BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet adalah bagian *integral* dari perkembangan teknologi modern dan telah menghasilkan perubahan besar dalam masyarakat. Salah satu aspek yang paling mencolok adalah penggunaan *email,* yang telah menjadi salah satu alat komunikasi paling umum dan luas digunakan di seluruh dunia. *Email* merupakan aplikasi yang sangat populer dan digunakan setiap hari untuk keperluan pribadi, bisnis atau resmi.

Meningkatnya jumlah pengguna *email* tentunya membawa dampak *positif* dan *negatif* bagi dunia *internet*. Dampak *negatif* yang sering muncul adalah sebagian pengguna *email* melakukan kejahatan digital. Kemudahan penyampaian *email* menjadi ancaman yang serius, terutama dalam penggunaan *email* sebagai wahana kejahatan di dunia *cyber*.

Salah satu kejahatan paling umum adalah *spoofing email. Spoofing* adalah *email* yang dipalsukan dan dikirim seolah-olah berasal dari sumber tepercaya. Pelaku pencurian identitas memanipulasi *data* di *header email* untuk menyamar sebagai pengguna *email* yang sah. Laporan *intelijen Symnatec* menunjukkan bahwa 68% dari seluruh *email* adalah *spam*, 1 dari 358,2 *email* diidentifikasi sebagai *email phishing* dan 274,0 *email* berisi *malware* (Yudhana et al., 2019).

Spoofing email digunakan oleh penulis untuk menyembunyikan alamat *email* asli dengan mengubah beberapa kolom di *email*, seperti "*from*", "*return-path*", dan "*replay to*". Untuk membuat *email* terlihat

seperti *email* asli dan mungkin menipu penerima yang tidak memahami *email* tersebut dan terjebak dalam skrip yang dibuat oleh penulisnya.

Penelitian ini bertujuan untuk menganalisa *email* yang diduga merupakan *email spoofing*. Mengumpulkan barang bukti dari *header email* yang mendukung proses analisis untuk melacak pelaku *spoofing*. *Header* akan menunjukkan *email server* asal, Oleh karena itu, diperlukan tindakan forensik untuk mengatasi kejahatan yang melibatkan email tersebut. Analisis forensik ini dilakukan dengan menggunakan berbagai perangkat (tools). *forensic* yaitu *email tracer, dossier, fortiguard labs* dan *messageheader*. Penelitian ini akan menggunakan pendekatan studi kasus tunggal dan akan dianalisis dengan menggunakan alat-alat (tools). *email tracer, dossier, fortiguard* labs dan messageheader Oleh karena itu, diharapkan penelitian ini akan menghasilkan keakuratan dalam penemuan barang bukti berdasarkan hasil analisis dari alat-alat forensik yang digunakan.

Kelebihan dalam mengaplikasikan tools tesrebut antara lain, Dari beberapa *tools* tersebut menjelaskan proses dan analisi pada *email spoofing* dapat dibuktiakan dari mana *email* tersebut dikirim, *IP address*, alamat, *domain email*. Sehingga bisa dikatakan bahwa *email* yang dianalisi benar-benar merupakan *emai spoofing* (M. arief Sutisna, 2018).

PT Kereta Api Indonesia (Persero), atau yang biasa disebut KAI atau 'Perusahaan,' merupakan sebuah Badan Usaha Milik Negara yang bertanggung jawab atas penyediaan, pengaturan, dan pengelolaan layanan angkutan kereta api di Indonesia. PT KAI (Divre III Palembang) terletak di alamat Jl. Jend. A. Yani No. 541, 13 Ulu, Plaju Palembang, yang Merupakan Badan Usaha Milik Negara (BUMN) Indonesia yang bertanggung jawab atas penyediaan, pengaturan, dan pengelolaan. perkeretaapian di Indonesia. Instansi ini menggunakan *email* sebagai

sarana pengirim surat dan *dokumen*, tidak waspadaan terhadap *email spoofing* akan mengakibatkan bahaya, apabila tidak dilakukan nya invetigasi terhadap *email* yang mencurigakan. Maka harus dilakukan pengecekan terlebih dahulu, sebelum membuka atau membalas pesan di karenakan bisa jadi adanya indikasi *email spoofing* di dalam pesan.

Setelah dilakukan pengamatan pada PT KAI divre III palembang, disini di temukan adanya indikasi ganguan, terhadap *system* pengiriman berbasis *email*. dalam melakukan *investigation* agar nantinya kendala dalam ancaman *spoofing email*, bisa dilakukan nya pencegahan dan penanganan agar dapat digunakan dengan baik. Proses ini melibatkan penerapan metode *NIST (National Institute of Standards and Technology)* dalam menganalisis bukti digital dan langkah-langkah untuk mengumpulkan informasi dari bukti digital.

Beberapa penelitian tentang ancaman dari *email spoofing* antara lain penelitian (Marzuki et al., 2022) Penerapan *DomainKeys* Mengidentifikasi *Email*, Kerangka Kebijakan Pengirim, *Anti-Spam*, dan *AntiVirus*: Analisis pada *Server Email*. Dengan demikian, pengidentifkasin *email spoofing*, jauh lebih aman dan bisa di antisipasi.

Penelitihan selanjutnya (Prawira & Samsudin, 2022) Investigasi dilakukan dengan metode *live* forensik, yaitu komputer digunakan dalam keadaan menyala. Penelitian tersebut juga memanfaatkan aliran penelitian *NIST (National Institute of Standards and Technology). Email* yang akan dianalisis adalah *header email* menggunakan tiga alat: *tracer email analyzer, email dossier* dan *mail header analysis*. Analisis ini membandingkan dan memeriksa keakuratan *header email* menggunakan *tools* ini. *Email* yang diduga merupakan *email spoofing* diperiksa menggunakan *tools*. Berdasarkan *header 'form' received' dan 'message-*

ID'. Berdasarkan hasil *tools* yang memenuhi nilai setelah dilakukan analisis maka dilakukan analisis *email* lanjutan.

Penelitihan lainnya dengan (Mushlihudin & Nofiyan, 2021) Metode National Institute of Standards and Technology (NIST) digunakan dengan tujuan menganalisis proses investigasi kejahatan di dunia maya atau forensik digital serta menciptakan bukti digital. Langkah analisisnya adalah pengumpulan, penelitian, analisis dan pelaporan. Menggunakan perangkat Wireshark untuk mencari bukti dan memanfaatkan alat Hashcalc untuk mendapatkan bukti yang diperoleh.

Penelitian yang dilakukan oleh Altulaihan (Altulaihan et al., 2023) tentang Masalah Keamanan *Email*, Alat, dan Teknik yang Digunakan dalam Investigasi. Pada penelitian ini telah dilakukan pengujian, dengan menggunakan alat investigasi sebagai, pengecekan terhadap masalah keamanan *email*.

Berdasarkan uraian hal tersebut, dalam penulisan ini, penulis tertarik untuk. meneliti mengenai permasalahan terhadap serangan *email spoofing*. Oleh karena itu penulis mengambi judul **"INVESTIGATION DIGITAL FORENSIC TERHADAP SERANGAN EMAIL SPOOFING PADA PT KAI DIVRE III PALEMBANG"**

1.2 Rumusan Masalah

Berdasarkan latar belakang dan pertanyaan penelitian yang telah dijelaskan sebelumnya, penulis merumuskan masalah sebagai berikut: "Bagaimana" Menganalisa *email* yang Diduga Merupakan Serangan *email spoofing*?". Dengan menggunakan *tools forensic* yaitu *email tracer, dossier, fortiguard labs* dan *messageheader.*

1.3 Batasan Masalah

Sementara itu, batasan masalah dari penelitian ini adalah :

- *Investigation* terhadap serangan *email spoofing* Dengan menggunakan *tools forensic* yaitu *email tracer, dossier, fortiguard labs* dan *messageheader.*

1.4 Tujuan Penelitian

Penelitian in bertujuan untuk menganalisa *email* yang diduga merupakan serangan *email spoofing.* Dengan menggunakan *tools forensic* yaitu *email tracer, dossier, fortiguard labs* dan *messageheader*

1.5 Manfaat Penelitian

Manfaat dari hasil penelitian ini meliputi :

a. Bagi penulis

   Memperdalam wawasan di bidang digital forensik, dan menerapkan ilmu yang di dapat ketika kuliah. Menguji keakuratan teori yang di ambil dari penelitian sebelumnya.

b. Bagi instansi perushaan

   Melakukan pengecekan tehadap kerentanan dan ketidak waspadaan terhadap ancaman serangan *email spoofing*.

c. Bagi akademik

   Sebagai landasan refrensi penelitan selanjutnya, yang berkaitan dengan digital *forensic* sebagai studi banding penelitian selanjutnya.

1.6 Penelitian Terdahulu

Penelitian terdahulu merupakan upaya dalam, mencari perbandingan dan inspirasi baru bagi penlitian selanjutnya. Selain itu penelitian sebelumnya membantu dalam mempromsikan penelitian dan juga *orisinalitas* penlitian.

Adapun penelitian sebelumnya telah dilakukan oleh (Ardhi, 2020) Penelitian berjudul "Pelacakan *Geolocation* pada Forensik *Email Terintegrasi Geo-Social Network Twitter*" dengan mengintegrasikan metode *email* forensik klasik dan *data mining* untuk mengetahui perbedaan hasil pelacakan kedua metode tersebut agar dapat saling mendukung informasi mengenai suatu lokasi yang sedang dilacak.

Tujuan Dengan melakukan analisis *header* dengan alat *eMailTrackerPro*, Peneliti dapat menemukan *ISP* yang digunakan peretas untuk mengirim *email*. *GeoSN* melacak lokasi pengguna dan menyematkan data ini ke dalam data Twitter. Data ini dapat digunakan untuk data mining untuk mendapatkan informasi lokasi pengguna, sehingga memudahkan penyelidikan oleh pihak yang berwajib. Data mining di Twitter memberikan informasi yang lebih akurat mengenai keberadaan *hacker*.

Penelitian lain juga dilakukan oleh (Riadi, Sunardi, & Fitri, 2022) *Email* adalah sistem Untuk mengirim dan menerima pesan yang berisi berkas, gambar, *audio*, dll. *NFDC Metode* ini telah berhasil digunakan untuk pengumpulan bukti. Simulasikan pengiriman email dengan alat pendeteksi *spam email* sederhana dan uji *email* dengan Penelitian menggunakan alat Wireshark. Hasil pengujian menunjukkan bahwa sebanyak 40 email diterima atau dimasukkan ke dalam kotak masuk korban, dan pengujian berhasil diselesaikan dengan mempertimbangkan parameter-parameter yang telah ditentukan. Beberapa parameter tersebut mencakup alamat IP pengirim atau spammer yang terdeteksi sebagai 72.125.68.109, dan alamat IP korban yang adalah 192.168.1.12.

Pada penelitian yang dilakukan oleh (M. A. Sutisna et al., 2021) Email sangat mudah di palsu untuk menipu Korban. Bagian *email* yang paling mudah diproses adalah *header email, header* yang sering digunakan untuk pemrosesan. Dia Dari dan tanggal. Penipuan atau pemalsuan sering disebut *email spoofing*.

Ada tiga jenis *spoofing email* yaitu *spoofing email* tanggal, *spoofing alamat*, dan *spoofing email*. Penipuan *Emai*l baru saja memalsukan alamat *email*. Penipuan *Email* Palsu Tanggal Pengiriman saja.

Pendeteksi *Email Spoofing* dapat dilakukan dengan cara menganalisis *header email*, terutama dengan memeriksa bidang (*field*) yang mengandung informasi tertentu. Diperlukan *sepeti From, Message-ID, Received, Date,*

Pemilihan yang tepat terhadap persoalan di atas menjadi tujuan dalam pembahasaan penulis dalam penelitian ini, yaitu dibutuhkan langkah dalam melakukan investigasi terhadap *spoofing email*, pada PT KAI drive III Palembang. Pada penelitian terdahulu ini penulis menggunakan sebuah *methode NIST*(*National Institute of Standards Technology*) Pada tahap *collection* yaitu melakukan sebuah simuasi yang digunakan sebagai analisis. Selain dengan menggunakan *tools* yang berakaitan dengan *email spoofing*. tahap *examination* mengolah *data* yang terkumpul secara forensic dengan Tahap pemeriksaan dilakukan menggunakan alat-alat (tools) yang sesuai. Tahap analisis melibatkan evaluasi hasil pemeriksaan dengan menggunakan alat-alat tersebut. Selanjutnya, tahap pelaporan merupakan langkah untuk menyajikan hasil analisis. dari pemriksaan dari tindakan forensik yang diambil (Riadi, Sunardi, & Nani, 2022).