# ABSTRAK

Peningkatan penggunaan aplikasi *Instant Messenger* (IM) seperti *WhatsApp, Line, Telegram,* dan *Facebook Messenger* meningkatkan risiko kejahatan digital. Aplikasi ini sering digunakan dalam aktivitas kriminal, sehingga diperlukan analisis bukti digital yang dapat mengungkap jejak yang tersisa di perangkat *Android*. Penelitian ini mengatasi keterbatasan penelitian sebelumnya yang hanya membandingkan fungsi aplikasi, tanpa mendalami analisis forensik dalam menghadapi tantangan keamanan terbaru. Penelitian ini menerapkan metode *National Institute of Standards and Technology* 800-101 Revisi 1 dengan simulasi 7 skenario yang berfokus pada penghilangan atau menghapus bukti digital. Menerapkan starategi dengan melakukan kombinasi *tools* forensik yang digunakan seperti *Magisk, Swift Backup*, *Magnet Axiom, Mobiledit Forensic* dan alat untuk melihat *database* menggunakan *SQLite Studio* dan *Hex Editor*. Hasil setiap aplikasi menunjukkan tingkat kerentanan yang berbeda, hasil menunjukkan bahwa dari 28 percobaan, sebanyak 24 bukti digital berhasil ditemukan, 1 tidak ditemukan dan 3 percobaan tidak dilakukan karena fitur yang diuji tidak tersedia pada aplikasi terkait. Temuan ini membuktikan bahwa strategi dan kombinasi alat yang digunakan efektif untuk mendapatkan serta menganalisis bukti digital secara menyeluruh, sekaligus menunjukkan adanya perbedaan dalam penyimpanan dan ketersediaan data antar aplikasi IM.



**Kata kunci** : Android, Instant Messenger, NIST, Digital Forensik, Bukti Digital

## ABSTRACT

*The increased use of Instant Messenger (IM) apps such as WhatsApp, Line, Telegram and Facebook Messenger increases the risk of digital crime. These apps are often used in criminal activities, so there is a need to analyze digital evidence that can reveal traces left on Android devices. This research overcomes the limitations of previous studies that only compare app functionality, without delving into forensic analysis in the face of the latest security challenges. This research applies the National Institute of Standards and Technology 800-101 Revision 1 method by simulating 7 scenarios that focus on removing or erasing digital evidence. Implementing strategies by performing a combination of forensic tools used such as Magisk, Swift Backup, Magnet Axiom, Mobiledit Forensic, and tools for viewing databases using SQLite Studio and Hex Editor. The results of each application show different levels of vulnerability, the results show that out of 28 trials, 24 digital evidence was successfully found, 1 was not found and 3 trials were not conducted because the tested features were not available in the related application. These findings prove that the strategies and tool combinations used are effective for obtaining and thoroughly analyzing digital evidence, while also showing differences in data storage and availability between IM applications.*



***Keywords :*** *Android, Instant Messaging, NIST, Digital Forensics, Digital Evidence.*