BAB I

PENDAHULUAN

1.1 Latar Belakang

Aplikasi *Instant Messenger* telah menjadi salah satu bentuk komunikasi yang telah membawa banyak kemudahan bagi kehidupan manusia baik dalam konteks komunikasi, pembelajaran dengan menyediakan komunikasi instan (Siregar, 2022). Penggunaan aplikasi IM tidak hanya sebatas pada mengirim dan menerima pesan teks tetapi juga mencakup berbagai media, panggilan suara, bahkan kode *One Time Password* dan hal yang paling penting dari fitur keamanan data pribadi (Shahrul & Wibawa, 2021). Tujuan utama dari fitur keamanan dan privasi adalah untuk melindungi pengguna meskipun tujuannya baik celah ini juga dapat dimanfaatkan oleh pengguna untuk tindakan kejahatan atau yang dikenal sebagai *cybercrime* (Holle, 2019).

Berdasarkan data Badan Siber dan Sandi Nasional, pengaduan terkait serangan siber yang diterima terdiri dari 15 kategori. 3 kategori yang paling banyak dilaporkan adalah *cybercrime, vulnerable indicator, web defacement* dan lainnya. Pengaduan siber yang paling dominan yaitu *cybercrime* dengan jumlah pengaduan tercatat sebanyak 1.417 pengaduan atau sekitar 86% dari total keseluruhan pengaduan yang masuk (BSSN, 2023). Pelaku tindak kejahatan kerap memanfaatkan fitur keamanan seperti enkripsi, perlindungan data, pengaturan privasi, bahkan mencoba mencari cara untuk mengubah, menghapus beberapa atau keseluruhan data yang dianggap penting dengan tujuan untuk menghilangkan atau menyembunyikan bukti digital (Putra, 2021).

Dalam konteks tersebut, proses analisis bukti digital menjadi penting karena dapat membantu melacak jejak digital serta memulihkan data yang telah dihapus atau rusak, bukti digital yang berhasil dikumpulkan secara sah dapat digunakan dalam proses penegakan hukum (Riadi, Umar, et al., 2018). Untuk menjamin validitas proses tersebut, pemilihan metode yang tepat dan terstandar sangat penting dalam proses ini. Salah satu metode yang diakui secara luas adalah metode yang dikembangkan oleh *National Institute of Standards and Technology* (Hamid et al., 2024).

Penelitian ini berada dalam lingkup *mobile forensik*, dengan fokus pada penerapan metode *physical* dan *logical* untuk mengekstraksi data dari perangkat *mobile*, termasuk aplikasi *Instant Messenger* yang terpasang (Rachmie, 2020). Penelitian-penelitian sebelumnya telah melakukan analisis dan perbandingan aplikasi IM berbasis *Android*, seperti *WhatsApp, Telegram, Line*, dan *Imo Messenger*, dengan menggunakan simulasi pengujian dalam 12 skenario untuk mengevaluasi performa aplikasi-aplikasi tersebut dalam konteks keamanan data digital (Sidik Asyaky et al., 2018). Selain itu, studi forensik digital terhadap *Facebook Messenger* menggunakan alat *Oxygen Forensic* berhasil mengekstraksi berbagai jenis data, termasuk percakapan teks, gambar, dan audio (Yudhana et al., 2018). Penelitian lain yang membandingkan aplikasi *WhatsApp, Telegram*, dan *Signal Messenger* mengandalkan 10 skenario pengujian dengan penilaian yang didasarkan pada indeks akurasi untuk mengukur tingkat keberhasilan dalam ekstraksi data (Kusumadewa & Syaifuddin, 2022).

Meskipun berbagai studi telah mengeksplorasi teknik ekstraksi data dan evaluasi keamanan aplikasi IM, penelitian-penelitian sebelumnya cenderung terbatas pada perbandingan fungsional dan tidak mendalami kompleksitas analisis bukti digital yang diperlukan untuk mengatasi konteks penghilangan data aplikasi IM. Berdasarkan permasalahan tersebut. Penelitian ini tidak hanya fokus pada skenario proses penghilangan data pada aplikasi IM tetapi melakukan strategi kombinasi efektivitas kemampuan alat-alat digital forensik untuk mengekstraksi data dan menganalisis bukti digital yang masih dapat ditemukan setelah data dihapus. Mengimplementasikan kombinasi alat-alat forensik seperti *Mobiledit Forensic, Magnet Axiom, SQLitestudio, dan Hex Editor*.

Aplikasi IM yang menjadi fokus dalam penelitian ini diantaranya adalah *WhatsApp, Line, Telegram,* dan *Facebook Messenger*. Pemilihan aplikasi-aplikasi ini didasarkan pada tingkat popularitas dan penggunaannya di Indonesia, sebagaimana ditunjukkan dalam data dari grafik databooks.katadata.co.id. Dengan pendekatan ini, penelitian tidak hanya bertujuan mengekstraksi data dari aplikasi IM, tetapi juga memberikan pendekatan yang lebih kuat dalam memberikan analisis terhadap aspek keamanan dan aktivitas pengguna pada aplikasi IM, serta memperkuat validitas bukti.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini yaitu :

1. Bagaimana implementasi framework NIST SP 800-101 Revisi 1 untuk investigasi pada perangkat *smartphone Android* ?
2. Bagaimana strategi yang digunakan untuk memperoleh bukti digital pada perangkat *smartphone Android* ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Menganalisis implementasi *framework* NIST versi SP 800-101 Revisi 1 pada perangkat *smartphone Android*.
2. Mengevaluasi strategi untuk mendapat bukti digital pada perangkat *smartphone Android*.

1.4 Batasan Masalah

Batasan masalah yang dibahas dalam penelitian ini adalah sebagai berikut :

1. Penelitian dilakukan pada aplikasi *WhatsApp, Line, Telegram, Facebook Messenger.*
2. Hasil analisis penelitian menggunakan *tools Magisk, Swift Backup, Mobiledit Forensic*, *Magnet Axiom*, *Hex Editor* dan *SQLite Studio*.
3. Metode yang digunakan menggunakan *Nasional Institute Of Standards And Tecnology* SP 800-101 Revisi 1.
4. Penelitian menggunakan *smartphone android*.

5. Penelitian melakukan analisis berdasarkan 7 skenario.
6. Analisis bukti digital hanya yang didapatkan dari *smartphone android* yang diinvestigasi.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi seluruh pihak yang terkait, diantaranya :

1. Manfaat bagi Universitas Siliwangi, sebagai bahan kepustakaan sarana pengembangan wawasan keilmuan khususnya prodi Informatika.
2. Manfaat bagi peneliti yang lain, membantu meningkatkan pemahaman dan sebagai media referensi.