BAB II

TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Penelitian lain yang dilakukan Suryana, et al (2016) *Email spoofing* dianggap sebagai tindakan membahayakan, karena melakukan manipulasi data pada *header email* untuk menyamar sebagai orang atau organisasi yang sah, contonya seperti melakukan pengerimian email dengan nama pengirim seolah dari administrator suatu organisasi. Pengirim *email spoofing* menyerang dengan berbagai macam isi pesan untuk membuat percaya korban yang menerimai *email* tersebut.

Penelitian lain yang dilakukan Mustafa, et al (2018) untuk melakukan analisis forensik pada sistem komputer dibutuhkan sebuah metode dan *tools* yang akan membantu investigator untuk melakukan investigasi forensik. Penelitian ini dimuali dengan pemilihan *tools* untuk membuat sebuah *email* palsu, yang kemudian dikirimkan keada korban sesuai dengan skenario. *Tools* yang digunaan dalam pembuatan *email* palsu hendaknya mempunyai akses bebas dan mudah digunakan. Sedangkan untuk metode yang digunakan pada saat tahap analisis *email* palsu tersebut adalah *header* analisis, dimana pada setiap bagian *Header email* memuat *filed-filed* seperti *from, to, subject, date, received,* dan yang lainnya.

Penelitian yang dilakukan oleh Kent et al., (2017) semua orang dapat menghapus *email* setelah membaca atau menggunakan konten penting dari isi pesan *email*. Berdasarkan studi rinci berbagai parameter seperti *Header* Analisis struktur *Email*, pelacakan *header E-mail*, pelacakan *IP*, *Bait Tactics, email* yang dihapus dari sampah terlihat. *Email* yang dihapus dapat dipulihkan dan dipulihkan dari tempat sampah / daur ulang dari *Yahoo, Rediff, Gmail* dan *email* lainnya jika secara tidak sengaja atau sengaja dihapus, tetapi jika *email* dihapus dari tempat sampah / daur ulang, peluang untuk memulihkannya sangat kecil. Dan karenanya terlihat bahwa lebih sedikit pekerjaan yang dilakukan pada email yang dihapus secara permanen.

Penelitian yang dilakukan oleh Faiz, et al (2017) *browser* merupakan salah satu aplikasi yang berguna untuk menerjemahkan *HTML* menjadi Bahasa yang dapat dipahami oleh *user*. Keamanan pada *browser* merupakan suatu tantangan tersendiri untuk mengembangkan fitur kemanan dan kemudahan dalam menggunakan *browser*. *Microsoft Edge* merupakan *browser default* dari *Windows 10* dengan berbagai fitur yang lebih baik dari *Internet Explorer* namun ternyata untuk segi keamanan lebih lemah jika dibandingkan dengan *browser Mozilla Firefox,* sedangkan *Google Chrome* lebih kuat pada passwordnya.

Penelitian yang dilakukan oleh Nataliana (2013) dirancang sebuah liasistem penjejakan mandiri *(personal tracking)* mempergunakan media *SMS* sebagai media pengiriman paket data koordinat posisi. Mekanisme

kerja sistem ini yakni jika posisi *GPS receiver* atau posisi *device* dan posisi pengamat berbeda ditempat yang berbeda, pengamat dapat mengetahui posisi *GPS receiver* dengan melakukan koneksi dengan *GPS receiver* tersebut guna mendapatkan data posisi. Setelah *GPS receiver* mempunyai data posisi dan pengamat ingin memperoleh posisi tersebut pada saat itu juga *(real time)* maka dibutuhkan sebuah media guna pengiriman data posisi alat yang diinginkan oleh pengamat. Dalam hal ini dipergunakan sebuah teknologi yang sudah umum digunakan yakni teknologi *SMS*. Dengan teknologi SMS maka *device personal tracking* perlu adanya penambahan modul yang berfungsi umtuk mengirimkan data posisi layaknya ponsel. Dengan kata lain perancangan dan realisi dimaksudkan guna mengadopsi kinerja ponsel yang diintergrasikan kedalam perangkat tracking, sehingga dimanapun dan kapanpun selama *device tracking* tersebut aktif maka pengamat dapat memperoleh data posisi *device* tersebut dimanapun berada.

B. Landasan Teori

1. E-mail

Menurut Hadianto, et al (2017) *e-mail* merupakan metode umum untuk berkomunikasi antara kedua belah pihak. Hal tersebut merupakan *file transfer* antara dua *server* pada nomor *port* yang spesifikasi. Sebuah *e-mail* biasanya ditulis pada sebuah aplikasi yang ada pada sisi *client (Web Client, MS otlook, Lotus Notes)* denga identitas pengirim, disimpan

dalam bentuk *file* , lalu dikirim kealamat tujuan melalui satu atau beberapa *server*. Meskipun komunikasi lewat *e-mail* telah dirancang agar segalanya menjadi lebih mudah,efisien, dan *powerfull*, penulisan *e-mail* dan komunaksinya telah menjadi fokus dari penyusup selama beberapa puluh taun, menemukan bahwa sangat bisa *e-mail* menjadi sumber transportasi umtuk mengantarkan isi pesan yang mengganggu, jahat, *siping*, dan *spam*.

2. Digital Forensik

Menurut Al-Azhar (2012) komputer forensik atau digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice),* yang dalam haini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara *scientific* (ilmiah) hingga bisa mendapatkan bukti – bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan. Hal yang sangat mendasar untuk dipahami oleh seseorang ahli digital forensik adalah prinsip – prinsip dasar digital forensik itu sendiri. Dalam hal ini *ACPO* (*Association of chief police officers)* merupakan asosiasi para pemimpin kepolisian di Inggris yang berkerja sama dengan *7safe*, sangat jelas menyatakan prinsip – prinsip dasar digital forensik sebagai berikut :

a. *No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.* (Sebuah. Tidak ada tindakan yang dilakukan oleh lembaga penegak hukum atau agen

mereka yang harus mengubah data yang disimpan di komputer atau media penyimpanan yang selanjutnya dapat diandalkan di pengadilan)

b. *In circumstances where a person finds it necessary to access original data held on a computer or an storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.* (Dalam keadaan di mana seseorang merasa perlu untuk mengakses data asli yang disimpan di komputer atau media penyimpanan, orang tersebut harus kompeten untuk melakukannya dan dapat memberikan bukti yang menjelaskan relevansi dan implikasi tindakan mereka.)

c. *An audit trail or the record of all processes applied to computer-based electronic evidence should be created and preserved, an independent third party should be able to examine those processes and achieve the same result.* (Jejak audit atau catatan semua proses yang diterapkan pada bukti elektronik berbasis komputer harus dibuat dan dilestarikan, pihak ketiga yang independen harus dapat memeriksa proses-proses tersebut dan mencapai hasil yang sama.)

d. *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.* (Orang yang bertanggung jawab atas penyelidikan

(petugas kasus) memiliki tanggung jawab keseluruhan untuk memastikan bahwa hukum dan prinsip-prinsip ini dipatuhi)

3. Komputer Forensik

Menurut Al-Azhar. (2012) pemeriksaan dan analisa barang bukti elektronik berupa koputer PC (*Personal Komputer*), laptop/*notebook*, *netbook* dan *tablet*. Pemeriksaan teerhadap jenis barang bukti ini biasanya berkaitan dengan *files recovery*, yaitu suatu metode untuk mengambil *file logical* atau memunculkan kembali *file* yang sudah dihapus (*deleted*) maupun hilang *(lost)* dikarenakan tidak tercatat lagi di *file system.*

4. National Institute of Standards and Technology (NIST)

Menurut Kent et al. (2017) penjelasan dari *National Institute of Standards and Technology (NIST)* yakni *collection, examination, analysis, dan reporting* sebagai berikut :

1. *Collection*

   Mengidentifikasi, memberi label, merekam, dan memperoleh data dari sumber yang mungkin dari data yang relavan, sambil mengikuti prosedur yang menjaga intergrasi data.

2. *Examination*

   Memproses data yang dikumpulkan secara forensik menggunakan kombinasi metode otomatis dan manual, dan menilai serta mengekstrasi data yan menarik, sambil menjaga integritas data.

3. *Analysis*

Menganalisis hasil pemeriksaan, menggunakan metode dan teknik yang dapat dibenarkan secara hukum, untuk memperoleh informasi berguna yang membahas pertanyaan-pertanyaan yang menjadi dorongan untuk melakukan pengumpulan dan pemeriksaan.

4. *Reporting*

Melaporkan hasil analisis, yang mungkin termasuk menggambarkan tindakan yang digunakan, menjelaskan bagaimana alat dan prosedur dipilih, menentukan tindakan apa yang perlu dilakukan (misalnya, pemeriksaan forensik sumberdata tambahan, mengamankan kerentanan yang diidentifikasi, meningkatkan keamanan yang ada kontrol), dan memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses forensik.

5. **FTK *(Forensic Tool Kit)***

Menurut Nikkel. (2016) FTK adalah alat yang dapat mengambil data dari perangkat, fitur yang didukung antara lain metadata, kompresi, pemecahan file keluaran (Fragmen gambar), *hashing* dan data yang terenskripsi. FTK tersedia pada beberapa sistem operasi yaitu *debian linux, fedora linux, OS X, dan windows.*