

BAB II

LANDASAN TEORI

2.1 Metadata

Definisi metadata secara sederhana dapat diartikan sebagai data tentang data (*data about data*). Namun definisi tersebut masih belum lengkap karena metadata tidak sesederhana itu. Salah satu ciri dari metadata adalah data tersebut harus terstruktur. Jadi definisi yang tepat untuk menggambarkan metadata adalah data terstruktur tentang data (*structured data about data*). Definisi tersebut masih sederhana dan belum sepenuhnya menjelaskan lebih detail tentang metadata. *Task Force on Metadata CC:DA (committee on cataloging: description and access)* dari ALA (*American library association*) menjelaskan secara lebih detail tentang metadata yaitu data yang terstruktur, ditandai dengan kode agar dapat diproses oleh komputer, mendeskripsikan ciri-ciri satuan-satuan pembawa informasi, dan membantu identifikasi, penemuan, penilaian dan pengelolaan satuan pembawa informasi tersebut.

Metadata adalah informasi yang ditanam pada sebuah file yang isinya berupa penjelasan tentang 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 (Putu Laxman Pendit 2007). Jika data tersebut dalam bentuk document docx metadatanya berupa keterangan mengenai *name file, content created, date last saved, content type, pages, word count, character count, line*

count, paragraph count, size, date created, date modified, date accessed, computer dan masih banyak lagi. Jika dalam bentuk pdf metadatanya berupa *name, type, folder path, size, date created, date modified, attributes, owner* dan *computer*. Untuk jenis data gambar jpg, metadata mengandung informasi mengenai siapa pemotretnya, kapan pemotretannya, dan setting kamera pada saat dilakukan pemotretan. Untuk audio jenis mp3 bisa tambahkan metadatanya berupa *album, year, genre, length, bit rate* dan rekaman yang dipakai lainnya. Untuk jenis video mp4 metadatanya bisa berupa seperti mp3 dengan tambahan *frame width, frame height, data rate, total bitrate, frame rate, channels* dan jenis perekam video lainnya.

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.

2.2 Konsep Metadata

Metadata dapat diartikan sebagai “data tentang data (*spasial*)”, berisikan informasi mengenai karakteristik data dan memegang peran penting di dalam mekanisme pertukaran data. Melalui informasi metadata diharapkan pengguna data dapat menginterpretasikan data secara sama, bilamana pengguna melihat langsung data spasialnya. Dokumen metadata berisikan informasi yang menjelaskan karakteristik data terutama isi, kualitas, kondisi dan cara perolehannya. Metadata dipergunakan untuk melakukan dokumentasi data spasial yang berhubungan tentang siapa, apa, kapan, dimana, dan bagaimana data spasial dipersiapkan.

2.3 Jenis Metadata

Adapun jenis-jenis metadata file antara lain:

1. Metadata Deskriptif

Data yang dapat mengidentifikasi sumber informasi sehingga dapat digunakan untuk memperlancar proses penemuan dan seleksi. Cakupan yang ada pada data ini adalah pengarang, judul, tahun terbit, tajuk subjek atau kata kunci dan informasi lain yang proses pengisian datanya sama dengan katalog tradisional.

2. Metadata Administratif

Data yang tidak hanya dapat mengidentifikasi sumber informasi tapi juga cara pengelolaannya. Cakupan dari data ini adalah sama dengan data deskriptif hanya saja ditambah dengan pembuat data, waktu pembuatan, tipe file, data teknis lain. Selain itu data ini juga mengandung informasi tentang hak akses, hak kekayaan intelektual, penyimpanan dan pelestarian sumber informasi.

3. Metadata Struktural

Data yang dapat membuat antara data yang berkaitan dapat saling berhubungan satu sama lain. Secara lebih jelas, Metadata ini digunakan untuk mengetahui hubungan antara berkas fisik dan halaman, halaman dan bab dan bab dengan buku sebagai produk akhir.

2.4 Skema Metadata

Ada beberapa skema metadata file diantaranya sebagai berikut ini.

1. *Semantic*

Dalam kaitannya dengan metadata, semantik dapat diartikan sebagai makna kata. Lebih jelasnya adalah kesepakatan untuk membuat istilah yang digunakan untuk mewakili suatu makna. Selain itu, terkadang juga diberi keterangan tentang status pada istilah tersebut.

2. *Content*

Dalam hal ini, konten bisa diartikan sebagai cara mengisi semantic. content tersebut bisa berupa peraturan untuk kriteria pengisian unsur skema atau peraturan untuk nilai-nilai unsur.

3. *Sintaksis*

Sintaksis dalam skema metadata dapat berarti sebagai machine readable (dapat dibaca mesin) atau dengan kata lain bahasa pemrograman. Sehingga *semantic* dan *content* yang telah dibuat dapat dibaca oleh mesin.

2.5 Contoh Metadata

Berikut beberapa contoh metadata berdasarkan skema metadata:

1. CDWA (*Categories for Descriptions of Works of Art*), skema untuk deskripsi karya seni
2. DCMES (Dublin Core Metadata Element Set), skema umum untuk deskripsi berbagai macam sumber digital.
3. EAD (Encoded Archival Description), skema untuk menciptakan sarana temu kembali pada *bahan kearsipan (archival finding aids) dalam bentuk elektronik*.

4. GEM (*Gateway to Educational Materials*), skema untuk bahan pendidikan dan pengajaran
5. MARC (Machine Readable Cataloging), skema yang digunakan di perpustakaan sejak tahun 1960-an untuk membuat standar cantuman bibliografi elektronik.
6. METS (Metadata Encoding and Transmission Standard), skema metadata untuk obyek digital yang kompleks dalam koleksi perpustakaan
7. MODS (Metadata Object Description Standard), skema untuk deskripsi rinci sumber-sumber elektronik
8. MPEG (Moving Pictures Experts Group) MPEG-7 dan MPEG-21, skema untuk rekaman audio dan video dalam bentuk digital
9. ONIX (Online Information Exchange), skema untuk data bibliografi pada penerbit dan pedagang buku
10. TEI (Text Encoding Initiative), skema untuk encoding teks dalam bentuk elektronik menggunakan SGML dan XML, khususnya untuk peneliti teks di bidang humaniora.
11. VRA (Visual Resources Association), skema untuk deskripsi karya visual dan representasinya.

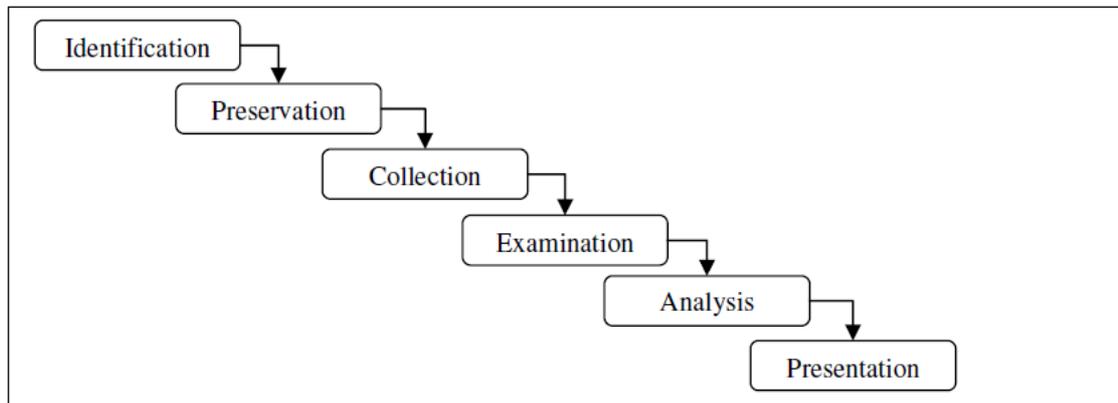
2.6 Framework

Framework merupakan suatu struktur konseptual dasar yang digunakan untuk memecahkan atau menangani suatu masalah kompleks. Framework dalam digital forensik dapat didefinisikan sebagai sebuah struktur untuk mendukung kesuksesan dalam penyelidikan forensik.

- *Common Phases of Computer Forensics Investigation Models*

berikut adalah beberapa *framework* yang dimuat dalam paper *Common Phases of Computer Forensics Investigation Models*.

- *DFRWS Investigative Model*



Gambar 2.1 Model *Digital Forensic Research Workshop* (Peter Shtepenson,2001)

Model *Digital Forensics Research Workshop* (DFRWS) dimulai dengan *Identifikasi* di mana tahap ini deteksi profil, sistem monitoring, analisis audit dilakukan. Fase *Preservation*, melibatkan tugas-tugas seperti menyiapkan manajemen kasus yang tepat dan memastikan dapat diterima di pengadilan. Fase ini sangat penting sehingga untuk memastikan bahwa data yang dikumpulkan bebas dari kontaminasi. Tahap berikutnya dikenal sebagai *Collection*, di mana data yang relevan sedang dikumpulkan dengan memanfaatkan berbagai teknik. Fase ini adalah dua fase penting, yaitu fase *Examination* dan *Analysis*. Dua tahap ini, tugas-tugas seperti bukti pencarian, bukti validasi, pemulihan data tersembunyi / data yang dienkripsi, *data mining*, waktu dilakukan. Tahap terakhir adalah *Presentation*. Tugas yang berhubungan dengan tahap ini adalah dokumentasi, kesaksian ahli.

Tahap *Identification* adalah tahap untuk mengenali dan menentukan jenis kejahatan yang dilakukan. Setelah jenis kejahatan dipastikan, tahap berikutnya adalah *Preparation* diikuti dengan *Approach Strategy* data fisik dan digital yang diakuisisi harus benar-benar terisolir, aman dan terawat. Kegiatan untuk memperhatikan proses-proses yang dilakukan sebelumnya telah benar, Semua tugas-tugas ini dilakukan saat fase *Preservation*. Berikutnya adalah tahap *Collection*, dimana ekstraksi data dan duplikasi dilakukan. Identifikasi data dan menemukan bukti-bukti potensial dari data yang dikumpulkan, menggunakan pendekatan sistematis yang dilakukan dalam fase berikutnya, yang dikenal sebagai fase *Examination*. Tugas yang menentukan dan signifikan dari bukti dan menarik kesimpulan berdasarkan bukti yang ditemukan dilakukan dalam tahap *Analysis*. Pada tahap *Presentation* temuan dirangkum dan disajikan. Proses penyelidikan selesai dengan melaksanakan pengembalian barang bukti pada fase *Returning Evidence*.

2.7 Pengertian Korelasi

Korelasi dapat diartikan sebagai hubungan. 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 berkorelasi apabila perubahan pada variabel yang satu akan diikuti perubahan pada variabel yang lain secara teratur dengan arah yang sama (korelasi *positif*) atau berlawanan (korelasi *negatif*).

Komputer berisi data dan program, Program merupakan file komputer yang digunakan untuk melakukan tugas tertentu, sedangkan data merupakan file hasil kerja program komputer yang dapat diedit, dibuka, dihapus, dan sebagainya. Sementara itu, folder adalah suatu tempat untuk mengumpulkan file

Pengujian metode ini ada empat jenis korelasi metadata yang dijadikan sebagai contoh, yaitu metadata *file date*, *size*, *type file* dan *author*. Investigator bisa mencari semua jenis file (tidak hanya lima jenis file yang telah dibahas diatas; Docx, Pdf, Jpg, Mp3 dan Mp4) yang ada didalam komputer berdasarkan dari empat pilihan korelasi tersebut.

2.8 Keunggulan dan Manfaat Metadata

Adapun kegunaan dan manfaat metadata yaitu:

1. Sebagai alat/*tool* pengelolaan investasi (data) seperti melakukan monitoring kemajuan pelaksanaan pekerjaan pembangunan data spasial, mendokumentasikan data data yang ada (selesai dikerjakan), menginformasikan data data yang dimiliki untuk dapat dimanfaatkan oleh pihak lain dan melakukan estimasi rencana kerja pengumpulan data dikemudian hari.
2. Sarana untuk menyebarluaskan kepemilikan data melalui mekanisme *clearinghouse*. Metadata merupakan faktor penting dalam konsep pemanfaatan data spasial bersama (data *sharing*).
3. Memberikan penjelasan (informasi) kepada pengguna data tentang tata cara pemrosesan dan mengintepretasikannya.

4. Metadata juga mengandung (berisikan) istilah-istilah baku yang dipakai dalam kasanah *data* spasial. Dengan pembakuan istilah, kesalahan arti dalam penuturan data spasial dapat dihindari.

Untuk mencapai tujuan tersebut di atas, maka penyusunan metadata harus dipersiapkan dengan mempertimbangkan berbagai hal sedemikian hingga produk informasi yang dihasilkan dapat dimanfaatkan oleh berbagai pihak. Informasi metadata ditetapkan berdasarkan 4 (empat) karakteristik yang menentukan peranan dari metadata, yaitu :

1. Ketersediaan - informasi yang diperlukan untuk mengetahui ketersediaan data
2. Penggunaan - informasi yang diperlukan untuk mengetahui kegunaan data
3. Akses - informasi yang diperlukan tentang tatacara mendapatkan data
4. Transfer - informasi yang diperlukan untuk mengolah dan menggunakan data.

Skema tingkat global terdapat beberapa tingkatan metadata yang biasa digunakan, yaitu :

1. *Discovery* metadata adalah informasi minimum yang diberikan untuk menjelaskan isi dari sumber data. Jenis metadata ini tentu saja tidak memenuhi kategori metadata yang bisa diaplikasikan pada tingkat internasional.
2. *Exploration* metadata adalah informasi yang lebih detil yang diberikan dalam menjelaskan isi dari sumber data. Jenis metadata ini diharapkan dapat membantu pengguna data untuk keperluan analisis

3. *Exploitation* metadata adalah metadata yang memuat informasi akses data, transfer data, *load* data, menginterpretasikan data dan penggunaan data untuk suatu aplikasi.

2.9 Konsep Analisis Metadata Forensik

2.9.1 pengertian 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.

File adalah kumpulan berbagai informasi yang berhubungan dan juga tersimpan di dalam secondary storage, secara konsep file memiliki beberapa tipe ada yang bertipe data terdiri dari *numeric*, *character* dan *binary*, lalu ada juga file yang bertipe program atau definisi file adalah arsip ataupun data yang tersimpan di dalam komputer.

File di komputer pada umumnya disimpan di dalam suatu folder tertentu tergantung dari pemilik komputer tersebut yang ingin dimana tempat menyimpannya, setiap file memiliki ekstensi masing-masing tergantung jenis file itu sendiri. Ekstensi file adalah sebagai tanda yang membedakan jenis-jenis dari file.

Pengertian file menurut beberapa ahli, yaitu sebagai berikut:

1. 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), dan *attribut file*.”

2. Lalu menurut Rachmad Hakim S. “File merupakan dokumen yang mengandung informasi tertentu dan dapat dibuka dengan program.”
3. Sindhunata “File adalah kumpulan catatan atau arsip.”
4. Terus menurut Mcleod (PEARSON) “File adalah koleksi record yang saling berhubungan, seperti satu file dari seluruh record yang berisi field kode-kode mata kuliah dan namanya.”
5. Sedangkan menurut Edi S. Mulyanta “File merupakan urutan data yang digunakan untuk melakukan *encode* informasi digital untuk urusan penyimpanan dan pertukaran data.”

2.9.2 Jenis-jenis File di Komputer

Memilih Properties pada file komputer ada tulisan tiga huruf sesudah titik. Itulah yang dinamakan *ekstensi file*. Fungsinya adalah untuk mengetahui atau membedakan jenis file. Untuk mengetahui *ekstensi file* lainnya Anda bisa membuka *Windows Explorer*, lalu pilih menu *View – Folder Options*. Pindah ke tab *Files Types*. Di sana terdapat puluhan dan mungkin ratusan ekstensi file. Semakin banyak Anda menginstall aplikasi maka daftar ekstensi file yang ada akan semakin panjang. Di antara beberapa ekstensi file di tunjukkan pada tabel 2.1 dan 2.2 berikut:

Tabel 2.1 Beberapa Ekstensi File

Ekstensi File	Jenis	Aplikasi
Doc	File dokumen	MS Word
JPG/JPEG (<i>Joint Photographic Experts Group</i>)	File gambar	PhotoShop, PhotoPaint, Paint, ACDSee dll
MP3	File audio	Winamp, Windows Media Player dll
PDF (<i>Portable Document Format</i>)	File dokumen adobe	Adobe raeder dll
MP4	File video	Pemutar video
PSD	File image, PhotoShop	PhotoShop

Tabel 2.2 Beberapa Ekstensi File (Lanjutan)

Ekstensi File	Jenis	Aplikasi
Gif (<i>Graphics Interchange Format</i>)	File gambar/animasi	PhotoShop, PhotoPaint, Paint, ACDSee, Ulead Gif Animator dll
Exe	File aplikasi (executable)	Sistem operasi windows
Asm	Source code pemrograman Assembly	Sembarang teks editor, seperti MS Word, NotePad, Wordpad

2.10 Klasifikasi Barang Bukti

Investigasi adanya file bukti digital sangatlah penting untuk keberlanjutan kasus yang sedang di investigasi, karena dengan adanya barang bukti itulah maka akan dilakukan analisa untuk mengungkap motif dan pelaku kejahatan tersebut.

Para investigator diharapkan dapat memahami jenis-jenis barang bukti sehingga pada saat melakukan proses investigasi mereka mengenali barang bukti yang menjadi prioritas untuk diutamakan.

Berikut akan dijelaskan klasifikasi barang bukti

1. Barang Bukti Elektronik

Barang bukti elektronik merupakan barang bukti yang bersifat fisik dan dapat dikenali secara visual. Adapun jenis-jenis barang bukti elektronik adalah sebagai berikut ini:

- a. Komputer, PC/Leptop/Netbook, Notebook, Tablet
- b. Hanphone, Smartphone
- c. Flashdisk/Thumbdrive
- d. Harddisk
- e. CD/DVD
- f. Router, Switch ,Hub
- g. Floppydisk
- h. Camera Video, CCTV
- i. Camera Digital
- j. Digital Recorder
- k. Musik/Video Player, dan lain-lain.

2. File Bukti Digital

Barang bukti digital merupakan setiap informasi pembuktian yang disimpan atau disalurkan dalam bentuk digital yang mana pihak dalam kasus hukum dapat gunakan untuk pemeriksaan pengadilan.

Berikut contoh barang bukti digital :

- a. *Logical file* yaitu file-file yang masih ada dan tercatat dalam file system yang sedang berjalan di suatu partisi.

- b. *Deleted file*, dikenal juga dengan istilah *unallocated cluster* yang merujuk pada *cluster* dan sektor tempat penyimpanan file yang sudah terhapus dan tidak teralokasikan lagi untuk file tersebut dengan ditandai dalam file *system* sebagai area yang dapat digunakan lagi untuk penyimpanan file-file baru.
- c. *Lost file* yaitu file yang sudah tidak tercatat lagi di file system yang sedang berjalan dari suatu partisi, namun file tersebut masih ada di sector penyimpanannya.
- d. *File slack* yaitu sektor penyimpanan yang berada diantara *end of file* dengan *end of cluster*.
- e. *Log file* yaitu file-file yang merekam aktifitas dari suatu keadaan tertentu.
- f. *Encrypted file* yaitu file yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma *kriptografi* yang kompleks, sehingga tidak bisa dibaca atau dilihat secara normal.
- g. *Steganography file* yaitu file yang berisikan informasi rahasia yang disisipkan ke file lain.
- h. *Office file* yaitu file-file yang merupakan produk dari aplikasi *office*.

3. Temuan File Bukti Digital

Temuan File bukti digital merupakan Bukti digital lebih bermakna sebagai *output analysis* yang didapat oleh investigator yang langsung mengarah untuk kepentingan *rekontruksi* kasus yang sedang dihadapi. Bukti digital adalah informasi yang langsung terkait dengan data-data yang diperlukan oleh investigator dalam proses penyidikan. Pada tahap akhir ini istilah yang lebih tepat adalah Temuan Bukti Digital menurut (Prayudi, 2014).