# INTISARI

WhatsApp merupakan salah satu media sosial dengan jumlah pengguna terbanyak di dunia dan telah menjadi bagian penting dalam kehidupan masyarakat Indonesia untuk berkomunikasi. Dengan penetrasi pengguna mencapai 91,7% dari total pengguna internet di Indonesia yang berusia lebih dari enam belas tahun, WhatsApp memiliki potensi besar sebagai sumber bukti penting dalam investigasi forensik digital, baik untuk kejahatan siber maupun kejahatan konvensional. Tantangan utama dalam melakukan pemeriksaan forensik terhadap WhatsApp adalah keberadaan fitur penghapusan pesan seperti *delete for everyone*, *view once*, dan *disappearing message* yang secara khusus dirancang untuk membatasi akses terhadap pesan oleh penerima. Penelitian ini bertujuan untuk mengembangkan metode pemulihan pesan dan media WhatsApp yang telah dihapus melalui ketiga fitur tersebut.

Tiga skenario percakapan yang menerapkan masing-masing fitur dilakukan pada perangkat Android versi 10 yang telah dibuka *bootloader*-nya. Selanjutnya, perangkat diakses dengan *root* untuk memungkinkan dilakukannya akuisisi secara fisik. Selama proses forensik, pedoman dari dokumen NIST SP 800-101r1 digunakan sebagai acuan agar integritas data dari perangkat tetap terjaga. Setelah proses akuisisi, berkas basis data SQLite dengan mode *Write-Ahead Logging (WAL)* yang digunakan oleh WhatsApp dianalisis untuk mengidentifikasi tabel dan kolom penting terkait pesan dan media. Teknik analisis heksadesimal kemudian diterapkan pada berkas WAL untuk menemukan pola representasi heksadesimal dari pesan dan media. Untuk mempercepat dan mengotomatisasi proses ekstraksi, dikembangkan sebuah program yang mampu mengenali pola berbasis *regex* dan heksadesimal.

Hasil pengujian menunjukkan bahwa dari total 40 pesan dan 13 media yang dikirim atau diterima dalam skenario percakapan, sebanyak 23 pesan dan 3 media berhasil ditemukan dalam berkas WAL menggunakan program yang dikembangkan. Sebagai perbandingan, jika pemeriksaan hanya dilakukan pada basis data utama, maka hanya 20 pesan dan 3 media yang berhasil ditemukan.

Kata kunci: Forensik Digital, WhatsApp, Pemulihan Pesan, Analisis Heksadesimal, Write-Ahead Logging

# ABSTRACT

*WhatsApp is one of the most widely used social media platforms in the world and has become an integral part of daily communication for many people in Indonesia. With a user penetration rate of 91.7% among internet users aged over sixteen in Indonesia, WhatsApp holds significant potential as a source of digital evidence in forensic investigations, both in cyber and conventional crimes. One of the main challenges in conducting forensic analysis on WhatsApp is the existence of message deletion features such as delete for everyone, view once, and disappearing messages, which are specifically designed to restrict recipient access to certain messages. This study aims to develop a method for recovering deleted WhatsApp messages and media affected by these three features.*

*Three conversational scenarios were carried out, each employing one of the aforementioned features, on an Android device running version 10 with an unlocked bootloader. The device was then rooted to allow for physical data acquisition. Throughout the forensic process, guidelines from NIST SP 800-101r1 were followed to ensure the integrity of the extracted data. The acquired SQLite database, which operates in Write-Ahead Logging (WAL) mode, was examined to identify important tables and columns related to messages and media. Hexadecimal analysis techniques were applied to the WAL file to identify hex patterns corresponding to specific messages and media. A custom program capable of recognizing regex-based and hexadecimal patterns was developed to automate the extraction process.*

*The experimental results show that out of a total of forty messages and thirteen media exchanged during the conversations, twenty-three messages and three media files were successfully recovered from the WAL file using the developed program. In contrast, when relying solely on the primary database, only twenty messages and three media files could be found.*

**Keywords**: Digital Forensics, WhatsApp, Message Recovery, Hexadecimal Analysis, Write-Ahead Logging