BAB I
PENDAHULUAN

1.1. Latar Belakang

Email yakni salah satu alat komunikasi untuk mengirim, menerima, dan mentransfer informasi melalui *system* komunikasi elektronik [1]. Istilah lain dari *email* yakni *termasuk system simple mail transfer protocol* (*SMTP*) dan *internet* yang memungkinkan organisasi untuk mengirim suatu pesan ke pesan lainnya. *Email* terdiri dari 2 bagian yakni judul dan isi judul yang berfungsi menyediakan informasi yang dibutuhkan untuk korespondensi *email* dan stempel waktu. Sedangkan *body* digunakan untuk menulis pesan atau data yang disampaikan kepada penerima [2]. *Email* itu sendiri memiliki sisi positif sisi negatifnya adalah para penjahat dunia maya juga menggunakan *email* sebagai alat untuk melakukan kejahatan namun karena proses pengiriman datanya yang cukup rumit maka jaminan data yang dikirimkan bisa diperiksa bahkan bisa saja terjadi pemalsuan *email* yang merugikan beberapa pihak. Salah satu kejahatan yang sering terjadi adalah *spoofing email* dan *phising*, *spoofing* ialah *email* yang dipalsukan dan di kirim oleh seseorang seolah-olah berasal dari sumber yang dapat dipercaya. Menurut *Anti Phising Working Group* (*APWG*) pada April 2024 merilis data bahwa 963,994 terjadi serangan *phising,* ini terjadi pada kuartal pertama tahun 2024 [3].

Dari permasalahan di atas peneliti berupaya mecari cara menginvestigasi yang bertujuan memberikan cara efektif untuk mengidentifikasi idetitas, keaslian dan malware dari *email* yang mencurigakan dengan menggunakan beberapa *tools* seperti *MXtoolbox, Whois Lookup, Talos, Sucuri tools*, dan *VirusTotal* untuk meningkatkan efektivitas penelusuran *email* mencurigakan. Langkah pertama yang akan dilakukan peneliti ialah melakukan pengumpulan pada *email* masuk yang dirasa mencurigakan. Setelah mendapatkan beberapa *email* yang dirasa mencurigakan selanjutnya menggunakan *tools* komputer forensik yang bertujuan untuk mengungkapkan keaslian *email* dan menganalisa keberadaan *malware*.

Peneliti bertujuan untuk meremuskan solusi tidak hanya mampu mengidentifikasi *email* yang mencurigakan, tetapi juga memberikan pendekatan yang sistematis dan terukur dalam menginvestigasi forensik digital terhadap *email*. Solusi ini difokuskan untuk meningkatkan efektivitas indetifikasi pengirim, keaslian *email*, serta memungkinkan adanya *malware* yang tersembunyi di dalam isi maupun lampiran *email*. Dengan memanfaatkan *tools* seperti *MXToolbox* untuk menganalisis *MX records* dan *DNS, Whois Lookup* untuk melacak kepemilikan *domain*, *Talos Intelligence* untuk mengevaluasi reputasi *IP* dan *domain*, *Sucuri* untuk mendeteksi potensi serangan berbahaya serta *VirusTo*tal untuk memeriksa lampiran *file*, peneliti berharap dapat membangun sebuah pendekatan forensik yang komprehensif. Melalui langkah-langkah ini, hasil penelitian diharapkan mampu menghasilkan panduan teknis yang tidak hanya berguna bagi kalangan akademis, tetapi juga bermanfaat bagi praktisi keamanan siber, institusi, dan pengguna umum dalam mengenali, menganalisis, serta merespon ancaman dari *email* mencurigakan. Tujuan jangka panjangnya adalah menciptakan sistem pertahanan awal yang mampu mendeteksi serangan *siber* berbasis *email* secara dini, sehingga mampu mengurangi risiko kerugian yang ditimbulkan oleh tindakan seperti *spoofing, phishing*, maupun penyebaran *malware*. Berdasarkan uraian di atas maka, penulis tertarik melakukan penelitian yang berjudul "***Analisis* Komputer Forensik dalam Penelusuruan Identitas, Keaslian dan *Malware* dari *Email* Masuk**".

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah di jelaskan peneltian ini berfokus pada dua permasalahan utama yaitu:

1) Bagaimana Teknik komputer forensik dapat digunakan untuk menentukan identitas *email*.
2) bagaimana metode verifikasi keaslian *email* masuk dapat diterapkan menggunakan teknik komputer forensik.

1.3. Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan, penelitian ini merumuskan beberapa masalah utama. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut:

1) Peneltian ini hanya memeriksa alamat *email* masuk yang bersifat mencurigakan atau diduga berisi *malware*, *phising,* atau bentuk tipuan maupun serangan *siber* lainnya.
2) Data yang digunakan dalam penelitian ini berasal dari kumpulan *email* yang dikumpulkan dari *email* masuk. Ini menggunakan alat forensik khusus yang mendukung forensik *email*, seperti, *mxtoolbox* dan *tools* lainnya.
3) Penelitian ini tidak mencakup analisis hukum terhadap isi *email*, pelacakan lanjutan terhadap pelaku serangan *siber*, maupun penanganan pasca identifikasi. Fokus utama penelitian hanya pada proses teknis analisis dan identifikasi awal mengguanakan *tools* komputer forensik untuk mengungkap identitas, keaslian, serta potensi keberadaan *malware* maupun kejahatan *siber* lainnya.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan

Sejalan dengan permasalahan yang telah dirumuskan, penelitian ini memiliki beberapa tujuan yang ingin dicapai. Adapun tujuan dari penelitian ini adalah sebagai berikut:

1) Mengimplementasikan teknik komputer forensik dalam penelusuran identitas *ip email* guna mengungkap sumber asli *email*. Mengembangkan metode pengambilan *email* untuk memverifikasi keaslian pesan berdasarkan *header email.*
2) Menganalisis dan mengidentifikasi potensi *malware* dalam *email* masuk menggunakan teknik komputer forensik, baik melalui analisis statis maupun dinamis.

3) Memanfaatkan dan menguji efektivitas alat bantu digital forensik seperti *MXToolbox, Whois Lookup, Talos*, *Sucuri*, dan *VirusTotal* dalam proses investigasi *email*. Melalui *tools* ini, peneliti ingin menunjukkan bagaimana Langkah-langkah teknis dapat dilakukan secara sistematis untuk memverifikasi keaslian pengirim, mengecek reputasi *domain*, serta mendeteksi adanya *malware* tersembunyi pada *email* masuk.

1.4.2. Manfaat

Berdasarkan tujuan dan ruang lingkup yang telah dijelaskan, penelitian ini diharapkan memberikan beberapa manfaat. Adapun manfaat dari penelitian ini adalah sebagai berikut:

1) Memberikan kontribusi dalam pengembangan ilmu forensik digital, khususnya dalam analisis *email* sebagai bagian dari kejahatan *siber*.
2) Meningkatkan kesadaran pengguna terhadap ancaman yang tersembunyi dalam *email* terutama yang berkaitan dengan serangan *phising, spoofing*, dan penyebaran *malware*. Dengan mengetahui ciri-ciri *email* mencurigakan pengguna dapat lebih waspada dan tidak mudah menjadi korban kejahatan *siber*.
3) Penelitian ini diharapkan dapat mendorong kesadaran akan pentingnya perlindungan data dan komunikasi digital. Dengan adanya metode penelusuran identitas, keaslian, dan keberadaan malware dalam *email,* pengguna dapat mengambil tindakan pencegahan lebih dini untuk menghindari kerugian akibat serangan *siber*.

1.5. Peneliti Terdahulu

Berdasarkan latar belakang yang telah diuraikan, peneliti merumuskan beberapa permasalahan utama dalam penelitian ini. Adapun rumusan masalah yang dimaksud adalah sebagai berikut:

Pertama penelitian yang dilakukan oleh Imam Riadi, Sunardi, dan Fitriyani Tella peneliti melakukan Penelitian ini bertujuan untuk mendeteksi dan menganalisis bukti forensik dari aktivitas *spam email* yang dikirim secara massal,

yang dapat digunakan untuk mengidentifikasi pelaku atau sumber serangan. Penelitian ini dilakukan dengan mensimulasikan pengiriman 40 *spam email* kepada seorang korban menggunakan *Easy Email Spammer* dan dianalisis dengan *Wireshark*, hasil dari penelitian ini yakni Penelitian ini berhasil menunjukkan bahwa dapat digunakan secara efektif dalam mendeteksi, mengumpulkan, dan menganalisis bukti forensik dari serangan *email spam*. Hasilnya dapat digunakan untuk meningkatkan keamanan *email*, membantu dalam identifikasi pelaku, dan menjadi referensi dalam investigasi kejahatan siber terkait *email spamming* [4].

Kedua, peneliti yang dilakukan oleh Chris Moulana Bachri dan Wawan Gunawan, penelitian ini dilakukan karena dilatarbelakangi oleh tingginya volume *spam email* di Indonesia, yang menempati peringkat ke-8 di dunia dalam pengiriman spam. Metode deteksi tradisional seperti *Naive Bayes, SVM*, dan *K-NN* telah digunakan sebelumnya, tetapi memiliki keterbatasan dalam mengidentifikasi pola *spam* yang semakin kompleks. Penelitian ini menggunakan metode *CNN* terdiri dari beberapa lapisan utama, yaitu lapisan *embedding* untuk mengubah teks menjadi *vektor numerik*, lapisan konvolusi untuk mengenali pola dalam teks, lapisan *pooling* untuk mengurangi dimensi data, dan *lapisan fully connected* untuk melakukan klasifikasi *spam* atau non-*spam* menggunakan fungsi aktivasi *sigmoid*. Secara keseluruhan, penelitian ini membuktikan bahwa *CNN* adalah solusi yang lebih baik dalam mendeteksi *email spam* dan dapat digunakan untuk meningkatkan keamanan digital serta mengurangi ancaman *siber* dari *email* berbahaya [5].

Ketiga, penelitian yang dilakukan oleh Rahmat Novrianda Dasmen, Muhammad Reihan Pratama, Husni Yasir, Ariff Budiman penelitian ini membahas analisis forensik digital, menggunakan metode *National Institute of Standard and Technology (NIST) SP 800-86*. Penelitian ini bertujuan untuk mendapatkan kembali bukti digital yang telah di hapus guna mengungkap kejahatan *siber* [6].

Keempat, penelitian yang dilakukan oleh Rahmat Novrianda Dasmen, Asti Triwulanda, Rasmila, Dedi kurniawan, julia penelitian ini membahas penerapan komputer forensik. Studi ini menunjukkan bagaimana komputer forensik dapat

digunakan untuk menelusuri, menganalisis, dan mengembalikan bukti digital, yang sangat penting dalam penyelidikan forensik digital [7].

Kelima, penelitian yang dilakukan oleh Abrar Alismail, M.M. Hafizur Rahman dan A. Ibrahim penelitian ini membahas ancaman keamanan *email*, alat yang digunakan dalam investigasi forensik *email*, serta teknik yang dapat diterapkan untuk melindungi *email.* Penelitian ini bertujuan untuk mengavaluasi insiden *email* forensik, serta memberikan solusi pelindungan dari ancaman *email*, oleh karena itu jurnal ini mengkaji metode terbaik untuk meningkatkan keamanan *email* dan melakukan investigasi forensik terhadap ancaman digital [8].