VOL. 18 NO. 1 MARET 2017

ISSN : 1411-3201

Jurnal Ilmiah DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

UNIVERSITAS AMIKOM YOGYAKARTA

VOL. 18 NO. 1 MARET 2017 ISSN:1411-3201

JURNAL ILMIAH DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

UNIVERSITAS
AMIKOM
YOGYAKARTA

VOL. 18 NO. 1 MARET 2017
JURNAL ILMIAH
Data Manajemen Dan Teknologi Informasi

Terbit empat kali setahun pada bulan Maret, Juni, September dan Desember berisi artikel hasil penelitian dan kajian analitis kritis di dalam bidang manajemen informatika dan teknologi informatika. ISSN 1411-3201, diterbitkan pertama kali pada tahun 2000.

PENANGGUNG JAWAB :
Rektor UNIVERSITAS AMIKOM YOGYAKARTA, Prof. Dr. M. Suyanto, M.M.

ALAMAT PENYUNTING & TATA USAHA
UNIVERSITAS AMIKOM YOGYAKARTA, Jl. Ring Road Utara Condong Catur Yogyakarta, Telp. (0274) 884201 Fax. (0274) 884208, Email : jurnal@amikom.ac.id

BERLANGGANAN
Langganan dapat dilakukan dengan pemesanan untuk minimal 4 edisi (1 tahun)
pulau jawa Rp. 50.000 x 4 = Rp. 200.000,00 untuk luar jawa ditambah ongkos kirim.

VOL. 18 NO. 1 MARET 2017 **ISSN : 1411- 3201**

JURNAL ILMIAH

DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

UNIVERSITAS AMIKOM YOGYAKARTA

JURNAL ILMIAH

DASI

KATA PENGANTAR

Puji syukur kehadlirat Tuhan Yang Maha Kuasa atas anugerahnya sehingga jurnal edisi kali ini berhasil disusun dan terbit. Beberapa tulisan yang telah melalui koreksi materi dari mitra bestari dan revisi redaksional dari penulis, pada edisi ini diterbitkan. Adapun jenis tulisan pada jurnal ini adalah hasil dari penelitian dan pemikiran konseptual. Redaksi mencoba selalu mengadakan pembenahan kualitas dari jurnal dalam beberapa aspek.

Beberapa pakar di bidangnya juga telah diajak untuk berkolaborasi mengawal penerbitan jurnal ini. Materi tulisan pada jurnal berasal dari dosen tetap dan tidak tetap UNIVERSITAS AMIKOM Yogyakarta serta dari luar UNIVERSITAS AMIKOM Yogyakarta.

Tak ada gading yang tak retak begitu pula kata pepatah yang selalu di kutip redaksi, kritik dan saran mohon di alamatkan ke kami baik melalui email, faksimile maupun disampaikan langsung ke redaksi. Atas kritik dan saran membangun yang pembaca berikan kami menghaturkan banyak terimakasih.

Redaksi

DAFTAR ISI

METADATA FORENSIK UNTUK MENDUKUNG PROSES INVESTIGASI DIGITAL

Moh. Subli [1], Bambang Sugiantoro [2], Yudi Prayudi [3]

[1]Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia
[2]Teknik Informatika UIN Sunan Kalijaga Yogyakarta
[3]Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia
Email : li_kerta89@yahoo.com [1], bambang.sugiantoro@uin-suka.ac.id [2], prayudi@staff.uii.ac.id [3]

Abstraksi

Metadata adalah informasi yang terstruktur yang menggambarkan, menjelaskan, menempatkan, atau membuat lebih mudah untuk mengambil, menggunakan, atau mengelola sebuah sumber informasi. Metadata sering disebut data tentang data atau informasi tentang informasi. Selama ini fokus dari analisis forensik itu lebih banyak kepada menemukan file-file yang contennya itu sesuai dengan tujuan investigasi. Cara lain yang bisa dilakukan yaitu dengan melakukan pendekatan metadata, mengapa metadata karena metadata menyimpan informasi lain dari sebuah file. Apabila ini dilakukan, 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. Cara ini umumnya belum terfasilitasi oleh alat-alat forensik yang ada, sehingga perlu dilakukan penelitian untuk melihat sejauh mana kemungkinan kemanfaatan metadata untuk mendukung proses investigasi digital.

***Kata Kunci** :*
Metadata File, Korelasi File, Sistem Aplikasi Metadata Forensik

Abstract

Metadata is structured information that describes, explains, locates, or make it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. During this time the focus of the forensic analysis was more to find the files that contennya accordance with the purpose of the investigation. Another way to do that is by doing approach metadata, why metadata for metadata store other information from a file. If this is done, it is expected that this process can be viewed directly metadata files in general and also be able to find files based on file correlation with the parameters of the metadata file. This method is generally not facilitated by forensic tools are there, so research must be done to see the extent to which the possibilities for the benefit of metadata to support digital investigation process.

***Keyword** :*
File Metadata, File Correlation, Application System Metadata Forensics

Pendahuluan

Metadata adalah informasi yang terstruktur yang menggambarkan, menjelaskan, menempatkan, atau membuat lebih mudah untuk mengambil, menggunakan, atau mengelola sebuah sumber informasi. Metadata sering disebut data tentang data atau informasi tentang informasi [1]. Metadata adalah informasi yang ditanam pada sebuah file yang isinya berupa penjelasan tetang file tersebut. Metadata ini mengandung informasi mengenai isi dari suatu data yang dipakai untuk keperluan manajemen file atau data itu nantinya dalam suatu basis data [2]. Melalui informasi metadata diharapkan pengguna data dapat mengintepretasikan data secara sama, bilamana pengguna melihat langsung data spasialnya. Dokumen metadata berisikan informasi yang menjelaskan karakteristik data terutama isi, kwalitas, kondisi dan cara perolehannya. Metadata dipergunakan untuk melakukan dokumentasi data spasial yang berhubungan tentang siapa, apa, kapan, dimana, dan bagaimana data spasial dipersiapkan [3].

Metadata adalah informasi tambahan yang menyertai dan mendeskripsikan tentang sebuah data tertentu. Misalnya, sebuah gambar memiliki metadata yang menginformasikan seberapa besar ukuran file gambar, kedalaman warnanya, resolusinya, kapan dibuat, dan sebagainya. Contoh lain, metadata sebuah dokumen teks berisi informasi tentang seberapa panjang dokumen tersebut, siapa yang membuat, kapan ditulis, dan ringkasan isinya. Adapun metadata pada halaman website adalah bagian yang dituliskan pada tag meta di bagian header halaman web, misalnya deskripsi singkat tentang website dan keywordnya [4].

Metadata direkam komputer secara otomatis saat sebuah file dibuat, sehingga bisa diketahui kapan file dibuat, siapa user pembuatnya, berapa ukuran filenya, demikian juga ekstensinya. Namun demikian, metadata juga dapat disusun secara manual. Untuk mengedit dan membaca metadata sebuah file, digunakan software pengolah metadata Sebagian informasi metadata juga bisa kita baca dengan melakukan klik kanan Properties pada file tersebut [5].

Selama ini fokus dari analisis forensik itu lebih banyak kepada menemukan file-file yang contennya itu sesuai dengan tujuan investigasi. Cara lain yang bisa dilakukan yaitu dengan melakukan pendekatan metadata, mengapa metadata karena metadata menyimpan informasi lain dari sebuah file. Apabila ini dilakukan, 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. Cara ini umumnya belum terfasilitasi oleh alat-alat forensik yang ada, sehingga perlu dilakukan penelitian untuk melihat sejauh mana kemungkinan kemanfaatan metadata untuk mendukung proses investigasi digital.

Sehingga dalam penelitian ini dibuatlah sebuah sistem aplikasi metadata forensik. Sistem aplikasi ini dibuat untuk memudahkan dalam memahami karakteristik metadata file secara umum dan memudahkan pencarian file-file berdasarkan korelasi metadata file tersebut.

Tinjauan Pustaka

Beberapa penelitian yang berhubungan dengan metadata forensik yaitu penelitian yang dilakukan oleh Usama Salama, Vijay Varadharajan, & Michael Hitchens (2012) [6] dalam penelitian ini bahwasanya peneliti telah menyelidiki berbagai jenis metadata yang umumnya tersedia dengan benda-benda digital seperti foto dan dokumen yang tersedia di Internet dan telah menganalisis berbagai jenis informasi metadata yang dihasilkan oleh perangkat kamera dan smartphone yang digunakan untuk menangkap dan menyimpan foto digital di web. Analisis yang digunakan adalah dengan pengembangan aturan heuristik yang dapat digunakan untuk meningkatkan kualitas pengambilan keputusan dalam penyelidikan forensik.

Penelitian yang sama di lakukan juga oleh M.P. Roberts & J. Haggerty (2013)[7] tentang peningkatan penggunaan internet untuk menyimpan data yang dipastikan bahwa tersedianya sumber daya yang berharga untuk pemeriksa forensik selama penyelidikan. Yang menarik adalah bukti yang terkait dengan penyebaran gambar tidak senonoh anak-anak yang menyebar melalui situs jejaring sosial dan forum web.

Penelitian lain juga dilakukan Sriram Raghavan & S V Raghavan (2013)[8] Secara tradisional, sumber bukti digital yang di analisis oleh individual meneliti berbagai artefak yang terkandung di dalamnya dan menggunakan metadata artefak untuk memvalidasi keaslian urutan mereka. Namun, ketika artefak dari gambar forensik, folder, file log, dan pembuangan paket jaringan telah di analisis, pemeriksaan artefak dan metadata dalam isolasi menghadirkan tantangan yang signifikan. Idealnya, ketika sebuah sumber diperiksa, itu adalah tugas yang berharga untuk menentukan korelasi antara artefak dan kelompok artefak yang terkait.

Selanjutnya Mark Phillips (2013)[9] menjelaskan metodologi secara keseluruhan, memperkenalkan dua tools opensource sederhana yang dikembangkan untuk membantu memberikan contoh perintah dalam menunjukkan beberapa permintaan analisis metadata secara umum dan Kam Woods, Alexandra Chassanoff & Christopher A. Lee (2013)[10] fokus 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.

Volume besar metadata tersedia dalam infrastruktur database untuk keperluan penyelidikan tetapi sebagian besar usaha terletak pada pengambilan dan analisis informasi yang dari sistem komputasi. Dengan demikian, dalam penelitian ini terutama relevansi metadata dalam desain dari alat forensik database yang umum independen dari DBMS yang difokuskan untuk digunakan. (Shraddha Suratkar & Harmeet Khanuja 2014)[11].

Begitu juga dalam lain yang mengkatakan bahwa metadata tidak terlihat saat melihat data dalam sejumlah bentuk seperti dokumen docx atau jpg. Namun demikian, pertimbangan penting dalam penemuan informasi untuk digunakan dalam investigasi forensik digital. Berbagai jenis dokumen dan file memiliki sejumlah format dan jenis metadata, yang dapat digunakan untuk menemukan sifat-sifat dari aktivitas file, dokumen atau jaringan. Selain itu, Metadata berguna dalam banyak keadaan, di mana ia dapat memberikan bukti kolaborasi antara kelompok orang, karena beberapa dari mereka tidak menyadari jenis informasi yang disimpan di dalam dokumen mereka. Dengan demikian, penyidik digital forensik dapat mengakses informasi dokumen tersembunyi ini. Dalam kasus hukum, identifikasi bukti digital yang relevan sangat penting untuk mendukung kasus, verifikasi dan pemeriksaan yang ada pada bentuk argumen hukum. Dalam penelitian ini, ditujukan bagaimana menggunakan format dan jenis metadata yang berbeda dalam memvalidasi argumen hukum untuk dijadikan bukti yang relevan (Fahad Alanazi & Andrew Jones 2015)[12].

Ezz El-Din Hemdan & Manjaiah D.H (2015)[13] juga dalam penelitiannya melakukan pendekatan analisis forensik untuk benda digital seperti foto digital dan dokumen. Benda-benda ini berisi metadata penting yang dapat digunakan oleh penyidik untuk membantu menyelidiki kejahatan yang berkaitan dengan cloud. Metadata dapat digunakan juga oleh penyerang untuk melakukan kegiatan ilegal sehingga ada kebutuhan serius untuk

melindungi metadata karena memberikan peneliti dengan informasi yang dapat dipercaya untuk melakukan penyelidikan forensik. Dalam pendekatan ini, metadata yang dihasilkan dari benda-benda dan juga algoritma hash diterapkan untuk menghasilkan nilai hash untuk menjamin integritas data yang diunggah ke layanan cloud seperti *ADrive, Box, Microsoft onedrive, Google Drive, Copy* dan *Dropbox*.

Pada tahun ini Andy Spore (2016)[14] mengatakan lebih banyak orang memahami peran metadata dari segi pengembangan strategi hukum dan dengan analisis forensik yang tepat, metadata dapat membantu pola sorot, penetapan waktu, dan titik kesenjangan dalam data.

Komputer dan Sistem Operasi

Komputer / laptop yang digunakan dalam pengujian metode sistem metadata forensik ini adalah Laptop merk HP dengan Resolusi Layar 1366x768, Ukuran Layar 14 FULL HD, Tipe Layar Active Matrix TFT Color LCD, CPU Intel® Core i3 2.40 GHz, Memori/RAM 2 GB DDR 3, Harddisk 500 GB, DVD DVD Writer, Koneksi Bluetoth 4.0 + HS, Wi-Fi, Gigabit Internet, Microphone, Port USB USB 3.0, Webcam terintegrasi, HDMI (untuk LCD projector), Flash Kamera, Baterai Lithium Ion (Li-Ion) dan Berat 2.2 Kilogram [15].

Sedangkan Sistem Operasi yang digunakan dalam komputer ini adalah jenis Sistem Operasi Windows 10. Sistem Operasi Windows 10 adalah Sistem Operasi yang dikembangkan oleh Microsoft Corporation yang menggunakan antarmuka dengan berbasikan GUI (*Graphical User Interface*) atau tampilan antarmuka bergrafis pada umumnya sistem oprasi ini banyak sekali di gunakan oleh masyarakat, dari kalangan menengah ke atas hingga ke bawah [16].

Tools Aplikasi

Merupakan alat yang digunakan untuk menggambarkan bentuk logika model dari suatu sistem dengan menggunakan simbol-simbol, lambang-lambang, diagram-diagram ataupun GUI yang menunjukan secara tepat arti dan fungsinya. Adapun tools aplikasi yang dijelaskan sebagai model sistem yang telah dirancang yaitu Netbeans IDE 8.0 untuk pemrograman Java.

NetBeans adalah *Integrated Development Environment* (IDE) berbasiskan Java dari Sun Microsystems yang berjalan di atas Swing. Swing sebuah teknologi Java untuk pengembangan aplikasi Desktop yang dapat bejalan di berbagai macam platforms seperti Windows, Linux, Mac OS X and Solaris. Suatu IDE adalah lingkup pemrograman yang diintegrasikan kedalam suatu aplikasi perangkat lunak yang menyediakan pembangun *Graphic User Interface* (GUI), suatu text atau kode editor, suatu compiler atau interpreter dan suatu debugger [17].

File

File merupakan data yang ada pada komputer. Setiap data yang ada pada komputer dapat dikategorikan sebagai file. File tidak hanya terbatas pada data-data tertentu saja. Setiap data baik itu data gambar, data angka, data kata, data video, data suara, data aplikasi, dan data-data lainnya merupakan sebuah file. Menurut Hendrayudi "File adalah data-data yang tersimpan dalam media yang mempunyai informasi besar file, tanggal & jam penyimpanan file, nama file, ciri file (ciri aplikasi yang membuat), & attribut file." [18]

Sistem metadata forensik yang telah dibangun ini bisa membaca semua macam tipe jenis file yang ada didalam komputer, tetapi dalam tahap pengujian metode sistem ini, ada tujuh macam tipe jenis file yang digunakan sebagai contoh yaitu file dokumen yang ber-extension DOCX, file ebook yang ber-extension PDF, file gambar yang ber-extension JPG, file audio yang ber-extension MP3, file video yang ber-extension MP4, file akuisisi yang ber-extension DD dan file hasil imaging yang ber-extension E01.

Standar Metadata

Metadata terdiri atas beberap jenis standar dalam menampilkan data. Secara sederhana yang dimaksud dengan standar metadata adalah satu set terminologi serta definisi umum yang digunakan dalam metadata serta dipresentasikan dalam format terstruktur. Standar metadata spasial dibuat dan dikembangkan untuk mendefinisikan informasi yang diperlukan oleh seorang pengguna prospektif untuk mengetahui ketersediaan suatu set data spasial, mengetahui kesesuaian set data spasial untuk penggunaan yang diinginkan, mengetahui cara-cara pengaksesan data spasial serta untuk mentransfer set data spasial dengan sukses. Walaupun demikian standar tidak menetapkan tatacara bagaimana informasi diorganisasikan dalam suatu sistem komputer atau dalam suatu transfer data, tidak juga menetapkan tatacara bagaimana informasi tersebut ditransmisikan, dikomunikasikan atau disampaikan kepada pengguna. Jika standar metadata geospatial terkesan sangat komplek itu karena standar tersebut didesain untuk mendeskripsikan seluruh data geospasial yang bisa dideskripsikan [19].

Beberapa standar yang digunakan dalam pembuatan metadata spasial, yaitu: FGDC, ISO 19115, Dublin Core dan SNI Metadata. Standar metadata ISO 19115/19139 merupakan standar untuk pembuatan metadata data geospasial. Format ISO 19115 merupakan standar internasional untuk metadata informasi geografi dan format ISO 19139 merupakan skema implementasi untuk ISO 19115. ISO 19115 mempunyai 409 elemen dan terdapat 22 elemen inti (*core element*) yang dibutuhkan untuk

mendeskripsikan data dan memiliki *elemen compound (role)* dibawahnya. Role tersebut terbagi menjadi 11 komponen utama, yaitu identifikasi, batasan, kualitas data, representasi spasial, sistem referensi, informasi data, referensi portal katalog, distribusi, informasi tambahan dan informasi skema aplikasi (ISO, 2003). Skema ISO 19139 digunakan untuk mendeskripsikan, melakukan validasi dan melakukan pertukaran metadata geospasial yang disiapkan dalam format XML (*Extensible Markup Language*) [20].

Beberapa karakteristik metadata yang ditampilkan dalam sistem ini yaitu dibagi dalam 3 kategori:

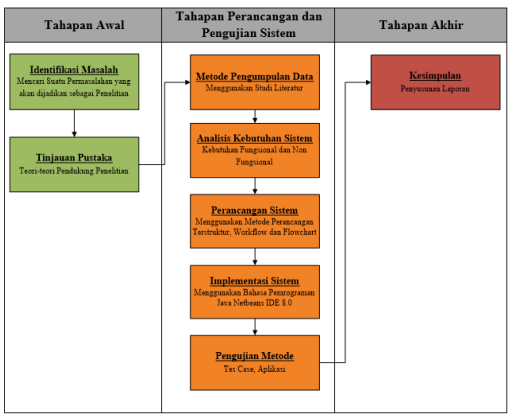
1. *Metadata General*, yaitu lokasi file, nama file, *type file*, *owner* dan *computer*.
2. *Metadata Detail*, yaitu *creationTime*, *lastAccessTime*, *lastModifiedTime*, *isDirectory*, *isOther*, *isRegularFile*, *isSymbolicLink* dan *Size*.
3. *Metadata Checksum*, yaitu Nilai MD5 dan SHA-256.

Korelasi File

Secara sederhana, korelasi dapat diartikan sebagai hubungan. Namun ketika dikembangkan lebih jauh, korelasi tidak hanya dapat dipahami sebatas pengertian tersebut. Korelasi merupakan salah satu teknik analisis dalam statistik yang digunakan untuk mencari hubungan antara dua variabel yang bersifat kuantitatif. Hubungan dua variabel tersebut dapat terjadi karena adanya hubungan sebab akibat atau dapat pula terjadi karena kebetulan saja. Dua variabel dikatakan berkolerasi apabila perubahan pada variabel yang satu akan di ikuti perubahan pada variabel yang lain secara teratur dengan arah yang sama atau berlawanan [21].

Dalam pengujian metode ini ada empat jenis korelasi metadata yang dijadikan sebagai contoh, yaitu metadata *file date*, *size*, *type file* dan *owner*. Sesorang investigasi bisa mencari semua jenis file yang ada didalam komputer berdasarkan dari empat pilihan korelasi tersebut.

Metode Penelitian



Gambar 1 Metode Penelitian Sistem Metada Forensik

Kerangka pemikiran metode penelitian yang di bangun secara garis besar dibagi menjadi tiga tahapan yaitu tahapan pertama atau tahapan awal dimulai dari identifikasi masalah dan tinjauan pustaka, tahapan kedua atau tahapan perancangan dan pengujian sistem dimulai dari metode pengumpulan data, analisis kebutuhan sistem, perancangan sistem, implementasi sistem dan pengujian metode, dan tahapan ketiga atau tahapan penyelesaian berupa kesimpulan atau penyusunan laporan dari penelitian ini. Berikut penjelasan masing-masing tahapan kegiatan yang dilakukan.

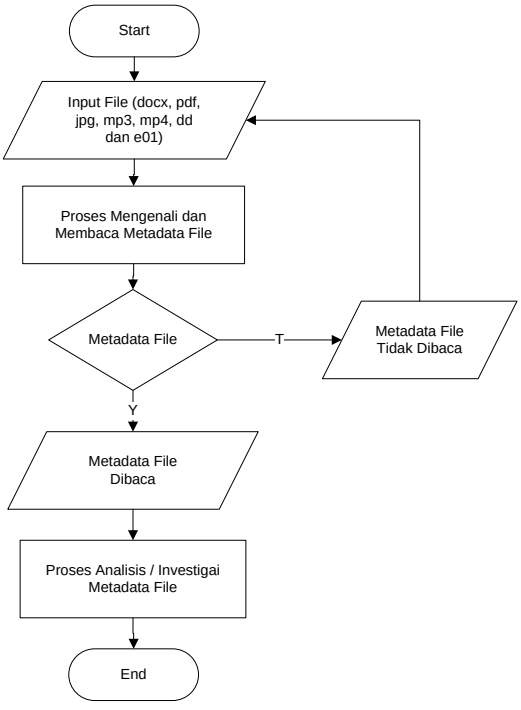
Metode yang digunakan untuk mengumpulkan data pada penelitian ini yaitu dengan melakukan studi literatur. Studi literatur dilakukan untuk mencari semua informasi yang berkaitan tentang konsep metadata forensik dalam membaca atau memahami karakteristik metadata file dan memudahkan pencarian dalam korelasi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

Hasil dan Pembahasan

Pada tahap ini di implementasikan program aplikasi yang telah dibuat, mulai dari hasil dan pembahasan. Hasil dari pembuatan program ini diuji pada beberapa file yang ada didalam komputer yang sudah ditentukan.

Membaca Karakteristik Metadata File

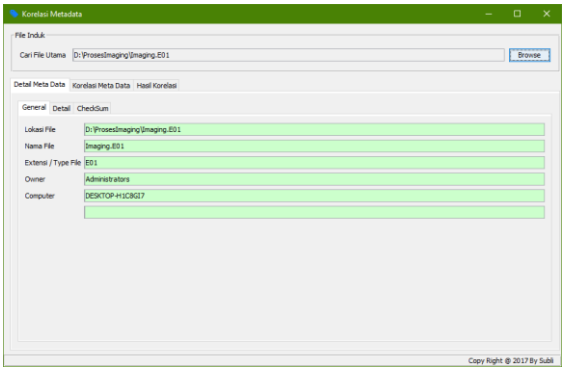
Berikut dijelaskan secara rinci penggunaan sistem untuk membaca metadata setiap file dalam *flowchart* dibawah ini:



Gambar 2 Flowchart Membaca Karakteristik Metadata File

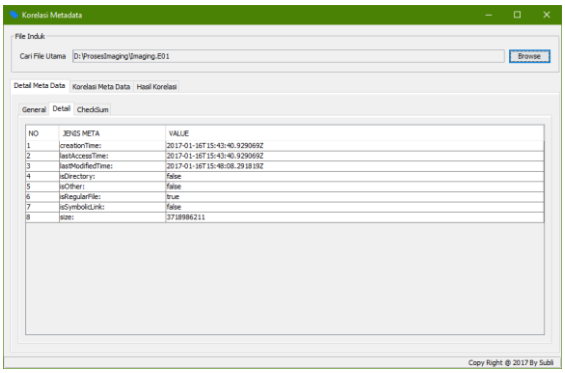
Pertama-tama dilakukan start atau sistem dijalankan, setelah itu dilakukan peng-inputan file yang akan di baca atau di kenali metadatanya, dimana file yang akan dibaca yaitu file ber-extension docx, pdf, jpg, mp3, mp4, dd dan E01, kemudian program akan melakukan pemrosesan file yang telah di inputkan, terdapat kondisi, dimana metadata file yang tidak bisa dibaca akan kembali ke inputan file objek, tetapi metadata file yang dapat terbaca akan langsung ditampilkan metadata filenya, selanjutnya dilakukan sebuah analisis/investigasi terhadap metadata file yang sudah dibaca dan terakhir program di tutup atau selesai di jalankan.

File yang akan dibaca metadatanya, terlebih dahulu akan di *browse* atau di cari sebuah file pada komputer, setelah itu program akan memproses file tersebut sampai ter-identifikasi metadatanya satu persatu, kemudian akan dimunculkan keterangan metadatanya di tabel detail metadata, seperti kita mencoba mem-*browse* sebuah file hasil akuisisi Imaging.E01 yang ada didalam Folder ProsesImaging di Data D, hasilnya seperti gambar 3, gambar 4 dan gambar 5 dibawah ini:



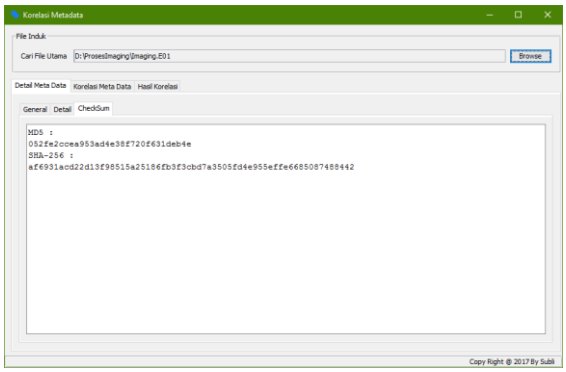
Gambar 3 Metadata General

Pada Gambar 3 Metadata General, ditemukan metadata file secara umum yang telah di inputkan sebelumnya, dimana **Lokasi File**: (berada di) D:\ProsesImaging\Imaging.E01, **Nama File**: (adalah) Imaging.E01, **Ektensi/Type File**: (adalah) E01, **Owner**: (adalah) Administrators dan **Computer**: (adalah) DESKTOP-H1C8GI7.



Gambar 4 Metadata Detail

Pada Gambar 4 Metadata Detail, ditemukan juga metadata file yang lebih rinci lagi pada file yang telah inputkan sebelumnya, dimana **CreationTime**: (adalah) 2017-01-16T15:43:40.929069Z, **LastAccessTime**: (adalah) 2017-01-16T15:43:40.929069Z, **LastModifiedTime**: (adalah) 2017-01-16T15:48:08.291819Z, **IsDirectory**: (adalah) false, **IsOther**: (adalah) false, **IsRegularFile**: (adalah) true, **IsSymbolicLink**: (adalah) false dan **Size**: (sebesar) 3718986211byte.

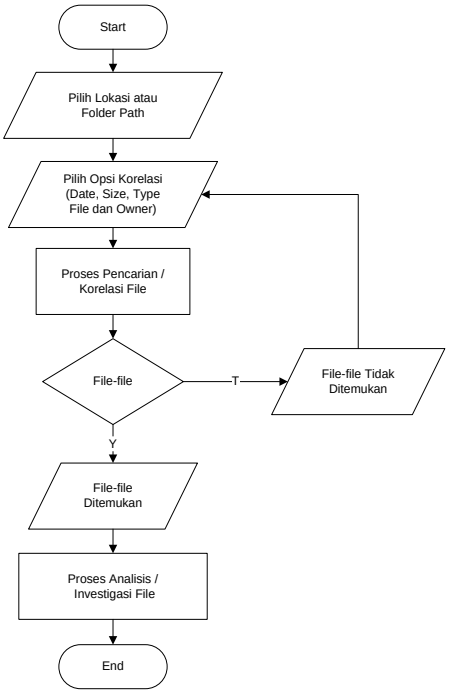


Gambar 5 Metadata Checksum

Selanjutnya pada Gambar 5 Metadata Checksum ditemukan juga metadata file nilai hashing dari file yang telah di inputkan sebelumnya, dimana **MD5**: (nilainya) 052fe2ccea953ad4e38f720f631deb4e dan **SHA-256**: (nilainya) af6931acd22d13f98515a25186 fb3f3cbd7a3505fd4e 955effe6685087488442.

Melakukan Korelasi Metadata File

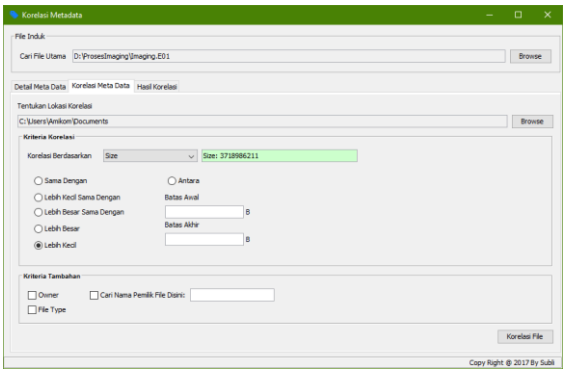
Berikut dijelaskan secara rinci penggunaan sistem untuk melakukan korelasi metadata file dalam *flowchart* dibawah ini:



Gambar 6 Flowchart Melakukan Korelasi Metadata File

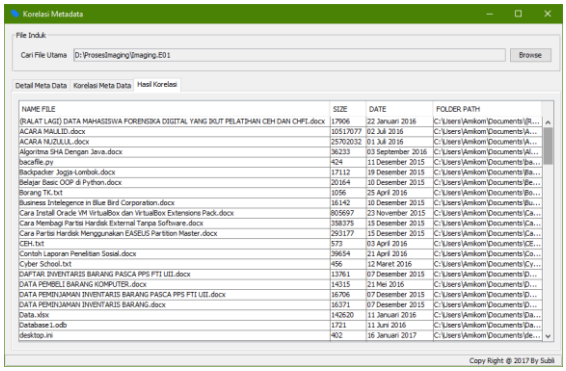
Pertama-tama dilakukan start atau sistem yang sudah dijalankan tinggal menunggu perintah mulai lagi, dilakukan penginputan lokasi korelasi terlebih dahulu (Data C, Data D atau Data E) atau Foder Path yang ada didalam komputer, setelah itu dilakukan pemilihan metadata file berdasarkan korelasi parameter dari Date, Size, Type File dan Owner, kemudian sistem akan melakukan proses menemukan korelasi metadata file yang telah dibuat, terdapat pernyataan atau kondisi dimana terdapat banyak file-file, jika file-file masih belum ditemukan korelasi metadatanya maka sistem akan kembali memilih opsi korelasi metadata file seperti biasa, tetapi apabila file-file sudah ditemukan dari korelasi metadata filenya berdasarkan parameter yang telah dibangun maka akan dilanjutkan ke analisis/investigasi file-file yang sudah ditemukan tersebut, dan yang terakhir sistem ini selesai digunakan dan ditutup.

Untuk melakukan korelasi metadata file, bisa dicoba dengan empat jenis korelasi yang telah dibuat yaitu metadata file date, size, type file dan owner. Disini akan dicoba dengan pencarian file berdasarkan korelasi metadata size file. Pada jenis korelasi size file sendiri, terdapat beberapa *option* yang bisa digunakan untuk mencari file-file yang size filenya bisa **Sama Dengan**, **Lebih Kecil Sama Dengan**, **Lebih Besar Sama Dengan**, **Lebih Besar**, **Lebih Kecil** dan **Antara** (misal dari file size berapa sampai dengan file size berapa yang akan ditemukan filenya) dengan file yang telah di inputkan sebelumnya dalam membaca karakteristik metada file, contohnya bisa dilihat seperti gambar berikut:



Gambar 7 Melakukan Korelasi File dengan Size File

Pada Gambar 7 Melakukan Korelasi File dengan Size File yaitu pilih lokasi korelasi terlebih dahulu, misal di Data C Documents, yang sebelumnya file yang telah di inputkan yaitu file akuisisi Imaging.E01 yang ada di Data D didalam folder ProsesImaging, kemudian dipilih Size dengan Option **Lebih Kecil**, selanjutnya klik button Korelasi File dan tunggu beberapa saat, maka file akuisisi Imaging.E01 yang sudah di input yang size filenya "3718986211 byte" akan mencari file-file yang ada di Data C Documents yang size filenya lebih kecil dari file yang sudah di inputkan sebelumnya, setelah menunggu beberapa saat maka ditemukan banyak sekali file-file yang ada di Data C Documents yang size filenya lebih kecil dari "3718986211 byte", hasilnya seperti gambar berikut:



Gambar 8 Hasil Korelasi Size File

Pada Gambar 8 Hasil Korelasi Size File, ada empat jenis yang ditampilkan dari sebuah file yaitu NAME FILE, SIZE, DATE dan FOLDER PATH. Dari sekian bayak file-file yang sudah ditemukan, diambil enam sampel yang dijadikan sebagai pembahasan melakukan korelasi metadata file berdasarkan korelasi size file, yaitu:

1. **Name File** (RALAT LAGI) DATA MAHASISWA FORENSIKA DIGITAL YANG IKUT PELATIHAN CEH DAN CHFI.docx dengan **Size** 17906 byte Lebih Kecil dari 3718986211 byte, **Date** 22 Januari 2016 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\(RALAT LAGI) DATA MAHASISWA FORENSIKA DIGITAL YANG IKUT PELATIHAN CEH DAN CHFI.docx
2. **Name File** ACARA MAULID.docx dengan **Size** 10517077 byte Lebih Kecil dari 3718986211 byte, **Date** 02 Juli 2016 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\ACARA MAULID.docx
3. **Name File** ACARA NUZULUL.docx dengan **Size** 25702032 byte Lebih Kecil dari 3718986211 byte, **Date** 01 Juli 2016 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\ACARA NUZULUL.docx
4. **Name File** Algoritma SHA Dengan Java.docx dengan **Size** 36233 byte Lebih Kecil dari 3718986211 byte, **Date** 03 September 2016 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\ Algoritma SHA Dengan Java.docx
5. **Name File** bacafile.py dengan **Size** 424 byte Lebih Kecil dari 3718986211 byte, **Date** 11 Desember 2015 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\bacafile.py
6. **Name File** Borang TK.txt dengan **Size** 1056 byte Lebih Kecil dari 3718986211 byte, **Date** 25 April 2016 dan **Folder Path** terletak di Data C:\Users\Amikom\Documents\Borang TK.txt

Kesimpulan dan Saran

Berdasarkan hasil yang didapat dari uraian diatas maka penelitian ini dapat ditarik kesimpulan:

1. Bahwa semua jenis file yang ada di dalam komputer, bisa dilihat detail metadatanya oleh algoritma metadata forensik yang sudah dibangun, termasuk tujuh macam file yang sudah dijadikan sampel yaitu DOCX, PDF, JPG, MP3, MP4, DD dan E01.
2. Metadata setiap file dapat dipahami secara umum, yaitu dibagi dalam tiga bagian; metadata secara general, metadata secara detail dan metadata nilai dari checksumnya. *Metadata General* terdiri dari lokasi file, nama file, type file, *owner* dan *computer*, *Metadata Detail* terdiri dari *CreationTime, LastAccessTime, LastModifiedTime, isDirectory, isOther, isRegularFile, isSymbolicLink* dan *Size*, dan *Metadata Checksum* terdiri dari nilai MD5 dan SHA-256.
3. Setelah melakukan korelasi metadata file, dapat ditemukannya file-file yang ada didalam komputer dari hasil pencarian korelasi berdasarkan parameter dari *Metadata File Date, Size, File Type* dan *Owner* yang ditampilkan dengan *Value File Name, Size, Date* dan *Path*.

Adapun saran-saran yang perlu diberikan dari hasil penelitian ini yaitu:

1. Dari segi hasil metadata file yang sudah ditemukan, perlu dikembangkan lagi menjadi lebih spesifik pembacaan metadatanya, karena setiap file memiliki masing-masing metadata yang berbeda.
2. Untuk korelasi metadata file dalam melakukan pencarian file-file tidak hanya korelasi berdasarkan parameter dari metadata file tersebut tetapi bisa dengan metode graph, bisa mencari file yang tidak ada dengan file yang ada.
3. Pengembangan dan penelitian lebih lanjut terkait algoritma metadata forensik ini yaitu bisa diketahuinya metadata file yang mana metadata yang belum dimodifikasi dan yang telah dimodifikasi.

Daftar Pustaka

[1] Niso. (2004). Understanding Metadata: NISO Press. Retrieved from www.niso.org

[2] Pendit, Putu Laxman. (2007). *Perpustakaan Digital: Perspektif Perpustakaan Perguruan Tinggi Indonesia*. Jakarta: Sagung Seto

[3] Technical Working Group Clearinghouse. (2005). *Panduan Pembangunan Metadata Spasial*. Marine and Coastal Resources Management Project: Bakosurtanal.

[4] Metadata, Daftar Istilah Komputer, IT Glossary, Definisi TIK. Retrieved from http://www.smitdev.com/posts/metadata362.php

[5] Metadata, Daftar Istilah Komputer, IT Glossary, Definisi TIK. Retrieved from http://www.smitdev.com/posts/metadata362.php

[6] Salama et al. (2012). Metadata Based Forensic Analysis of Digital Information in the Web. ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE & SECURE KNOWLEDGE MANAGEMENT, JUNE 5-6, 2012, ALBANY, NY

[7] M.P. Roberts & J. Haggerty. (2013). MetaFor: Metadata Signatures for Automated Remote File Identification in Forensic Investigations. Proceedings of the European Information Security Multi-Conference (EISMC 2013)

[8] Sriram Raghavan & S V Raghavan. (2013). AssocGEN: Engine for Analyzing Metadata Based Associations in Digital Evidence. IEEE Louisville Chapter. 978-1-4799-4061-5/13

[9] Mark Phillips. (2013). Metadata Analysis at the CommandLine. Code{4}lib Journal. Issue 19, 2013-01-15

[10] Woods et al. (2013). Managing and Transforming Digital Forensics Metadata for Digital Collections. University of North Carolina - School of Library and Information Science 216 Lenoir Drive, CB #3360, 100 Manning Hall Chapel Hill, NC 27599-3360 (919) 962-8366

[11] Suratkar, Khanuja. (2014). On The Role of Log Based Metadata in Forensic Analysis of Database Attacks. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622. International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

[12] Alanazi, Jones. (2015). The Value of Metadata in Digital Forensics. European Intelligence and Security Informatics Conference

[13] Ezz El-Din Hemdan & Manjaiah D.H. (2015). Forensic Analysis Approach Based on Metadata and Hash Values for Digital Objects in the Cloud. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Special Issue 7, October 2015

[14] Andy Spore. (2016). Using Metadata in Litigation. ProQuest

[15] Hewlett, Bill., & Packard, Dave. (2016). Spesification Notebook: HP. Retrieved from www.hp.com

[16] Gates, Bill., & Allen, Paul. (201). Excess: Windows 10. Retrieved from https://www.microsoft.com/en-us/software-download/windows10

[17] Netbeans. (2016). Excess: Netbeans IDE 8.0. Retrieved from https://netbeans.org/

[18] Hendrayudi. (2014). *Definisi File*. Retrieved from http://www.pengertianku.net/2014/09/definisi-atau-pengertian-file-secara-jelas.html

[19] Rita, Susilawati, S.S. (2006). *MENGENAL METADATA SEBAGAI SEBUAH ALAT INVESTASI DATA. Rekomendasi tentang pemanfaatan dokumen ISO 19115 sebagai standar metadata nasional di Indonesia, Tim Kerja Standar Metadata, Pusat Sistem Jaringan dan Standardisasi data Spasial, Badan Koordinasi Survey dan Pemetaan Nasional, 2006.*

[20] Silviana, Arlis, Rita., & Mahendra, Saputra, Riyan. (2014). *PENGEMBANGAN MODUL KONVERSI METADATA SPOT 5 VIRTUAL RECEPTION SESUAI FORMAT ISO 19115/19139: Seminar Nasional Penginderaan Jauh 2014*

[21] Universitas Ciputra. (2016). *Pengertian Korelasi dan Macam-macam Korelasi.* Retrieved from http://ciputrauceo.net/blog/2016/5/16/pengertian-korelasi-dan-macam-macam-korelasi