BAB 1
Pendahuluan

1.1 Latar Belakang

Electronic mail (email) atau yang dalam bahasa Indonesia diartikan sebagai "surat elektronik" adalah sebuah layanan internet yang dapat digunakan untuk mengirim pesan secara elektronik. Pesan elektronik yang dikirim dapat berupa teks, file gambar, audio, video atau lainnya. Penggunaan email saat ini memainkan peranan penting dalam kehidupan banyak orang dan telah menjadi metode komunikasi utama di antara entitas bisnis (Chung & Ho, 2007). Email menjadi bagian yang penting karena akun email diperlukan untuk mendaftar ke situs jejaring sosial, *instant messaging*, dan layanan lain yang tersedia di internet (The Radicati Group, 2018).

Berdasarkan data yang dirilis oleh The Radicati Group, Inc. pada tahun 2018, jumlah pengguna email di tahun 2019 diperkirakan akan mencapai 3,93 miliar pengguna di seluruh dunia. Angka ini bertumbuh 3% dari jumlah pengguna email di tahun 2018 yang mencapai 3,823 miliar pengguna, lebih dari setengah populasi penduduk di dunia. Pada akhir tahun 2022 jumlahnya diperkirakan akan terus meningkat hingga 4,258 miliar pengguna. Selain itu, total email yang dikirim dan diterima per hari di tahun 2019 diperkirakan dapat mencapai 293,6 miliar email. Data-data tersebut dituangkan dalam Tabel 1.1 dan Tabel 1.2.

Tabel 1.1 Perkiraan jumlah pengguna email di seluruh dunia tahun 2018-2022

	2018	2019	2020	2021	2022
Worldwide Email Users (in Billion)	3,823	3,930	4,037	4,147	4,258
% Growth		3%	3%	3%	3%

Tabel 1.2 Perkiraan lalu lintas pengiriman dan penerimaan email per hari tahun 2018-2022

	2018	2019	2020	2021	2022
Total Worldwide Emails Sent/Received Per Day (in Billion)	281.1	293.6	306.4	319.6	333.2
% Growth		4,4%	4,4%	4,3%	4,3%

Proses pengiriman email sama seperti proses pengiriman surat konvensional, untuk sampai ke penerimanya harus melalui beberapa tahapan. Jika dalam surat konvensional, surat yang dikirim oleh pengirim harus melalui beberapa kantor pos, mulai dari kantor pos cabang, kantor pos pusat, dan petugas pengirim surat (kurir) kemudian sampai kepada penerima. Sedangkan pada email, jalur yang harus dilalui dari pengirim ke penerima harus melalui beberapa *router*, *mail servers*, dan beberapa jaringan komputer (Kiswanto, 2017). Kemajuan teknologi yang cukup pesat membuat email menjadi media bagi penjahat untuk melakukan aksinya. Baik pada kasus kriminal murni yang melibatkan email maupun kasus kriminal yang terjadi di jaringan internet. Penjahat dunia maya memalsukan email untuk melakukan berbagai kegiatan yang ilegal melalui sistem email. Kegiatan ilegal ini meliputi: *spamming*, *phishing*, *cyber bullying*, pornografi anak, pelecehan seksual, maupun penyebaran virus, *worm*, *hoax*, *Trojan horse* (Banday, 2011c).

Forensik email adalah sebuah studi tentang sumber dan isi sebuah email sebagai bukti untuk mengidentifikasi pengirim dan penerima email, tanggal dan waktu transmisi, catatan terperinci dari transaksi sebuah email, maksud dan tujuan pengirim email, dan lain-lain. Studi ini melibatkan investigasi metadata, pencarian kata kunci, dan pemindaian port. Ada beberapa pendekatan teknik investigasi dalam forensik email yang dapat dilakukan untuk mengungkapkan kasus kriminal yang melibatkan email, yaitu: *header analysis*, *bait tactics*, *server investigation*, *software embedded identifiers*, dan *sender mailer fingerprints*.

Penelitian mengenai forensik email dengan menggunakan teknik *header analysis* telah banyak dilakukan untuk mengidentifikasi apakah email yang diterima merupakan email asli atau telah dipalsukan (*spoofed*). Teknik *header analysis* merupakan suatu teknik analisis yang dilakukan pada metadata yang terdapat pada *header* sebuah email. Metadata tersebut berisi informasi mengenai pengirim dan/atau jalur yang dilalui oleh email selama dalam perjalanan menuju alamat email yang dituju. Beberapa di antaranya mungkin telah dipalsukan untuk menyembunyikan identitas pengirim. Teknik *header analysis* dilakukan dengan cara menganalisis *header email* secara rinci dan menemukan korelasi dari setiap *field* pada *header* (Banday, 2011b).

Beberapa perangkat lunak *open source* telah dikembangkan untuk melakukan analisis terhadap *header email* untuk mengumpulkan bukti penipuan melalui email, contohnya: eMailTrackerPro, EmailTracer, Adcomplain, Aid4Mail Forensic, AbusePipe, AccessData's FTK, EnCase Forensic, FINALeMAIL, Sawmill-GroupWise, Forensics Investigation Toolkit (FIT), Paraben (Network) E-mail Examiner, dan lain-lain. *Tools* tersebut memiliki fitur pelaporan penyalahgunaan, opsi klasifikasi email, serta mendukung beberapa teknik

enkripsi (Banday, 2011c). Selain itu, *tools* ini dapat membantu dalam hal mempelajari sumber dan isi email sehingga serangan atau niat jahat dari intrusi dapat diselidiki. *Tools* tersebut menyediakan format *browser* yang mudah digunakan, pelaporan otomatis, dan fitur lainnya seperti membantu mengidentifikasi asal dan tujuan email, melacak jalur yang dilalui oleh email, mengidentifikasi *spam* dan jaringan *phishing*, dan lain-lain (Banday, 2011b).

Studi komparatif telah dilakukan dengan membandingkan 5 *tools* yang populer dan digunakan secara luas dalam forensik email menggunakan 9 kriteria penilaian dari masing-masing *tools*, yaitu: syarat input *file* dalam *hard disk*, opsi pencarian, informasi yang dapat diekstraksi atau ditampilkan oleh *tool*, kemampuan *recovery*, format *file* email yang didukung, dukungan visualisasi, sistem operasi yang didukung, perangkat tambahan yang didukung, dan format ekspor yang didukung. Kelima *tools* tersebut adalah MailXaminer, Aid4Mail, Digital Forensic Framework, eMailTrackerPro, dan Paraben E-Mail Examiner. Berdasarkan kriteria "informasi yang diekstraksi", hasil studi menunjukkan bahwa *tools* MailXaminer, Aid4Mail, dan Digital Forensic Framework hanya dapat menunjukkan rincian email, tanggal dan waktu dari suatu email. Sedangkan *tool* eMailTrackerPro dapat menampilkan alamat IP pengirim email beserta lokasi geografisnya. *Tool* ini juga mampu menemukan penyedia layanan jaringan (ISP) pengirim dan menampilkan tabel *routing* yang dapat mengidentifikasi jalur antara pengirim dan penerima email. *Tool* Paraben E-Mail Examiner menampilkan informasi yang tersedia berdasarkan hasil pemeriksaan *header* dan isi email, termasuk lampiran (Devendran, Shahriar, & Clincy, 2015).

Beberapa *tools* forensik email yang telah tersedia belum ada yang dapat memetakan informasi yang terdapat pada *header email* dengan menerapkan konsep 5W1H (*Who, What, When, Where, Why,* dan *How*). Penggunaan konsep 5W1H dalam dunia forensik ini dapat mempermudah proses investigasi karena dengan menerapkan metode ini, suatu kasus atau masalah dapat terpecahkan. Saat pertanyaan-pertanyaan konsep 5W1H dapat terjawab, hal ini membantu investigator untuk menemukan titik terang, bukti yang kuat, ataupun petunjuk yang merujuk ke bukti selanjutnya dari sebuah kasus yang sedang ditangani.

Prinsip 5W1H dalam dunia forensik dijabarkan sebagai berikut:

a. *Who* (siapa), akan menunjukkan siapa pengirim dan penerima email.
b. *What* (apa), akan menunjukkan subjek dari email dan file lampiran yang ada di dalam email.
c. *When* (kapan), akan menunjukkan kapan email dikirim oleh pengirim dan kapan email diterima oleh penerima.
d. *Where* (di mana), akan menunjukkan alamat IP serta lokasi *server* pengirim email.

e. *How* (bagaimana), akan menunjukkan proses pengiriman email dari pengirim hingga sampai di penerima, *server* apa saja yang dilewati dan protokolnya.
f. *Why* (mengapa), akan menunjukkan mengapa pengirim mengirim email kepada penerima.

Jawaban dari pertanyaan-pertanyaan *Who*, *What*, *When*, *Where*, dan *How* ini bisa didapatkan informasinya dari *header email*. Namun untuk jawaban pertanyaan *Why*, informasinya tidak secara langsung tersirat dari *header email*. Sehingga pada penelitian ini, fokus penelitian yang dikerjakan adalah melakukan pembacaan dari *header email* dan melakukan pemetaan informasinya untuk menjawab pertanyaan *Who*, *What*, *When*, *Where*, dan *How* (4W1H).

Penerapan konsep 4W1H dalam forensik email ini dapat menjelaskan dengan detail terkait kasus yang sedang diinvestigasi dan email menjadi barang bukti dalam kasus tersebut. Diharapkan dengan adanya *tool* ini dapat mempermudah investigator dalam melakukan aktivitas forensik email, karena *tool* ini dapat mengekstraksi dan memetakan informasi dari *header email* dengan cepat serta mudah untuk dibaca. Selain itu akan muncul tanda jika *header email* yang diujikan terindikasi sebagai *email fraud* atau *email spoofing*. Dari hasil ekstraksi tersebut, investigator dapat dengan mudah menemukan informasi mengenai siapa pengirim email, siapa penerima email, kapan email dikirim oleh pengirim, kapan email diterima oleh penerima dan informasi lainnya. Sehingga investigator dapat dengan mudah dan cepat dalam memperoleh serta membaca informasi penting yang terdapat dalam *header email*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, rumusan masalah dapat dituliskan sebagai berikut:

1. Bagaimana merancang suatu *tool* forensik email yang dapat membaca *header email* kemudian informasinya dipetakan ke dalam konsep 4W1H?
2. Bagaimana pengujian *tool* yang telah dibuat dalam mendukung proses investigasi?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. *Tool* yang dibuat dalam penelitian ini dapat mem-*parsing field* dari *header email*.

2. *Tool* mengambil *field* yang memuat informasi yang dapat menjawab pertanyaan 4W1H, yaitu *From*, *To*, *Cc*, *Bcc*, *Subject*, *Content-Disposition*, *Date*, *Received-SPF*, *Received*, dan *X-Received*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini, yaitu:

1. Merancang suatu *tool* untuk mendukung forensik email dalam membaca *header email* kemudian memetakan informasinya dengan konsep 4W1H.
2. Melakukan pengujian terhadap *tool* yang telah dibuat dalam proses investigasi.

1.5 Manfaat Penelitian

Melalui penelitian ini, diharapkan *tool* yang dibuat dapat memberikan kontribusi terhadap perkembangan ilmu pengetahuan di bidang forensika digital khususnya dalam forensik email. Serta membantu investigator dalam melakukan proses investigasi forensik terhadap *header email*.

1.6 Metode Penelitian

Metode penelitian merupakan langkah-langkah yang disusun untuk menyelesaikan penelitian secara sistematis. Dalam penelitian ini metode yang digunakan adalah sebagai berikut:

1. **Studi Literatur**

   Tahapan ini dilakukan pertama kali untuk mendapatkan informasi yang akan digunakan sebagai acuan dasar dan penunjang dari tema penelitian. Acuan dasar dan penunjang ini didapatkan dari berbagai sumber, seperti buku, artikel, *paper*, jurnal, makalah, dan laporan penelitian yang didapatkan secara *online* maupun *offline*. Studi literatur dilakukan untuk mencari informasi yang berkaitan dengan *header email* untuk memahami *value* dari masing-masing *field* yang ada pada *header*.

2. **Analisis Kebutuhan *Tool***

   Tahapan ini dilakukan untuk menganalisis kebutuhan *tool* yang akan dibuat. Kebutuhan ini meliputi proses-proses apa saja yang nantinya dapat dilakukan oleh *tool* yang dibuat. *Tool* diharapkan dapat membaca masukan berupa *header email*. Keluaran yang diharapkan adalah pemetaan dari informasi *header email* tersebut untuk menjawab pertanyaan-pertanyaan:

a. *Who* (siapa pengirim dan penerima email?)
b. *What* (apa subjek dari email? apa file lampiran yang ada pada email?)
c. *When* (kapan email dikirim dan diterima?)
d. *Where* (di mana letak server pengirim email?)
e. *How* (bagaimana proses pengiriman email dari pengirim ke penerima serta *server* apa saja yang dilewati dan protokolnya?)

3. Perancangan *Tool*

Metode yang digunakan untuk membuat *tool* ini adalah dengan membuat algoritma pembacaan *header* dari sebuah email kemudian dilakukan *parsing* berdasarkan *keyword* yang telah ditetapkan. Berikut *field* yang dibutuhkan untuk dapat menjawab pertanyaan-pertanyaan 4W1H:

a. Untuk menjawab *who*, dibutuhkan *field* "*From*", "*To*", dan "*Cc*".
b. Untuk menjawab *what*, dibutuhkan *field* "*Subject*" dan "*Content-Disposition*".
c. Untuk menjawab *when*, dibutuhkan *field* "*Date*" dan "*X-Received*".
d. Untuk menjawab *where*, dibutuhkan *field* "*Received*".
e. Untuk menjawab *how*, dibutuhkan *field* "*Received*".

Teknik *parsing* yang dilakukan oleh *tool* ini adalah dengan teknik pencarian *keyword* dari *field* yang dibutuhkan.

4. Implementasi *Tool*

Implementasi adalah proses penerapan rancangan yang telah dibuat sebelumnya. *Tool* akan melakukan *parsing* terhadap *header email* masukan, kemudian membaca *field*: "*From*", "*To*", "*Cc*", "*Subject*", "*Content-Disposition*", "*Date*", "*X-Received*", dan "*Received*". Dari semua *field* tersebut kemudian dipetakan untuk dapat menjawab pertanyaan-pertanyaan:

a. Siapa pengirim email?
b. Siapa penerima email?
c. Apa subjek dari email?
d. Apa file lampiran yang ada pada email?
e. Kapan email dikirim?
f. Kapan email diterima?
g. Di mana server pengirim email?
h. Bagaimana perjalanan email dari pengirim hingga sampai ke penerima?

Tool akan dibuat menggunakan bahasa pemrograman Java dengan *compiler* Netbeans IDE 8.0.

5. **Pengujian *Tool***

   Pada proses ini, akan diujikan sejumlah skenario email yang *header email*-nya dijadikan sebagai masukan untuk dibaca oleh *tool* dan kemudian hasil keluaran dari *tool* berupa informasi yang menjawab pertanyaan-pertanyaan: *Who*, *What*, *When*, *Where*, dan *How*. Pengujian dilakukan untuk menilai apakah proses penguraian *field header email* berhasil menjawab pertanyaan-pertanyaan tersebut.

1.7 Sistematika Penulisan

Berikut adalah sistematika penulisan yang merupakan gambaran secara umum tentang proses penelitian dan penulisan laporan yang dilakukan, terdiri dari:

Bab I Pendahuluan

Pada bab ini dijabarkan permasalahan yang menjadi latar belakang dilakukannya penelitian, di dalamnya berisi gambaran tentang perkembangan suatu sistem dan permasalahannya. Bab ini juga membahas perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan dalam penyusunan laporan.

Bab II Landasan Teori

Pada bab ini ditampilkan *literature review* sebelumnya yang berkaitan dengan penelitian yang dilakukan saat ini. Selain itu juga menjelaskan mengenai teori-teori yang terkait untuk memecahkan masalah dalam penelitian yang dilakukan.

Bab III Metode Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang akan digunakan, perancangan, implementasi, dan pengujian *tool* dengan beberapa skenario.

Bab IV Hasil dan Pembahasan

Pada bab ini akan dibahas hasil pengujian *tool* yang telah dilakukan dengan beberapa skenario yang telah ditetapkan.

Bab V Kesimpulan dan Saran

Pada bab ini akan dipaparkan kesimpulan dari hasil penelitian yang telah dilakukan beserta saran yang direkomendasikan untuk pengembangan penelitian selanjutnya.