BAB I
PENDAHULUAN

1.1 Latar Belakang

Dilansir dari We Are Sosial pada januari 2024 pada pencatatan tahunan, total pengguna media sosial di Indonesia adalah sebanyak 139 juta identitas [1]. Whatsapp menjadi media sosial paling banyak digunakan sebanyak 90,9% dari total seluruh pengguna internet di Indonesia, dan akan diprediksi bertambah setiap tahun. Banyaknya pengguna media sosial Whatsapp meningkatkan potensi kejahatan siber yang memanfaatkan Whatsapp sebagai wadah untuk melakukan penipuan dengan bermacam motif. Berdasarkan informasi dari Badan Siber dan Sandi Nasional (BSSN), terdapat 151,4 juta kasus serangan siber di sepanjang tahun 2023, dan kasus kejahatan penipuan melalui platform media sosial dan email menjadi urutan ketiga paling rentan pada kasus serangan siber [2]. Banyak modus atau teknik manipulasi yang dilakukan oleh para penipu sehingga tindak kejahatan siber terus terjadi. Salah satunya adalah teknik *social engineering*. *Social engineering* merupakan sebuah teknik manipulasi yang dipakai oleh penjahat siber untuk mengeksploitasi kepercayaan manusia demi mendapatkan informasi rahasia korbannya, yang memungkinkan terjadinya kejahatan siber lebih lanjut [3]. Pada kasus penipuan melalui media Whatsapp ini banyak menggunakan file dengan format .apk yang berkedok undangan pernikahan digital atau cek resi paket. Penyebaran pesan dengan file.apk yang menyerupai undangan pernikahan atau cek resi paket adalah kasus yang sering terjadi dalam dua tahun terakhir, yang mengakibatkan banyak korban. Penipu menggunakan motif tersebut untuk dapat mengambil informasi korban dan mengakses layanan perbankan melalui ponsel korban, yang dapat mengakibatkan pengalihan dana dari akun *m-banking* atau *e-wallet* korban kepada pelaku [4].

Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang melarang seseorang untuk mengakses, mengubah, atau menghapus data pribadi orang lain tanpa izin yang sah (Pasal 65 ayat 1), maka kasus pengambil alihan akses *m-banking* secara ilegal ini dikategorikan sebagai kasus pelanggaran data, karena data pribadi ini diakses tanpa izin dari pemilik akun.

Kasus pelanggaran data memiliki fase dan tujuan yang berbeda dengan kasus kejahatan siber secara umum, karena adanya eksfiltrasi data, yaitu pengambilan data secara tidak sah dari sistem korban dan memindahkannya ke sistem yang dikendalikan oleh penyerang, dimana data yang dicuri dibawa keluar dari lingkungan korban. Tahap ini membedakan kasus pelanggaran data dengan kasus serangan siber yang lain, seperti kasus serangan *ransomware* yang mengenkrip data korban kemudian meminta tebusan dan juga kasus serangan DDoS yang bertujuan untuk mengganggu atau menonaktifkan layanan tanpa mencuri data. Maka dari itu, penting untuk menggunakan kerangka investigasi khusus untuk menangani kasus jenis pelanggaran data [5].

Investigasi forensik digital sangat penting dalam mengungkap pelanggaran data dan menemukan fakta penting mengenai sumber serta tingkat insiden. Pengumpulan bukti untuk menjawab pertanyaan 5W1H (apa yang terjadi, siapa yang terlibat, kapan, di mana, mengapa, dan bagaimana insiden terjadi) merupakan tujuan utama dari forensik digital. Berdasarkan kerangka kerja forensik yang sudah dilakukan sebelumnya, seperti metode NIST [6], IDFIF [7], dan DFRWS [8] hanya menghasilkan data-data mentah dari alat-alat forensik yang digunakan sehingga belum bisa menyediakan analisis menyeluruh untuk menjelaskan 5W1H dari insiden yang terjadi atau cakupan lengkap dari jenis dan motif serangan. Selain itu, *framework* tersebut lebih fokus pada investigasi kejahatan siber umum, penipuan siber, atau serangan siber daripada investigasi pelanggaran data seperti kasus penipuan yang memungkinkan pelaku mengambil akses *e-wallet* atau *m-banking* korban.

Pada tahun 2023, Arif Rahman Hakim dkk melakukan sebuah penelitian dengan sebuah *framework* digital forensik pada suatu kasus pelanggaran data yaitu "*Digital Forensics framework for Reviewing and Investigating*" atau yang disebut dengan *framework* D4I. *Framework* tersebut merupakan metode atau kerangka kerja analisa dan investigasi forensik baru yang khusus untuk diterapkan ketika terjadi kasus pelanggaran data, karena mampu mengkategorikan artefak sehingga memberikan hasil yang lebih tepat dan menyeluruh serta memberikan jawaban komprehensif terhadap pertanyaan investigasi 5W1H (Who, What, When, Where, Why, How) [5]. *Framework* ini dirancang bukan untuk menggantikan proses

digital forensik yang sudah ada, tetapi melengkapi dan meningkatkan tahapan pemeriksaan dan analisis. Kerangka D4I bekerja dengan menyediakan langkah demi langkah dan secara lebih mudah melakukan investigasi serangan siber yang memungkinkan *framework* ini untuk mengidentifikasi serangan jenis pelanggaran data [9]. Berdasarkan hasil penelitian tersebut, maka *framework* D4I akan menjadi metode analisa dan investigasi digital forensik di penelitian ini.

Pada penelitian ini, penulis bertujuan untuk melakukan investigasi dan analisa digital forensik pada kasus pelanggaran data melalui aplikasi Whatsapp menggunakan *framework* D4I dengan studi kasus file CekResi SiCepat Express dengan format APK. Penelitian ini diharapkan dapat meningkatkan proses identifikasi digital forensik dengan lebih baik melalui peningkatan tahapan pemeriksaan dan analisis yang didasarkan pada sifat, jenis, dan tipe bukti. Selain itu, penelitian ini juga bertujuan untuk menyediakan atau menyajikan bukti digital forensik yang diperlukan dalam investigasi. Penelitian ini diharapkan dapat mendukung penyelidikan dengan memberikan panduan yang jelas dalam setiap tahap analisis forensik melalui penjelasan yang mendalam dan contoh prosedur investigasi mengguunakan *framework* D4I.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah yang diangkat pada penelitian ini adalah sebagai berikut:

a) Bagaimana melakukan investigasi digital forensik menggunakan *framework* D4I pada kasus pelanggaran data melalui media sosial Whatsapp dengan studi kasus CekResi SiCepat Express .apk?
b) Bagaimana hasil analisis digital forensik menggunakan *framework* D4I pada kasus pelanggaran data melalui media sosial Whatsapp dengan studi kasus CekResi SiCepat Express .apk?

1.3 Tujuan Masalah

Tujuan dari penelitian ini dengan judul "Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan *Framework* D4I (Studi Kasus: CekResi SiCepat Express .apk)" adalah :

a) Melakukan investigasi digital forensik pada kasus pelanggaran data melalui media sosial Whatsapp dengan studi kasus CekResi SiCepat Express .apk menggunakan *framework* D4I
b) Memberikan hasil analisa digital forensik pada pelanggaran data melalui media sosial Whatsapp dengan studi kasus CekResi SiCepat Express .apk menggunakan *framework* D4I.

1.4 Batasan Masalah

Untuk memudahkan dalam penyelesaian kedepannya pada penelitian ini, maka akan dibatasi pada beberapa hal berikut:

a) Penelitian ini berfokus pada penipuan melalui aplikasi Whatsapp dengan media CekResi SiCepat Express .apk
b) Akuisisi data *non-volatile* dilakukan secara offline dengan *tool* forensik MOBILedit Forensik Express
c) Proses analisis yang dilakukan pada barang bukti file .apk yang diduga *malware* adalah analisis kode atau analisis statis
d) Alat forensik yang digunakan dalam proses dan analisa file .apk yang dicurigai adalah Jadx GUI
e) Penelitian ini berfokus pada kasus penipuan melalui aplikasi Whatsapp pada sistem operasi Android