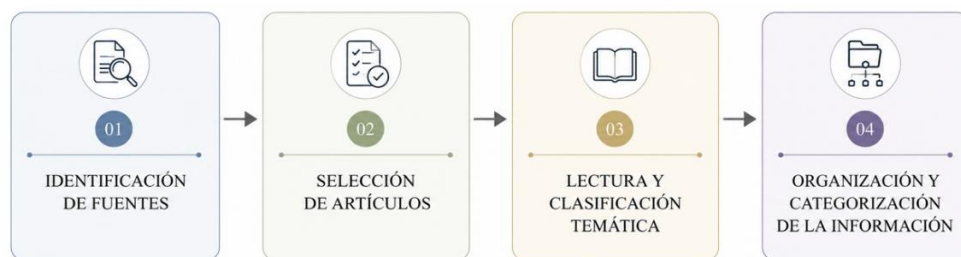


Figura 1. Representación del enfoque adoptado para la revisión y análisis de la literatura científica.

2.2. Estrategia de búsqueda y selección de documentos

La recopilación de información se realizó entre mayo y junio de 2025 mediante la consulta de bases de datos académicas ampliamente utilizadas en el ámbito científico, para realizar la búsqueda de información se utilizaron varias bases de datos académicas como Google Scholar, IEEE Xplore, SpringerLink, ScienceDirect, MDPI y Taylor & Francis. La revisión se hizo con términos en inglés y español relacionados con el análisis forense de redes, por ejemplo: “network forensics”, “detección de ciberataques”, “evidencia digital”, “forense en SDN”, “herramientas forenses en IoT”, “forense en la nube” y “seguridad con aprendizaje automático”.

Para elegir los estudios se tomaron en cuenta trabajos científicos revisados por otros expertos, publicados entre 2020 y 2024, que se pudieran leer completos y que trataran sobre técnicas, métodos o herramientas usadas en el análisis del tráfico de red. En especial, se incluyeron aquellos que estuvieran relacionados con la detección, reducción o respuesta frente a incidentes de ciberseguridad. Se excluyeron trabajos duplicados, investigaciones centradas en ámbitos ajenos al análisis forense de redes y publicaciones que no contaban con respaldo académico verificable.

Los criterios de inclusión y exclusión aplicados se presentan en la Tabla 1. Tras el proceso de revisión, se seleccionaron 22 artículos que cumplieran con las condiciones establecidas. Posteriormente, estos estudios fueron organizados considerando aspectos como la técnica forense analizada, las herramientas empleadas, el entorno tecnológico de aplicación y el nivel de automatización incorporado en cada propuesta.

Tabla 1. Criterios de inclusión utilizados

Base de datos	Tipo de publicación	Año de publicación	Criterios de inclusión principales
Google Scholar	Artículos científicos	2020–2024	Técnicas y herramientas forenses aplicadas a redes.
IEEE Xplore	Revistas y conferencias	2020–2024	Enfoque técnico y casos prácticos sobre análisis forense.
ScienceDirect	Artículos académicos	2020–2024	Estudios con experimentación en entornos reales o simulados.
SpringerLink	Libros y artículos	2020–2024	Estudios de revisión con cobertura tecnológica actualizada.
Taylor & Francis	Artículos científicos	2020–2024	Publicaciones indexadas con enfoque en seguridad y ciberforense.

2.3. Organización y categorización de la información recopilada

Una vez seleccionados los artículos, se realizó una lectura detallada de cada estudio con el propósito de identificar sus principales aportes y características. Este análisis ayudó

a ver qué cosas tenían en común los distintos estudios revisados y en qué se diferenciaban. Con eso fue más fácil organizarlos y usarlos como base para seguir desarrollando el trabajo.

Para organizar mejor la información que se recopiló, se usaron cuatro aspectos principales. Primero, se revisó qué tipo de técnica forense trataba cada estudio. Luego, se anotaron las herramientas que se usaban o que proponían los autores. También se tomó en cuenta el entorno donde se aplicaban estas soluciones, como el Internet de las Cosas (IoT), la nube, las redes SDN o las redes 6G. Por último, se observó si las propuestas eran más automáticas o no, es decir, si utilizaban inteligencia artificial, aprendizaje automático o sistemas distribuidos para ayudar en el análisis.

Con base en los criterios definidos, los estudios elegidos se organizaron en tres grupos principales que sirven como guía para este trabajo. El primero incluye los trabajos que tratan sobre las técnicas usadas para analizar redes. El segundo reúne los estudios enfocados en las herramientas que ayudan a detectar o reducir ataques. Y el tercero recoge los problemas y dificultades que se han encontrado al aplicar estas soluciones en situaciones reales.

Para ordenar mejor la información revisada, se creó una tabla comparativa donde se reunieron datos como el objetivo de cada estudio, cómo se realizó, qué resultados principales se encontraron y qué limitaciones mencionaron los propios autores. Esto ayudó bastante a comparar los trabajos entre sí y a notar patrones, similitudes y también puntos que todavía necesitan más investigación. En la Figura 2 se muestra de manera resumida cómo se organizaron estas categorías para el análisis de los artículos seleccionados.

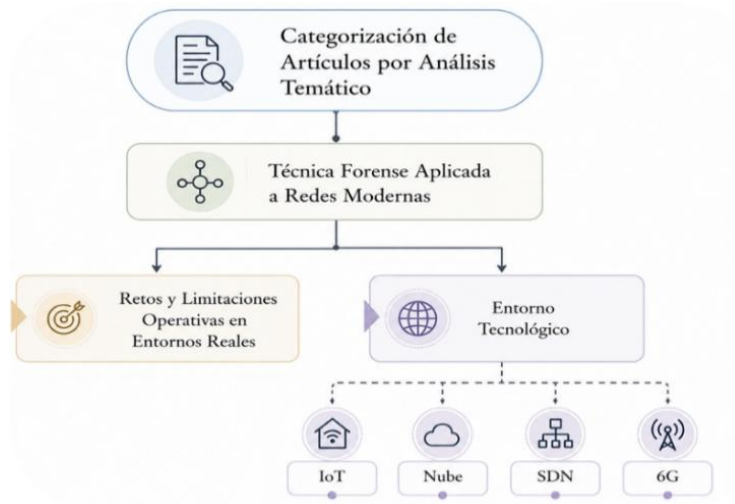


Figura 2. Estructura de categorización de artículos para el análisis temático.

3. Resultados

3.1. Principales técnicas forenses identificadas en redes

La revisión de los estudios seleccionados permitió identificar diversas técnicas forenses empleadas en el análisis del tráfico de red. Estas técnicas han sido desarrolladas y adaptadas para entornos tecnológicos con características diferentes, entre ellos el Internet de las Cosas (IoT), las redes 6G, la computación en la nube y las arquitecturas basadas en Software Defined Networking (SDN). Aunque todas estas propuestas tienen el mismo objetivo de ayudar a detectar incidentes de seguridad y entender lo que ocurrió durante un ataque, no todas funcionan de la misma manera. Algunas son más automáticas que otras, algunas permiten un análisis más profundo, y otras requieren más conocimientos técnicos para poder utilizarlas. También varían según el tipo de entorno en el que pueden aplicarse.

Los estudios revisados dejan ver que la técnica forense que se utiliza no siempre es la misma, sino que depende mucho del entorno en el que se aplica. Aspectos como la cantidad de tráfico que maneja la red, los recursos disponibles, la facilidad o dificultad para acceder a la información y lo compleja que sea la infraestructura influyen bastante en qué tan bien funciona cada método en la práctica.

Dentro de las técnicas que más se mencionan en los estudios, una de las más usadas en redes tradicionales es la inspección profunda de paquetes (Deep Packet Inspection,

DPI). Este método permite mirar no solo los datos básicos que se mueven por la red, sino también lo que llevan dentro, lo que ayuda a entender mejor lo que está pasando y a notar cuando algo no parece normal. Sin embargo, cuando se usa en entornos como el Internet de las Cosas (IoT), surgen varios problemas, ya que muchos dispositivos no tienen la capacidad necesaria para manejar o almacenar tanta información, lo que dificulta mantener este tipo de revisión de manera continua.

Ante estas limitaciones, algunos estudios proponen el uso de métodos basados en NetFlow, que en lugar de analizar todo el contenido de los datos, se centran solo en información resumida del tráfico. Esto ayuda a reducir el uso de recursos y a crear una especie de “perfil” del comportamiento de la red para detectar cuando algo no encaja. Según lo señalado por Qureshi et al. (2021) y Ghabban et al. (2021), estas ventajas han hecho que este enfoque sea más utilizado en situaciones donde es importante ahorrar recursos y mantener el sistema funcionando de forma eficiente.

Las investigaciones relacionadas con redes 6G muestran una creciente incorporación de técnicas basadas en inteligencia artificial para el análisis forense del tráfico. Entre los métodos más usados están aquellos que aprenden a partir de ejemplos previos, como los árboles de decisión, Random Forest y redes neuronales convolucionales. Estas técnicas se entrenan para reconocer patrones que pueden estar relacionados con comportamientos extraños o sospechosos (Abuowaida et al., 2025; Dunsin et al., 2024).

Los estudios revisados indican que estos modelos necesitan primero aprender a partir de ejemplos ya clasificados para poder funcionar bien. Aunque esto requiere una preparación inicial, luego permiten automatizar muchas tareas y manejar grandes cantidades de información, algo especialmente útil cuando hay mucho tráfico o cuando los datos viajan protegidos. También se ha visto su uso en entornos con varios servicios en la nube, donde la información está repartida y los diferentes formatos dificultan entender y relacionar lo que ocurre en un incidente de seguridad.

Como se detalla en la Tabla 2, las técnicas forenses quedan organizadas según tres criterios: su adecuación al entorno tecnológico, el grado de automatización que ofrecen y los principales retos operativos que conllevan. Esta síntesis estructurada deja a la vista

las ventajas y limitaciones de cada enfoque, y puede servir de referencia a quienes deban elegir una metodología acorde a sus necesidades.

Tabla 2. Comparación de técnicas forenses en redes según el entorno tecnológico y grado de automatización

Técnica forense	Entorno más aplicado	Nivel de automatización	Ventaja principal	Limitación destacada
Deep Packet Inspection (DPI)	Redes tradicionales, IoT	Bajo	Análisis profundo del contenido	Alto consumo de recursos
NetFlow Forensics	IoT, Nube	Medio	Perfilado de tráfico ligero	Limitado sin carga útil
Árboles de decisión	6G, Multinube	Alto	Clasificación rápida de eventos	Requiere entrenamiento supervisado
Seguimiento de rutas SDN	SDN	Medio	Precisión en reconstrucción de eventos	Dependencia del controlador central
Análisis de tráfico cifrado	Nube, 6G	Bajo	Identificación sin descifrar	Baja precisión si los patrones no son claros

Comparar estos enfoques deja una conclusión clara: ninguno funciona igual de bien en todos los escenarios. Cada técnica equilibra de forma distinta precisión, escalabilidad, exigencias computacionales y aplicabilidad práctica, y por eso elegir la más adecuada depende del contexto de los recursos con que se cuenta y de la naturaleza del incidente que se investiga. En definitiva, lo que separa un análisis exitoso de uno inconcluso suele ser qué tan bien se ajusta la técnica elegida a las condiciones reales del entorno forense.

3.2. Herramientas de análisis forense digital aplicadas a entornos reales

El análisis detallado de los artículos deja ver un grupo heterogéneo de herramientas forenses orientadas al estudio de redes, elegidas no únicamente por su potencia técnica sino por su capacidad de adaptarse al entorno donde se usan. Una red física tradicional, una arquitectura SDN y una nube híbrida operan bajo reglas distintas, con limitaciones y desafíos propios de cada caso. Ante esta variedad de opciones, los investigadores y especialistas suelen escoger, adaptar o incluso crear sus propias herramientas según lo que necesiten, tratando de encontrar un equilibrio entre que sean fáciles de usar, que funcionen bien, que se ajusten a distintos casos y, en algunos casos, que no resulten costosas.

Los dispositivos IoT suelen tener poca capacidad y recursos limitados, lo que hace que las herramientas forenses tradicionales tengan muchas dificultades para funcionar bien en estos entornos.

Wireshark y Tcpdump mantienen su uso para la captura y visualización de tráfico, aunque las restricciones del hardware afectan su efectividad en estos entornos. Como respuesta a esa limitación ha surgido IoTScope, una solución más ligera que permite el monitoreo no intrusivo: observar comportamientos anómalos sin instalar agentes en los dispositivos, algo que muchas veces resultaría inviable o riesgoso (Zhang, 2024). El patrón se repite: mientras más restringidos son los recursos disponibles, más ingenio exigen las soluciones desarrolladas.

En la computación en la nube el panorama cambia por completo. El consumo de recursos deja de ser el problema central; lo que preocupa ahora es la volatilidad de los datos, la fragmentación entre contenedores y la urgencia de actuar antes de que la evidencia se pierda. FTK Imager Cloud y X-Ways Forensics se han consolidado como herramientas confiables para examinar entornos virtuales y recuperar datos en medio de sistemas distribuidos. Autopsy, por su parte, nació para el análisis forense de sistemas físicos pero se ha reinventado: ahora se adapta a estructuras remotas y automatiza parcialmente tareas repetitivas, una cualidad apreciada en investigaciones con poco personal o plazos ajustados (Abuowaida et al., 2025; Nayak et al., 2023).

La forma centralizada en que funcionan las redes definidas por software (SDN) tiene dos caras. Por un lado, facilita el acceso a información detallada desde distintos puntos de la red, lo que permite usar herramientas como FlowRadar, que pueden guardar y recuperar información del tráfico sin afectar demasiado el rendimiento. Por otro lado, esta misma estructura implica una mayor responsabilidad en el manejo de esa información.

Gracias a esa capacidad ha sido posible detectar ataques de intermediario (man-in-the-middle), alteraciones en rutas o saturación maliciosa de conmutadores, reconstruyendo eventos casi en tiempo real y con un nivel de detalle difícil de igualar en otros entornos (Nayak et al., 2023). De forma paralela, también se han creado módulos para tareas forenses que se integran directamente en los controladores OpenFlow. Esto ayuda a que la respuesta sea más rápida y permite tener una mejor visión de lo que está pasando en el tráfico de la red.

La inteligencia artificial también se está usando en este campo. El análisis forense digital ya no solo se basa en guardar y revisar lo que pasó, sino que empieza a apoyarse en sistemas que aprenden de los datos para intentar identificar comportamientos extraños o patrones que una persona podría no notar fácilmente. TensorFlow Forensics y los entornos personalizados en Jupyter Notebook permiten entrenar modelos para clasificar tráfico, también se pueden separar eventos, o relacionar distintos incidentes a partir de cómo van ocurriendo en el tiempo.

Como se observa en la Figura 3, este conjunto de herramientas apunta hacia soluciones modulares, escalables y preparadas para la automatización, en sintonía con los retos actuales del tráfico cifrado, los sistemas híbridos y las arquitecturas fragmentadas. Lejos de debilitar el campo, esa fragmentación parece haberlo empujado a evolucionar: ya no se persigue una herramienta todopoderosa, sino un repertorio flexible capaz de adaptarse a distintos frentes y escenarios. El análisis forense en redes, en consecuencia, avanza menos hacia una solución única y más hacia una estrategia plural.

	Captura de tráfico	Análisis	Automatización	Visualización
IoT	Wireshark	Tcpdump	IoTScope	Sin herramienta específica
Nube	Sin herramienta específica	FTK Imager Cloud	Autopsy	X-Ways Forensics
SDN	Sin herramienta específica	Módulo forense OpenFlow	FlowRadar	Sin herramienta específica
IA	TensorFlow Forensics	Jupyter Notebook	Sin herramienta específica	Sin herramienta específica
	 Captura y análisis de tráfico		 Automatización de tareas forenses	
	 Modelo de aprendizaje automático		 Sin herramienta consolidada reportada	

Figura 3. Herramientas forenses según entorno tecnológico y tipo de funcionalidad principal.

3.3. *Análisis comparativo de enfoques en distintos escenarios de red*

No existe, según la literatura revisada, una metodología única que sirva para todo el análisis forense de redes. Una técnica puede rendir muy bien en entornos controlados, centros de datos físicos, sin embargo, mostrar limitaciones serias al trasladarse a la nube o al ecosistema IoT, escenarios menos predecibles y más fragmentados. Esa variabilidad no es solo un rasgo de cada infraestructura: también obliga a quienes investigan a replantear su enfoque de forma constante, ajustándolo a las limitaciones físicas, lógicas y operativas propias de cada entorno.

La debilidad de las redes IoT es uno de los grandes retos en este campo, ya que muchos dispositivos tienen muy poca capacidad para procesar información, usan sistemas que no siempre se entienden entre sí y además no existe un acuerdo común sobre cómo deben funcionar o comunicarse.

Recuperar un registro, tarea sencilla en otras redes, puede resultar imposible aquí muchos dispositivos simplemente no los generan, o los conservan solo de forma efímera. Esa limitación ha llevado a la estrategia forense a desplazarse hacia puntos intermedios, como las puertas de enlace o los routers domésticos, desde donde sí es posible interceptar tráfico en tiempo real y construir patrones de comportamiento

anómalo a partir de lo capturado. El método ha probado su eficacia para identificar ataques de denegación de servicio y rastrear redes de bots formadas por dispositivos cotidianos, tal como lo muestran simulaciones recientes en entornos realistas (Zhang, 2024).

Las redes 6G siguen siendo, en gran medida, un terreno experimental donde la mayoría de soluciones aún no salen del laboratorio. Aquí los problemas se multiplican: baja latencia, movilidad extrema y un cifrado cada vez más fuerte hacen que el análisis convencional pierda eficacia. Ante esto, la investigación ha empezado a centrarse en métodos que intentan entender lo que ocurre a partir de información básica de los datos, sin necesidad de acceder directamente al contenido que va cifrado. Para ello se usan sistemas distribuidos que ayudan a relacionar esa información y detectar comportamientos extraños casi en el momento en que ocurren. Aunque estas ideas resultan prometedoras, también generan dudas importantes, especialmente en lo relacionado con la privacidad, ya que no todo puede ser observado libremente. Además, la información que se obtiene puede no ser del todo clara y a veces es difícil de comprobar de la misma forma en distintos casos.

Uno de los problemas más importantes en la computación en la nube es que los datos no están en un solo lugar, sino repartidos en diferentes servidores. Además, muchas veces esa información está dentro de máquinas virtuales que pueden crearse y eliminarse en muy poco tiempo. Los estudios revisados coinciden en que no es suficiente con analizar una sola parte del sistema, sino que es necesario usar herramientas que permitan ver lo que ocurre en varias capas a la vez y así poder reconstruir con más claridad el orden en que sucedieron los eventos.

Esa mirada de conjunto ha permitido esclarecer incidentes como accesos no autorizados, escaladas de privilegios o fugas de datos sensibles que, sin ella, quedarían enterrados entre millones de líneas de código y paquetes de red efímeros.

Para entender mejor estas diferencias, se muestra la Tabla 3, donde se comparan aspectos importantes como qué tan fácil es acceder a la evidencia, desde dónde se puede obtener la información y qué tan bien funcionan las herramientas automáticas en

cada caso. Esta tabla ayuda a resumir de forma clara los principales retos que presenta cada tipo de entorno. Este recurso ofrece una visión sintética pero precisa de los retos que impone cada tipo de infraestructura.

Tabla 3. Comparativa de desafíos y estrategias forenses según entorno tecnológico.

Entorno	Evidencia disponible	Punto de captura recomendado	Automatización viable	Desafíos clave
IoT	Limitada y volátil	Gateway, router intermedio	Parcial	Dispositivos cerrados, protocolos diversos
Nube	Distribuida, logs dispersos	Hypervisor, contenedores	Alta	Acceso limitado al hardware
Redes SDN	Metadatos de flujo	Controlador OpenFlow	Alta	Latencia de análisis en tiempo real
6G	Metadatos cifrados	Sensores distribuidos	Baja	Cifrado, movilidad, privacidad de usuarios

La Tabla 3 muestra que ningún entorno comparte el mismo perfil de evidencia, punto de captura o nivel de automatización viable. IoT y redes 6G presentan los niveles más bajos de automatización, mientras que nube y SDN concentran la mayor parte de las soluciones automatizadas disponibles en la literatura revisada.

3.4. Identificación de brechas y áreas de mejora

La revisión de la literatura permitió identificar cuatro hallazgos recurrentes relacionados con las brechas y limitaciones operativas del análisis forense en redes: restricciones de interoperabilidad entre soluciones, dificultades para preservar la cadena de custodia digital en entornos virtualizados, una dependencia persistente del juicio humano dentro

de procesos parcialmente automatizados, y una desarticulación entre los procesos técnicos forenses y los marcos legales que deben sostenerlos.

El primer punto importante tiene que ver con que no todas las plataformas funcionan igual entre sí, sobre todo cuando se usan varios servicios en la nube al mismo tiempo. Ghabban et al. (2021) señalan que cada proveedor maneja de forma distinta el acceso a los datos, cuánto tiempo los guarda y qué tanto se pueden ver. Por esta razón, cuando una investigación involucra más de un proveedor, se vuelve complicado unir la información obtenida de cada uno, lo que hace que el análisis del caso se vuelva más fragmentado.

El segundo hallazgo corresponde a la preservación de la cadena de custodia en sistemas virtualizados. Entre las soluciones reportadas figura el uso de blockchain para sellar digitalmente la evidencia, enfoque que Egger et al. (2025) desarrollan en el contexto de esquemas de aprendizaje federado orientados a preservar la privacidad de los datos durante el proceso de verificación. También se reportan técnicas de hashing distribuido para comprobar que la evidencia recolectada no ha sido alterada. Sin embargo, la mayoría de los estudios coinciden en que, aunque estas soluciones existen, en la práctica todavía se usan poco en entornos reales donde se necesita que funcionen de forma continua.

El tercer hallazgo tiene que ver con qué tanto del proceso forense se realiza de forma automática. Aquí se nota que hay una diferencia entre automatizar solo algunas tareas específicas y automatizar todo el proceso de investigación de principio a fin. Por ejemplo, las técnicas mencionadas antes, como los árboles de decisión usados en redes 6G, logran un alto nivel de automatización, sobre todo en la parte donde se clasifican los eventos (Tabla 2).

No obstante, la literatura reporta que la validación de hallazgos y la interpretación de patrones complejos continúan requiriendo intervención humana. Soni (2024), Jarrett & Choo (2021) documentan esta dependencia al señalar que la automatización no sustituye por completo el criterio del analista cuando se trata de distinguir tráfico legítimo de comportamientos sospechosos en redes empresariales. En esta misma

línea, Dunsin et al. (2024) reportan una tendencia creciente a incorporar modelos explicativos en las soluciones de inteligencia artificial aplicadas a forensia digital, con el fin de que cada inferencia generada por el sistema pueda ser auditada por un investigador humano.

El cuarto hallazgo tiene que ver con la falta de conexión entre el trabajo técnico de la investigación forense y los pasos legales que deberían acompañarlo. Jiménez et al. (2024) señalan que, en sistemas definidos por software, las tareas de análisis forense y la respuesta ante incidentes suelen realizarse por separado, lo que complica entender con claridad el origen real de un ataque. Esto se vuelve aún más delicado cuando el incidente puede terminar en un proceso legal contra los responsables. Esta desarticulación se observa de forma puntual en el contexto de SDN documentado por los autores, sin que ninguno de los estudios revisados aborde de manera sistemática la heterogeneidad de los marcos normativos entre distintos países, aspecto que el conjunto de la literatura analizada deja, por ahora, sin resolver.

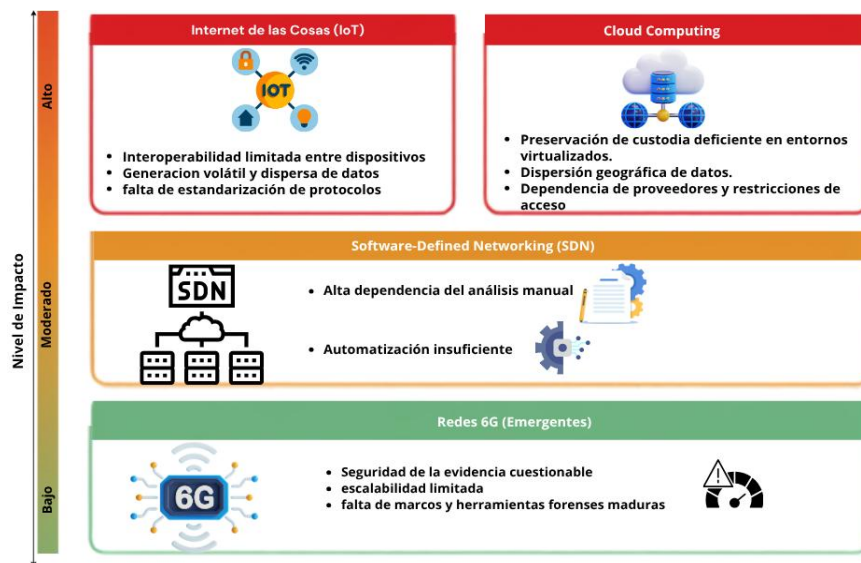


Figura 4. Mapa de brechas comunes en el despliegue de técnicas forenses en redes.

4. Discusión

Lo que muestran los resultados sobre técnicas forenses no es solo una lista de opciones disponibles, sino una tensión que atraviesa todo el campo: a mayor profundidad de análisis, mayor demanda de recursos, y eso limita seriamente lo que es posible hacer en

entornos como IoT. La inspección profunda de paquetes funciona bien en redes tradicionales, pero en dispositivos con capacidad de procesamiento reducida su rendimiento cae de forma considerable, algo que Akinbi (2023), ya planteaba al advertir que los marcos metodológicos heredados simplemente no escalan hacia ecosistemas de bajo consumo. NetFlow forensics alivia esa limitación al trabajar con metadatos de flujo, pero lo hace sacrificando profundidad. No es una solución, es un compromiso. Las técnicas de aprendizaje supervisado usadas en redes 6G y en la nube son las que muestran un mayor nivel de automatización según la literatura, algo que ya había sido señalado por Qureshi et al. (2021) respecto al uso del aprendizaje automático en la forensia. Sin embargo, esta automatización se limita sobre todo a la clasificación de eventos, y no llega a cubrir la verificación ni la interpretación de los resultados. Mezclar estos aspectos podría llevar a pensar que el proceso forense está más avanzado de lo que realmente está. En el caso de SDN, el seguimiento de rutas aprovecha la arquitectura centralizada para recolectar registros con eficiencia, pero esa misma centralización introduce una dependencia del controlador que ÇiL & DEMİRCİ (2024) documentan con detalle al comparar distintos controladores en términos de sus capacidades forenses.

En cuanto al ecosistema de herramientas, lo que la revisión deja ver no es una fragmentación accidental sino una tendencia deliberada hacia soluciones especializadas por entorno. Ghabban et al. (2021) Esto ya se venía mencionando al comparar distintas herramientas forenses de red: existen muchas soluciones especializadas, pero todavía falta una forma común que permita que todas trabajen de manera más integrada. El caso de Autopsy es un buen ejemplo de esto, ya que aunque fue creada inicialmente para analizar sistemas físicos, con el tiempo ha logrado adaptarse a entornos remotos y a la nube. Esto muestra que la utilidad de una herramienta no depende solo de cómo fue diseñada al inicio, sino también de su capacidad para ir cambiando y ajustándose a las necesidades del área, como señalan Zareen et al. (2024) y confirman Nayak et al. (2023) al valorar su automatización parcial en contextos con recursos humanos limitados. Algo similar ocurre con el análisis de tráfico cifrado: en lugar de intentar descifrar, los investigadores han aprendido a inferir. (Abd Elmonsef Sarhan et al. (2023) muestran que es posible extraer patrones útiles de

mensajería instantánea y VoIP sin romper el cifrado de extremo a extremo, y Alqabbani et al. (2023) advierten que en redes 6G esa lógica no es una opción más entre varias sino una condición de viabilidad.

Las brechas que emergen del análisis no son fallas puntuales de herramientas concretas; son limitaciones que se repiten en distintos entornos y que apuntan a problemas más profundos. La interoperabilidad sigue siendo un obstáculo real, especialmente en entornos multinube donde cada proveedor aplica sus propias políticas de acceso y retención de datos, fragmentando la evidencia antes de que pueda integrarse en una sola investigación. La cadena de custodia en sistemas virtualizados presenta desafíos similares: se han propuesto mecanismos como blockchain o hashing distribuido para verificar la integridad de la evidencia, siguiendo la línea de lo que documentan Egger et al. (2025) en los esquemas de aprendizaje federado todavía se está explorando su uso, pero en la práctica su adopción es baja porque puede exigir demasiados recursos de procesamiento, algo que no siempre es posible en entornos reales. A pesar del avance de la automatización, el criterio humano sigue siendo necesario. Como señalan Jarrett & Choo (2021) y Soni (2024) estas herramientas ayudan a acelerar el trabajo, pero no reemplazan la capacidad del analista para entender el contexto y diferenciar lo que es normal de lo que puede ser sospechoso. Además, Dunsin et al. (2024) añaden un punto importante: si los resultados de estos sistemas van a usarse en un proceso legal, no basta con que sean precisos, también deben poder explicarse de forma clara. Finalmente, Jiménez et al. (2024) muestran que, en el caso de las redes SDN, sigue existiendo una separación entre el análisis técnico y los procedimientos legales, lo que dificulta asignar responsabilidades cuando un incidente termina teniendo consecuencias judiciales.

En conjunto, estos resultados muestran algo que va más allá de las herramientas en sí: el análisis forense de redes todavía tiene un retraso importante en la parte legal y organizativa, algo que no se soluciona únicamente con mejoras técnicas. También es importante mencionar algunas limitaciones de este trabajo. Al tratarse de una revisión con un enfoque más interpretativo, se priorizó comprender a fondo los estudios en lugar de abarcar todo lo publicado. Además, la búsqueda se centró en artículos entre 2020 y 2024 en seis bases académicas, por lo que quedaron fuera documentos técnicos de la

industria que, aunque no siempre son revisados por pares, suelen mostrar de forma más rápida cómo se están usando realmente estas herramientas en la práctica. Por eso, las comparaciones presentadas deben entenderse como una guía de tendencias generales y no como resultados obtenidos a partir de pruebas directas entre herramientas.

5. Conclusiones

Esta revisión muestra que el análisis forense de redes ha ido avanzando, pero no de la misma manera en todos los aspectos. Por un lado, las herramientas y métodos técnicos han mejorado bastante y ahora permiten detectar y reconstruir mejor los ataques. Sin embargo, ese progreso no se refleja igual en la parte práctica, legal ni en el trabajo humano que hay detrás. Muchas de las técnicas actuales ya automatizan tareas concretas, como ordenar o clasificar eventos, pero todavía es el analista quien debe revisar, interpretar y dar sentido a los resultados. Esta diferencia es importante para entender realmente en qué punto se encuentra el desarrollo de esta área.

Este trabajo deja tres ideas principales. La primera es que los problemas encontrados, como la poca compatibilidad entre herramientas, las dificultades para conservar correctamente la evidencia, la dependencia del criterio del analista y la falta de conexión entre lo técnico y lo legal, no son casos aislados, sino situaciones que se repiten en distintos entornos como IoT o redes 6G. La segunda es que la gran cantidad de herramientas distintas que existen no es un problema menor, sino una muestra de que cada entorno está desarrollando sus propias soluciones, lo que hace necesario avanzar hacia formas más comunes de trabajo que permitan integrarlas mejor. La tercera es que muchas veces no se le da suficiente importancia al aspecto legal: una investigación puede ser correcta desde lo técnico, pero perder fuerza si no puede sostenerse en un juicio, sobre todo cuando las leyes cambian según el país o la jurisdicción.

Estos resultados se relacionan directamente con el objetivo que se planteó al inicio del estudio, que era analizar las herramientas, los métodos y los problemas que aún persisten en el análisis forense aplicado a IoT, la nube, SDN y redes 6G. La revisión muestra que esos vacíos realmente existen y que no se pueden resolver por separado. Hace falta una visión más completa, donde el avance de la tecnología vaya acompañado

del fortalecimiento del trabajo humano y de reglas más claras y parecidas entre sí, en lugar de seguir avanzando cada uno por su lado.

A partir de estas conclusiones, también se pueden plantear algunas ideas para trabajos futuros. La primera tiene que ver con crear reglas comunes que permitan juntar la información obtenida en distintas plataformas de la nube sin que pierda valor como evidencia, en lugar de seguir desarrollando soluciones separadas para cada proveedor. La segunda se centra en mejorar los mecanismos que aseguran que la información no se altere, como el uso de blockchain o técnicas similares, pero buscando que no consuman tantos recursos y puedan usarse más fácilmente en la práctica. Una tercera línea, de carácter más jurídico que técnico, debería orientarse a evaluar modelos de cooperación legal entre jurisdicciones que acompañen el desarrollo de arquitecturas distribuidas, como SDN o IoT, de forma que la validez legal de la evidencia no dependa exclusivamente del país donde esta fue recolectada.

En definitiva, avanzar en el análisis forense de redes no depende únicamente de mejores algoritmos. Requiere una articulación más deliberada entre el desarrollo técnico, la formación de analistas capaces de interpretar lo que la automatización no resuelve, y marcos legales que acompañen, en lugar de rezagarse frente al ritmo de las amenazas digitales actuales.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Financiamiento

Este trabajo no fue financiado por ninguna organización u empresa.

Declaración sobre inteligencia artificial

Los autores declaran que se utilizaron herramientas de inteligencia artificial generativa para los siguientes fines: Traducción del resumen, mejora de redacción. Los autores asumen la plena responsabilidad del contenido del manuscrito.

Aporte de los autores

Leonidas Antonio Inca Portilla: Coordinación general, redacción de la introducción, búsqueda bibliográfica, análisis bibliográfico, análisis comparativo de escenarios.

Ronaldo Steven Rosales Espinoza: Búsqueda bibliográfica, redacción de resultados, análisis crítico de hallazgos, redacción de la discusión y conclusiones.

Ana Maria Ruiz Alcivar: Diseño metodológico, estrategia de búsqueda, selección de artículos, clasificación y categorización de la información.

Nayelhy Marisol Ponce Cabrera: Redacción de resultados, análisis de técnicas forenses, análisis de herramientas, análisis comparativo de enfoques.

Referencias

Abd Elmonsef Sarhan, S., Youness, H. A., & Bahaa-Eldin, A. M. (2023). A framework for digital forensics of encrypted real-time network traffic, instant messaging, and VoIP application case study. *Ain Shams Engineering Journal*, 14(9), 102069. <https://doi.org/10.1016/j.asej.2022.102069>

Abuowaida, S., Owida, H. A., Mohammad, S. I. S., Alshdaifat, N., Elsoud, E. A., Alazaidah, R., Vasudevan, A., & Alshurideh, M. T. (2025). Evidence Detection in Cloud Forensics: Classifying Cyber-Attacks in IaaS Environments using machine learning. *Data and Metadata*, 4, 699–699. <https://doi.org/10.56294/dm2025699>

Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. *WIREs Forensic Science*, 5(6), e1496. <https://doi.org/10.1002/wfs2.1496>

Alqabbani, A., Saleem, K., & Almazyad, A. S. (2023). Digital Communication Forensics in 6G and beyond Networks. *Applied Sciences*, 13(19), 10861. <https://doi.org/10.3390/app131910861>

Alzakari, S. A., Aljebreen, M., Ahmad, N., Alhashmi, A. A., Alahmari, S., Alrusaini, O., Al-Sharafi, A. M., & Almukadi, W. S. (2025). An intelligent ransomware based cyberthreat detection model using multi head attention-based recurrent neural networks with optimization algorithm in IoT environment. *Scientific Reports*, 15(1), 8259. <https://doi.org/10.1038/s41598-025-92711-4>

ÇiL, A., & DEMİRCİ, M. (2024). A comparative analysis of software-defined network controllers in terms of network forensics processes and capabilities. *Sigma Journal of Engineering and Natural Sciences – Sigma Mühendislik ve Fen Bilimleri Dergisi*, 42(2), 425–437. <https://doi.org/10.14744/sigma.2022.00107>

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, 48, 301675. <https://doi.org/10.1016/j.fsidi.2023.301675>

Egger, M., Urbanke, R. L., & Bitar, R. (2025). Federated One-Shot Learning With Data Privacy and Objective-Hiding. *IEEE Transactions on Information Forensics and Security*, 20, 5166–5180. <https://doi.org/10.1109/TIFS.2025.3570132>

Fakiha, B. (2024). Investigating the Secrets, New Challenges, and Best Forensic Methods for Securing Critical Infrastructure Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 15(1), 104–114. <https://doi.org/10.58346/JOWUA.2024.11.008>

Ghabban, F. M., Alfadli, I. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021). Comparative Analysis of Network Forensic Tools and Network Forensics Processes. 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 78–83. <https://doi.org/10.1109/ICSCEE50312.2021.9498226>

González Arias, R., Bermejo Higuera, J., Rainer Granados, J. J., Bermejo Higuera, J. R., & Sicilia Montalvo, J. A. (2024). Systematic Review: Anti-Forensic Computer Techniques. *Applied Sciences*, 14(12), 5302. <https://doi.org/10.3390/app14125302>

Jarrett, A., & Choo, K.-K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science*, 3(6), e1418. <https://doi.org/10.1002/wfs2.1418>

Jiménez, M. B., Fernández, D., Eduardo Rivadeneira, J., & Flores-Moyano, R. (2024). A Filtering Model for Evidence Gathering in an SDN-Oriented Digital Forensic and Incident

Response Context. IEEE Access, 12, 75792–75808.
<https://doi.org/10.1109/ACCESS.2024.3405588>

Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W. B., Mansoor, K., & Rubab, S. (2021). Forensic Analysis of Social Networking Applications on an Android Smartphone. *Wireless Communications and Mobile Computing*, 2021(1), 5567592.
<https://doi.org/10.1155/2021/5567592>

Nayak, S. C., Tiwari, V., & Samanthula, B. K. (2023). Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), 0605–0611. <https://doi.org/10.1109/CCWC57344.2023.10099169>

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 12(5).
<https://doi.org/10.14569/IJACSA.2021.01205103>

Ragab, M., Ashary, E. B., Alghamdi, B. M., Aboalela, R., Alsaadi, N., Maghrabi, L. A., & Allehaibi, K. H. (2025). Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. *Scientific Reports*, 15(1), 4470. <https://doi.org/10.1038/s41598-025-88843-2>

Soni, N. (2024). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. *Computer and Telecommunication Engineering*, 2(4), 3070. <https://doi.org/10.54517/cte3070>

Waseem, Q., Alshamrani, S. S., Nisar, K., Wan Din, W. I. S., & Alghamdi, A. S. (2021). Future Technology: Software-Defined Network (SDN) Forensic. *Symmetry*, 13(5), 767. <https://doi.org/10.3390/sym13050767>

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, 19, 100544. <https://doi.org/10.1016/j.iot.2022.100544>

Zareen, M. S., Aslam, B., Tahir, S., Rasheed, I., & Khan, F. (2024). Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit. *Computers*, 13(12), 333. <https://doi.org/10.3390/computers13120333>

Zhang, H. (2024). Simulation of network forensics model based on wireless sensor networks and inference technology. *Measurement: Sensors*, 34, 101261. <https://doi.org/10.1016/j.measen.2024.101261>