

BAB 1

PENDAHULUAN

A. Latar Belakang Masalah

Pertumbuhan teknologi informasi dan komunikasi sangat cepat. *Email* adalah salah satu media yang digunakan untuk bertukar informasi data, gambar dan lainnya. Seiring perkembangan pesat pertukaran informasi dan komunikasi, menyebabkan kejahatan dunia maya berkembang. Jadi bagi para pelaku kejahatan dunia maya atau kejahatan dunia maya diperlukan bukti. Kejahatan yang dilakukan oleh *cybercrime* dapat dilakukan secara forensik melalui *email*. Penelitian ini akan melakukan forensik pada *email* dengan cara mengakuisisi *email* berbasis *android* sebagai bukti digital dengan menggunakan metode forensik dari *Institute Nasional Standar dan Teknologi (NIST)*. Pada tahap pengumpulan bukti yang dilakukan pada *smartphone Android lollipop 5.0.2 tipe Xiaomi Mi4i*, untuk melakukan akuisisi pada *email* berbasis *Android* maka *email* harus dibuka menggunakan *browser*. Dalam penelitian ini menggunakan *browser* asli dari android. Pada tahap pengujian, dari serangkaian proses yang telah dilakukan dalam memperoleh alamat *IP* pengirim di *header email*, selain alamat *IP* pengirim juga ditemukan alamat *IP* penerima, alamat *email* pengirim, protokol *email*, *email* pengirim waktu, waktu *email* yang diterima dan enkripsi *email*. Pada tahap akhir dari proses akuisisi dalam *email* berhasil dilakukan dengan memperoleh alamat *IP* mengirim

email di *header* sebagai bukti digital. Dalam penelitian selanjutnya dapat melacak alamat *IP* pengirim *email*. Umar, et al (2018)

Email telah menjadi pembawa utama untuk mengirim spam dan konten berbahaya melalui jaringan. *Email* juga merupakan sumber utama berbagai kegiatan kriminal di Internet. *Computer Forensics* adalah proses sistematis untuk menyimpan dan menganalisis *email* yang disimpan untuk keperluan proses hukum dan masalah sipil lainnya. Analisis *email* sangat menantang karena tidak hanya berbagai bidang yang dapat dipalsukan oleh peretas atau pengguna jahat, tetapi juga fleksibilitas penyusunan, pengeditan, penghapusan *email* menggunakan *offline* (mis., *MS Outlook*) atau *online* (mis., *Surat Web*) aplikasi *email*. Menuju ke arah ini, sejumlah alat forensik *open source* telah banyak digunakan oleh para praktisi. Namun, alat-alat ini telah dikembangkan secara terisolasi daripada pendekatan kolaboratif. Mengingat bahwa pengguna alat forensik *email* perlu memahami sejauh mana alat akan berguna untuk keadaannya dan melakukan analisis forensik yang sesuai. Dalam tulisan ini, kami menguji serangkaian fitur umum untuk membandingkan dan membedakan lima alat forensik *email open source populer*. Studi ini menemukan bahwa semua alat forensik email tidak serupa, menawarkan jenis fasilitas yang berbeda. Dengan menggabungkan alat analisis, dimungkinkan untuk memperoleh informasi terperinci di bidang forensik *email*. Devendran, et al (2015)

Tindak kejahatan dalam bentuk penipuan dapat menggunakan berbagai macam media sosial yang salah satunya *Gmail*, aplikasi tersebut

dapat untuk melakukan kejahatan penipuan berupa transaksi *chat* yang didalamnya berupa pesan teks, gambar, dan video untuk melakukan transaksi penipuan. Kejahatan digital ini berbentuk penipuan dari pelaku terhadap korban dalam proses mengirimkan berita palsu yang akan dilaksanakan seminar *android* dan korban sudah mengirimkan uang pendaftaran untuk mengikuti seminar tetapi setelah mengkonfirmasi kepada pihak yang bersangkutan, tidak ada yang mengirimkan berita akan diadakannya seminar *android*. Dengan adanya penipuan ini maka membutuhkan *Software Ftk Imager* untuk mengambil data bukti transaksi penipuan antara pelaku dan korban untuk dapat dijadikan barang bukti yang akan di proses ke ranah hukum.

B. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah :

1. Bagaimana pengujian *NIST* untuk melakukan analisis bukti digital pada *E-mail* ?
2. Bagaimana pengujian analisis forensik pada *email* untuk pembuktian digital yang diharapkan menjadi barang bukti dalam penanganan kasus penipuan ?

C. Batasan Masalah

Batasan penelitian berikut :

1. Proses analisis pada metode *NIST (National Institute of Standards and Technology)* Kent et al., (2017) antara lain :
 - a) *Collection, Examination, Analysis, Reporting*

- b) Barang bukti yang dicari pada *email* adalah pesan *teks*, gambar, yang telah dihapus.
- c) Proses tracking *email* hanya untuk mengetahui alamat pengirimnya.

2. Pembuktian forensik pada barang bukti digital menggunakan *Gmail*

antara lain :

- a) Pengumpulan barang bukti.
- b) Proses akuisisi dan analisis menggunakan sistem operasi *windows* 8 64 bit.
- c) Laptop dalam keadaan menyala untuk melakukan analisis.
- d) Akun *email* dalam keadaan *login* pada *web*.

D. Tujuan Penelitian

Tujuan penelitian ini adalah untuk mendapatkan bukti digital untuk dijadikan bukti-bukti kejahatan sesuai dengan konsep analisis bukti digital penipuan dan pencemaran nama baik dengan metode *NIST*.

E. Manfaat Penelitian

Manfaat dari penelitian ini antara lain :

1. Menambah pengetahuan tentang investigasi media sosial *Email* untuk membantu pihak yang berkepentingan untuk mengungkap kasus kejahatan digital yang menggunakan *Email* sebagai sarana komunikasinya.
2. Mengetahui proses akuisisi dan analisis pada *Email*.