

BAB I

PENDAHULUAN

1.1 Latar Belakang

Bukti digital dalam penyelidikan terus berkembang dengan kemajuan teknologi, kita dihadapkan pada perangkat digital yang lebih baru, artefak yang lebih banyak dan berbagai macam format file, perkembangan tersebut membawa keuntungan, dan pada saat yang bersamaan memberikan peluang baru bagi kejahatan di bidang teknologi informasi. Berbagai jenis pelanggaran dan tindak kejahatan dalam dunia komputer khususnya masalah data atau *file*, seperti pencurian data, penggandaan data, penghapusan data sampai dengan masalah memanipulasikan data yang semakin sering terjadi pada saat ini. (Raghavan & Raghavan, 2014a).

Berbagai kasus yang terjadi saat ini, adanya bukti digital yang dapat membantu investigator mengungkap suatu kasus tindak pidana. Salah satunya melalui informasi mengenai isi dari sebuah data atau file yang di sebut dengan metadata file.

Metadata merupakan informasi yang tertanam pada sebuah file berupa penjelasan tentang file tersebut. Metadata mengandung informasi mengenai isi dari suatu data yang dipakai untuk keperluan manajemen file atau data itu nantinya dalam suatu basis data. Metadata sering disebut “informasi tentang informasi” atau “data tentang data”.

Investigator analisis forensik dalam penanganan bukti digital utama dengan pendekatan berbasis metadata masih banyak secara manual dalam mencari korelasi file

yang terkait. File yang dikorelasikan berada dilokasi (folder) yang terpisah dan banyaknya file tentu akan menjadi tantangan yang berat bagi para investigator forensik dalam menganalisis barang bukti digital tersebut.

Metadata forensik pernah dilakukan oleh penelitian sebelumnya tetapi dengan membangun tools dan parameter yang berbeda. Penelitian dengan berbasis metadata forensik pernah dilakukan oleh (Subli, Sugiantoro & Prayudi, 2017). Dalam penelitiannya membuat sebuah sistem metadata forensik untuk membaca karakteristik metadata secara umum dan mencari file-file korelasi metadata dengan salah satu parameter yaitu *file owner*, *file size*, *file date* dan *file type*. Menurut (Raghavan & Raghavan, 2013) Dengan menggunakan tools metadata forensik tentu akan sangat mempermudah investigator dalam menganalisis korelasi bukti digital.

Penelitian yang dilakukan ini untuk memahami dan membaca karakteristik metadata secara umum dan detail metadata yang spesifik dan mengidentifikasi, menganalisis korelasi metadata untuk mengelompokkan file yang terkait atau hubungan yang di anggap relevan dalam konteks penyelidikan secara otomatis berdasarkan parameter metadata yaitu *Author*, *Size*, *File Type* dan *Date*. Menggunakan beberapa dan seluruh parameter yang sudah ditentukan, sehingga dapat memperbanyak temuan barang bukti dan mempermudah analisis bukti digital tersebut. Penelitian ini diharapkan dapat memberikan kontribusi pada analisis forensik dalam menganalisis korelasi bukti digital dengan pendekatan berbasis metadata.

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini sebagai berikut.

- a. Bagaimanakah karakteristik metadata file
- b. Bagaimana menentukan korelasi antara file Bukti Digital
- c. Bagaimana menguji kinerja sistem untuk melakukan analisis metadata file dalam proses investigasi

1.3 Batasan Masalah

Batasan masalah pada penelitian metadata forensik ini sebagai berikut:

- a. Membaca karakteristik metadata secara umum dan detail metadata.
- b. Parameter korelasi metadata yang berdasarkan *Author*, file type (*type file*), tanggal file (*file date*), ukuran file (*file size*).
- c. File yang diuji dan dipahami ada beberapa jenis diantaranya file dengan ekstensi *Jpg, Mp4, dan wmv* yang berada pada komputer bukan berdasarkan hasil *imaging/akuisisi*.

1.4 Tujuan Penelitian

Tujuan dalam penelitian metadata forensik ini antara lain:

- a. Melakukan pembacaan metadata untuk memahami karakteristik metadata setiap file
- b. Melakukan korelasi metadata file yang bisa mencari file-file yang terkait.
- c. Melakukan pengujian kinerja sistem untuk melakukan analisis metadata file dalam sebuah proses investigasi bukti digital.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dalam penelitian metadata ini dapat memberikan kontribusi antara lain:

- a. Mempermudah seorang analisa/investigator dalam memahami karakteristik metadata setiap file.
- b. Mempermudah seorang analisa/investigator dalam menemukan file-file yang terkait dengan korelasi metadata file

1.6 Literatur Penelitian

Berikut ini akan dibahas ulasan tentang penelitian yang telah dilakukan sebelumnya yang berkaitan dengan metadata antara lain.

(Salama, Varadharajan & Hitchens, 2012) menganalisis berbagai jenis metadata yang umum tersedia dengan objek digital seperti foto dan dokumen yang tersedia di Internet. Dan menganalisis berbagai jenis informasi metadata yang dihasilkan oleh kamera dan perangkat smartphone yang digunakan untuk menangkap dan menyimpan foto digital di web. Mengembangkan peraturan heuristik yang dapat digunakan untuk meningkatkan kualitas pengambilan keputusan dalam investigasi forensik. Dan menekankan perlunya melindungi metadata.

(Crossley, Asimakopoulou, Sotiriadis, & Bessis, 2013) dalam penelitiannya mengatakan penyimpanan data komputasi *cloud* dan dampak penandaan metadata sebagai metode potensial untuk melacak informasi file asli. untuk mengatasi masalah yang diajukan ke pemeriksa forensik yang mencoba menganalisis format file gambar

yang dapat dipertukarkan dari ekstensi file nama jpg untuk gambar yang telah disimpan di dalam *cloud* untuk mengidentifikasi informasi.

Penelitian yang sama dilakukan oleh (Raghavan & Raghavan, 2013) dalam penelitiannya menyajikan mesin analisis AssocGEN yang menggunakan metadata untuk menentukan asosiasi antara artefak *file user*, *log* dan pembuangan paket jaringan dan mengidentifikasi metadata untuk mengelompokkan dan menentukan korelasi antara artefak dan kelompok artefak yang terkait.

Penelitian yang dilakukan oleh (Woods, Cassanhoff & A Lee 2013) berfokus pada metadata yang dihasilkan oleh *tools open-source* yang mendukung Digital Forensik XML (DFXML). Bagaimana bagian-bagian dari metadata ini dapat digunakan saat merekam peristiwa PREMIS untuk menggambarkan kegiatan yang relevan dengan pelestarian dan akses dari metadata tersebut.

Penelitian lain juga dilakukan oleh (Raghavan & Raghavan, 2014) Melakukan analisis metode untuk secara otomatis mengidentifikasi asosiasi di antara bukti digital pada sintaksis dan tingkat semantik menggunakan metadata. penerapan metode ini untuk mengidentifikasi asosiasi metadata dari koleksi gambar dokumen-dokumen, dokumen pengolah kata dan menghasilkan interkom korelasi untuk tujuan mengidentifikasi atau file yang relevan dari kumpulan file besar dalam bukti digital. menunjukkan bahwa hubungan file yang diidentifikasi dengan menggunakan bantuan metadata dalam mengidentifikasi foto-foto dan dokumen yang dicopy.

(Alanazi & Jones, 2015) mengatakan bagaimana menggunakan berbagai format dan jenis metadata untuk memvalidasi berbagai jenis dokumen dan file yang memiliki

sejumlah format dan jenis metadata, yang dapat digunakan untuk menemukan properti dari file, dokumen atau aktivitas sebuah jaringan. Selain itu pula, metadata banyak digunakan di kondisi apapun, dimana metadata dapat memberikan beragam bukti antara sekelompok orang, karena sebagian diantaranya tidak mengetahui jenis informasi yang tersimpan dalam dokumen mereka.

(Spore & Andy, 2016) mengatakan tujuan pemeriksaan forensik terhadap metadata yaitu mengaitkan data dengan informasi lain, pengguna yang mengaksesnya, direktori file tempat penyimpanannya, terakhir kali dicopy, dan sebagainya. Dalam sebuah kasus Metadata dapat menghasilkan bukti tidak langsung untuk mendukung barang bukti. Anda bisa melihat bagaimana file diakses, sesuai urutan, dan oleh siapa. Hampir semua tindakan yang Anda lakukan dengan sebuah file mengubah beberapa aspek metadatanya. Dengan analisis forensik yang tepat, metadata dapat membantu menyoroti pola, menetapkan *timelines*, dan menunjukkan kesenjangan dalam data.

Penelitian berikutnya dilakukan oleh (Kumar et al., 2016) mengatakan suatu hari sorang secara langsung dan tidak langsung sudah banyak sekali perangkat pintar yang melekat. Seseorang dapat menemukan keberadaannya jika kita memantau perangkat yang mereka gunakan dengan mengumpulkan metadata foto yang diposkan oleh mereka di media sosial. Beberapa situs sosial media memiliki fitur untuk memposting tempat masa lalu mereka. Untuk menyediakan aplikasi Android sederhana, ini akan menggunakan fitur *Geo tagging* yang tersedia dengan sebagian besar smartphone. Dan dengan menggunakan data berbasis lokasi ini bisa melacak orang berdasarkan garis bujur dan garis lintang dari *Global Positioning System (GPS)*. bisa menggunakan ini

untuk mengumpulkan foto yang diposkan oleh seseorang dan menganalisisnya untuk mengetahui posisi mereka saat ini. memverifikasi metadata yang terkait dengan gambar dan melacak di suatu negara, kota, *rute*, dan jalan negara berdasarkan Ketinggian GPS, GPS Latitude, GPS Bujur dan posisi GPS.

(Subli, Sugiantoro & Prayudi, 2017) penelitiannya dengan melakukan pendekatan metadata, maka diharapkan proses ini bisa melihat langsung metadata file secara umum dan juga dapat menemukan file-file berdasarkan korelasi file dengan parameter dari metadata file tersebut. Menggunakan salah satu parameter yang sudah ditentukan.

Penelitian ini konsep yang akan diusulkan dan yang membedakan dengan penelitian sebelumnya adalah pada segi teknik pencarian korelasi dengan memanfaatkan metadata file dengan beberapa atau keseluruhan parameter yang sudah ditentukan bisa mengkorelasikan file yang satu dengan yang lainnya apabila file tersebut terkait.

1.7 Metodologi Penelitian

Penelitian perlu disusun langkah-langkah penyelesaian penelitian secara sistematis yang disebut dengan metodologi, adapun metodologi yang digunakan pada penelitian ini menggunakan *Framework DFRWS (Digital Forensic Research Workshop)* sebagai berikut:

1. Identification

Tahap identifikasi masalah adalah tahap awal dalam penelitian ini yaitu merumuskan masalah yang akan di jadikan sebagai objek penelitian

2. *Preservation*

Tahapan ini disebut juga pelestarian bukti digital melibatkan tugas-tugas seperti menyiapkan manajemen kasus yang tepat dan memastikan dapat diterima di pengadilan. Mengisolasi, mengamankan, dan melestarikan keadaan bukti fisik dan digital, ini termasuk mencegah pihak yang tidak bertanggung jawab menggunakan perangkat digital atau membiarkan perangkat elektromagnetik lain digunakan dalam radius yang terpengaruh.

3. *Collection*

Metode yang digunakan untuk mengumpulkan data pada penelitian ini yaitu dengan melakukan studi literatur. Studi literatur dilakukan untuk mencari semua informasi yang berkaitan tentang konsep metadata forensik dalam membaca atau memahami karakteristik metadata file dan memudahkan pencarian dalam korelasi metadata file, seperti membaca buku-buku, paper atau jurnal-jurnal dan mengunjungi situs-situs yang ada di internet yang berhubungan dengan metadata forensik

4. *Examination*

Pencarian bukti yang mendalam dan sistematis terkait dengan dugaan kejahatan, berfokus mengidentifikasi dan menemukan bukti potensial, mungkin di dalam lokasi yang tidak konvensional, bangun dokumentasi terperinci untuk analisis.

5. *Analysis*

Tahap ini menentukan signifikansi, merekonstruksi fragmen data dan menarik kesimpulan berdasarkan bukti yang ditemukan. Mungkin diperlukan beberapa pemeriksaan dan analisis untuk mendukung teori kejahatan.

6. *Presentation*

Merangkum dan memberikan penjelasan kesimpulan. Harus ditulis dalam istilah orang awam menggunakan istilah abstrak. Istilah yang diabstraksikan harus merujuk pada detail spesifik.

1.8 Sistematika Penulisan

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis

dan evaluasi dari penelitian yang diangkat.

BAB V PENUTUP

Bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.