PENGEMBANGAN *OUTPUT* DFXML UNTUK MANAJEMEN BUKTI DIGITAL

Putry Wahyu Setyaningsih
14917223

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Program Magister Teknik Informatika
Universitas Islam Indonesia
2018

Lembar Pengesahan Pembimbing

Pengembangan *Output* DFXML Untuk Manajemen Bukti Digital

Putry Wahyu Setyaningsih

14917223

Yogyakarta, 14 Januari 2018

Pembimbing I	Pembimbing II
Dr. Bambang Sugiantoro, MT	Yudi Prayudi, S.Si, M.Kom

Lembar Pengesahan Penguji

Pengembangan *Output* DFXML Untuk Manajemen Bukti Digital

Putry Wahyu Setyaningsih

14917223

Yogyakarta, 14 Januari 2018

Tim Penguji,

Dr. Bambang Sugiantoro, MT.
Ketua

Yudi Prayudi, S.Si., M.Kom
Anggota I

Dr. Imam Riadi, M.Kom
Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

UNIVERSITAS ISLAM INDONESIA PROGRAM PASCASARJANA FAKULTAS TEKNOLOGI INDUSTRI

Dr. R. Teduh Dirgahayu, ST., M.Sc

ii

Abstrak

Pengembangan *Output* DFXML Untuk Manajemen Bukti Digital

Kasus yang terjadi di dunia maya banyak meninggalkan jejak berupa barang bukti elektronik. Bukti elektronik akan dapat dibaca setelah melalui akuisisi, dari proses akuisisi tersebut disebut sebagai bukti digital. Salah satu cara untuk mendapatkan bukti digital dengan melalui akuisisi, *tools* yang digunakan untuk melakukan akuisisi adalah DFXML. DFXML akan menghasilkan file dd dan file XML. Hasil dari DFXML adalah file XML dimana file XML menghasilkan banyak elemen-elemen dari akuisisi bukti digital. Dalam hal ini *output* tersebut mengalami kendala dalam pengelolaan file dan pembacaan file XML dari hasil DFXML sehingga perlu dilakukan adanya solusi lain untuk bisa mengatasi masalah dalam pengelolaan *output* hasil DFXML. Solusi dari permasalahan tersebut dengan cara membangun sebuah sistem untuk manajemen *output* DFXML. Dengan solusi yang diberikan maka akan memudahkan investigator dalam melakukan pembacaan file XML dan memudahkan dalam pengelolaan hasil akuisisi dari bukti digital. Solusi yang diberikan dengan tujuan untuk membangun sebuah sistem guna menampilkan dan membaca file XML dan mampu mengelola hasil *output* DFXML. Dengan menggunakan data hasil akuisisi bukti elektronik menjadi bukti digital, maka hasil yang didapatkan adalah file dd dan file XML, dimana kedua file tersebut akan di unggah kedalam sistem yang dibangun untuk memudahkan pengelolaan *output* DFXML, maka secara umum solusi yang diberikan mampu menyelesaikan masalah dalam pengelolaan *output* DFXML.

Kata kunci

Bukti Elektronik, Akuisisi, Bukti Digital, DFXML, Elemen, XML

Abstract

DFXML *Output* Development For Evidence Digital Management

Crimes that occured in cyberspace many leaves trace of electronic evidence. Electronic evidence will be readable after the acquisition, from the acquisition process referred to as digital evidence. One way to get digital evidence by acquisition, the tools used to make the acquisition are DFXML. DFXML will generate dd files and XML files. The result of DFXML is an XML file where XML files generate many elements from the acquisition of digital evidence. In this case the output is experiencing constraints in file management and XML file readings from the DFXML results so it needs to be done another solution to be able to overcome the problem in managing output DFXML results. Solution of the problem by building a system for DFXML output management. With the solution provided it will facilitate the investigator in the reading of XML files and facilitate the management of the acquisition of digital evidence. The solution is given in order to build a system to display and read XML files and be able to manage DFXML output results. By using the data acquisition of electronic evidence into digital evidence, the results obtained are dd files and XML files, where the two files will be uploaded into the system built to facilitate the management of output DFXML, then in general the solution provided to solve problems in the management output DFXML.

Keywords

Electronic Evidence, Acquisition, Digital Evidence, DFXML, Elements, XML

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 14 Januari 2018

Putry Wahyu Setyaningsih, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Sitasi publikasi 1

Kontributor	**Jenis Kontribusi**
Author Putry Wahyu Setyaningsih	Mendesain eksperimen (50%) Menulis *paper* (60%)
Author Bambang Sugiantoro	Mendesain eksperimen (30%) Menulis dan mengedit *paper* (20%)
Author Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (20%)

Halaman Kontribusi

Bapak Dr. Bambang Sugiantoro, MT selaku Pembimbing I dan Bapak Yudi Prayudi, S.Si., M.Kom selaku Pembimbing II yang telah memberikan arahan-arahannya kepada penulis, sehingga penulisan tesis ini bisa selesai dengan baik.

Halaman Persembahan

Dalam tesis ini saya persembahkan kepada :

Papa Sapto Wahyu Widiyanto dan Mama Tri Widatiningsih, S.Pd. Terimakasih tak henti-hentinya selalu memberikan dukungan.

Kedua adik saya Bagus Wahyu Setyawibawa dan Sakti Wahyu Widipermana yang telah memberikan dukungan serta candatawa.

Herdito Cahyo Utomo, terimakasih waktu yang selalu diberikan dantak pernah lelah untuk selalu memberikan dukungannya dari jaman skripsi Strata 1 sampai akhirnya sekarang tesis Strata 2.

Kata Pengantar

Laporan Tesis yang berjudul "PENGEMBANGAN *OUTPUT* DFXML UNTUK MANAJEMEN BUKTI DIGITAL" disusun guna memenuhi salah satu syarat akademik untuk menempuh kelulusan Program Pascasarjana Magister Teknik Informatika pada Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta.

Dalam laporan tesis ini, penulis menyampaikan rasa terimakasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya kepada semua pihak yang terkait dalam penyelesaian tugas akhir ini sesuai dengan masa waktu yang telah diberikan, diantaranya kepada :

1. Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta.
2. Bapak Yudi Prayudi, S.Si., M.Kom selaku Ketua PUSFID Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta sekaligus Pembimbing II yang telah meluangkan banyak waktunya dalam membimbing dan membantu penulis selama penulisan Tesis ini.
3. Bapak Dr. Bambang Sugiantoro, MT selaku Pembimbing I yang telah memberikan arahan-arahan dalam membimbing dan membantu penulis selama penulisan Tesis ini.
4. Bapak Dr. Imam Riadi, M.Kom selaku Penguji yang telah memberikan masukan, saran dan kritikannya kepada penulis dalam tahap perbaikan-perbaikan penyusunan laporan tesis ini.
5. Teman-teman Magister Informatika Angkatan XI khususnya teman-teman forensika digital.

Dalam penyelesaian tesis ini, penulis menyadari bahwa masih banyak kekurangan yang sekiranya perlu untuk di perbaiki demi tujuan yang lebih baik lagi baik dalam proses pembuatan sistem maupun dalam penulisan laporan ini.

Untuk itu penulis mengharapkan kritik dan saran kepada seluruh pembaca yang bersifat membangun sebagai bahan evaluasi dan pembelajaran agar lebih baik lagi untuk di kemudian hari. Semoga laporan ini dapat bermanfaat bagi kita semua. Amin.

Wassalamuallaikum warohmatullohi wabarokatuh.

Yogyakarta, 14 Januari 2018

Putry Wahyu Setyaningsih, S.Kom

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

Kasus kejahatan yang terjadi saat ini banyak melibatkan berbagai macam barang bukti. Menurut (POLRI, 2017) barang bukti adalah benda bergerak atau tidak bergerak, berwujud atau tidak berwujud yang telah dilakukan penyitaan oleh penyidik untuk keperluan pemeriksaan dalam tingkat penyidikan, penuntutan dan pemeriksaan di sidang pengadilan. Barang bukti sangat penting dalam upaya pembuktian sebuah tindak kejahatan di pengadilan. Dalam KUHAP tidak menyebutkan definisi barang bukti secara tegas, namun barang bukti dapat dikatakan memiliki pengertian yang sama dengan benda sitaan. Penyitaan adalah serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan (Simbolon, Albisar, Mulyadi, & Leviza, 2016).

Layaknya kejahatan yang dilakukan secara konvensional, kejahatan dunia mayajuga meninggalkan jejak atau pun barang bukti yang disita dan dapat memberikan sebuah petunjuk dalam pembuktian sebuah kasus kejahatan. Dalam forensika digital terdapat dua istilah barang bukti yang sering digunakan yaitu barang bukti elektronik dan barang bukti digital. Menurut (Al-Azhar, 2012) barang bukti elektronik yang bisa juga disebut perangkat digital lebih berupa kepada barang bukti yang berwujud secara fisik dan dapat dikenali secara visual yang berupa perangkat elektronik seperti komputer, *handphone*, laptop, dan lain sebagainya yang memiliki bentuk fisik. Sedangkan barang bukti digital merupakan data digital yang tersimpan di dalam perangkat elektronik tersebut dan baru akan muncul setelah barang bukti elektronik tersebut diakusisi. Salah satu contohnya adalah ketika dalam sebuah kasus *cybercrime*, perangkat penyimpanan data *flashdisk* digunakan sebagai bukti elektronik, *flashdisk* tersebut kemudian dilakukan proses akuisisi, hasil proses akuisisi tersebut disebut sebagai bukti digital. Kriteria bukti digital yang dapat diterima di pengadilan ada 5 kriteria, yaitu:dapat diterima, bukti yang otentik, bukti yang lengkap, bukti yang dapat diandalkan dan bukti yang dapat dipercaya (Prayudi, 2015)

Digital Forensics XML (DFXML) adalah pengembangan dari bahasa XML yang dirancang untuk mewakili berbagai macam informasi forensik dan hasil pengolahan forensik (Garfinkel, 2011). DFXML tercipta dari proses akuisisi bukti elektronik. Bukti elektronik diakuisisi dengan aplikasi DFXML yang akan menghasilkan sebuah bukti digital yang berupa file dengan ekstensi dd dan file dengan ekstensi XML. Dalam setiap mengakuisisi satu bukti elektronik menjadi bukti digital akan menghasilkan dua file yang berbeda, file yang dihasilkan dari DFXML adalah satu file dengan ekstensi dd dan file dengan ekstensi XML. Elemen-elemen XML pada DFXML yang dihasilkan, bergantung pada jumlah bukti digital yang terdapat pada bukti elektronik. Semakin banyak bukti digital yang terdapat pada bukti elektronik, maka elemen XML yang tercipta akan semakin banyak. Padahal tidak semua elemen XML tersebut dapat digunakan sebagai informasi dasar untuk kepentingan manajemen bukti digital.

Salah satu format penyimpanan data yang memiliki struktur hirarkis yang sama dengan database relasional dan mudah dalam pertukaran informasi yaitu XML. Menurut (Tekli & Member, 2016) XML atau *eXtensible Markup Language* sebagai model representasi data semi terstruktur standar pada *web* yang memiliki kemampuan untuk menyaring informasi dan membentuk ulang terstruktur menjadi format semi terstruktur yang telah terbukti penting dalam memfasilitasi skala pengolahan data otomatis. Dengan menggunakan format dokumen XML, memungkinkan banyak kemudahan dan perbaikan dalam mendukung integrasi berbagai *platform* sistem dan aplikasi, baik melalui infrastruktur intranet maupun internet, dan informasi yang dibutuhkan tersebut dapat diakses dari mana saja dan dengan *computing device, platform*, atau aplikasi yang kita gunakan.

Selama ini sistem yang sudah ada menyulitkan investigator dalam menangani file-file *output* DFXML, sehingga perlu dibuat suatu mekanisme lain untuk menangani *output* hasil DFXML. File hasil *output* DFXML akan dimasukkan kedalam sistem yang telah dibuat kemudian investigator dapat melakukan manajemen bukti digital. Bentuk manajemen bukti digital yang memiliki kemampuan dapat melihat file-file yang dimasukkan kedalam sistem, membaca bagian terpenting dari elemen XML, mengubah data dinamis pada *chain of custody* dan menghapus file bukti digital.

Akuisisi hasil bukti digital yang berupa file XML dan file dd kemudian di masukkan ke dalam sistem dimana dalam sistem yang dibuat akan menguraikan hasil dari DFXML menjadi

sebuah *form* yang mudah dibaca oleh investigator. Sistem yang mampu mengelola file hasil DFXML yang berupa file dd dan file XML, sistem yang mampu menambah data dinamis pada *chain of custody*, sistem yang mampu membaca elemen-elemen XML yang penting, mampu merubah data yang salah pada *chain of custody*, dan mampu menghapus file bukti digital.

Atas dasar permasalahan tersebut, salah satu solusi yang diajukan adalah dengan membuat sebuah sistem yang mampu mengidentifikasi elemen-elemen XML apa saja yang dapat digunakan untuk kepentingan manajemen bukti digital pada *file* DFXML yang telah diakuisisi sehingga perlu dilakukan sebuah penelitian mengenai pengembangan sistem *output* DFXML untuk manajemen bukti digital. Dengan sistem yang dibuat akan memudahkan investigator dalam mengelola beberapa file DFXML dan dapat dikelola secara bersamaan.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah yang akan dibahas adalah sebagai berikut :

1. Bagaimana membangun sebuah sistem yang mampu mengelola *output* dari DFXML?
2. Bagaimana kinerja sistem dalam menangani berbagai *output* DFXML?

1.3 Batasan Masalah

Batasan-batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Data yang disimpan hanya berfokus pada file hasil *imaging* dari file dd.
2. Data yang disimpan hanya file XML hasil *output* DFXML.
3. Hanya menampilkan dan membaca metadata tertentu.
4. Sistem hanya untuk satu pengguna.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang diuraikan diatas, dapat ditentukan tujuan penelitian sebagai berikut :

1. Merancang sebuah sistem guna menampilkan metadata *output* DFXML untuk manajemen bukti digital yang mudah dibaca.
2. Kinerja pada sistem yang didapat kemudahan dan keterbatasan dalam mengimplementasikan *output* DFXML kedalam sistem manajemen bukti digital yang dapat menyimpan file dd dan membaca hasil file XML.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

1. Memberikan manfaat terhadap pengembangan ilmu forensika digital pada umumnya.
2. Membantu investigator untuk membaca dan menganalisa metadata barang bukti dari sebuah kasus.
3. Membantu investigator dalam memberikan informasi kasus dan informasi barang bukti dalam setiap kasus.
4. Penelitian ini diharapkan mampu memberikan solusi untuk manajemen bukti digital yang terorganisir dan dapat dikelola untuk mempermudah pemeliharaanya.

1.6 *Review* Penelitian

Merujuk pada penelitian terdahulu yang telah dilakukan sebelumnya berkaitan dengan konsep manajemen bukti digital.Penelitian pertama dilakukan oleh (Garfinkel, 2011b) DFXML dapat digunakan untuk menggambarkan artefak forensik dengan menyajikan sebuah API (*Application Programing Interface*) yang memungkinkan untuk sebuah prototipe dengan langkah pengolahan digital forensik untuk kemudahan menghasilkan objek DFXML.

Penelitian kedua dilakukan oleh (Vries, Alink, Bhoedjang, Boncz, & Vries, 2006) yang menggunakan pendekatan XML untuk pengelolaan dan query forensik di ekstraksi dari bukti digital. Penggunaan XML sebagai *output* membuat XIRAF mengekstrak fitur secara otomatis.

Penelitian ketiga dilakukan oleh (Cohen et al., 2009) penelitian ini menggunakan kerangka AFF4 sebagai standar *platform* manajemen bukti. Penelitian ini menghasilkan sebuah tempat penyimpanan tambahan yang signifikan terhadap beberapa jenis bukti dari beberapa perangkat.

Penelitian keempat dilakukan oleh (Turner, 2005) menggunakan metode *selective imager* yang memungkinkan struktur file logis dari *disk* dapat dilihat hasil metadatanya. *Digital Evidence Bag* terdiri dari sebuah direktori yang mencakup file banyak yang berisi metadata seperti nama, organisasi, pemeriksa forensik dan hash yang terkandung pada bukti digital.

Penelitian kelima dilakukan oleh (Levine & Liberatore, 2009) DEX membuat ekstensif menggunakan atribut XML yang diperlukan untuk aturan parsing kompleks. DEX memiliki tujuan yang memungkinkan untuk membuat bukti asli dari deskripsi XML dan memungkinkan perbandingan alat dan validasi.

Rangkuman terhadap penelitian sebelumnya yang telah dilakukan, dapat dilihat pada tabel 1.1 seperti tabel di bawah ini.

Tabel 1.1 Perbandingan Penelitian Terdahulu

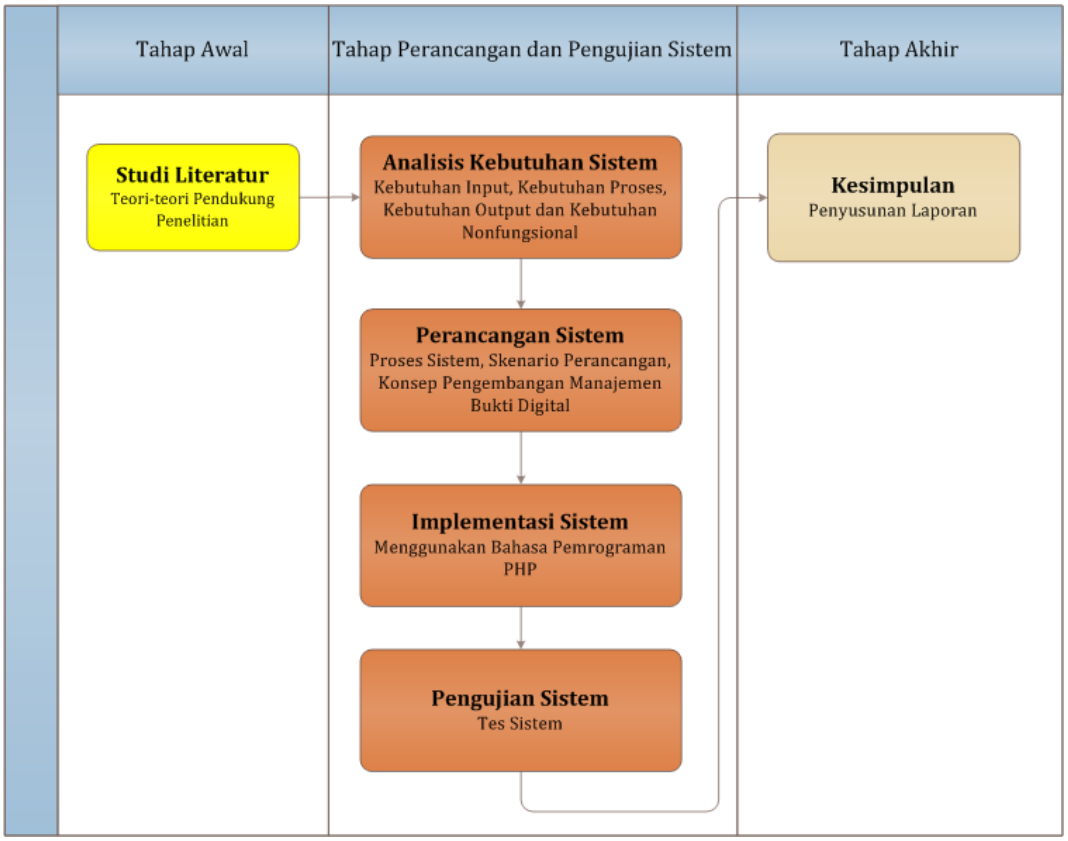
No	Paper	Masalah Utama	Metode yang digunakan	Hasil yang didapat
1	(Garfinkel, 2011b)	*DigitalForensics*XML&*the* DFXML*Toolset*	DFXML dapat digunakan untuk menggambarkan artefak forensik dengan menyajikan sebuah API (*Application Programing Interface*) yang memungkinkan untuk sebuah prototipe	Sebuah langkah pengolahan digital forensik untuk kemudahan menghasilkan objek DFXML
2	(Vries et al., 2006)	XIRAF – *Ultimate Forensic Querying*	Menggunakan pendekatan XML untuk pengelolaan dan *query* forensik di ekstraksi dari bukti digital	Penggunaan XML sebagai *output* membuatXIRAF mengekstrak fitur secara otomatis
3	(Cohen et al., 2009)	*Extending the Advanced Forensic Format to Accommodate Multiple Data Sources, Logical Evidence, Arbitrary Information and Forensic Workflow*	Menggunakan kerangka AFF4 sebagai standar *platform* manajemen bukti.	Menghasilkan sebuah tempat penyimpanan tambahan yang signifikan terhadap beberapa jenis bukti dari beberapa perangkat
4	(Turner, 2005)	*Unification of digital evidence from*	Menggunakan metode *selectiveimager* yang	*Digital Evidence Bag* terdiri dari sebuah direktori yang mencakup file

No	Paper	Masalah Utama	Metode yang digunakan	Hasil yang didapat
		disparatesources	memungkinkan struktur file logis dari disk dapat dilihat hasil metadatanya	banyak yang berisi metadata seperti nama, organisasi, pemeriksa forensik dan *hash* yang terkandung pada bukti digital
5	(Levine & Liberatore, 2009)	DEX: *Digital Evidence Provenance SupportingReproducibility and Comparison*	DEX membuat ekstensif menggunakan atribut XML yangdiperlukan aturan *parsing kompleks*	DEX memiliki tujuan yang memungkinkan untukmembuat bukti asli dari deskripsi XML dan memungkinkan perbandinganalat dan validasi.
6	(Widatama, 2017)	Penyimpanan informasi metadata bukti digital dan akses kontrol terhadap bukti digital	Dengan metode LPBD memiliki 4 struktur bagian untuk menyimpan sebuah file bukti digital, yaitu: *warehouse, cabinet, rack* dan *bag*	Mampu menyelesaikan solusi perlunya penyimpanan bukti digital dan dokumentasi terhadap bukti digital.
7	Usulan Penelitian	Membangun Sistem Untuk Manajemen Bukti Digital untuk *Output* DFXML	Mengimplementasikan sebuah sistem untuk manajemen bukti digital yang dapat memudahkan investigator dalam pembacaan metadata pada	Pengembangan *Output* DFXML Untuk Manajemen Bukti Digital

No	Paper	Masalah Utama	Metode yang digunakan	Hasil yang didapat
			output DFXML	
		File *imaging* bukti digital yang menghasilkan format XML, membuat investigator mengalami kesulitan dalam melaporkan apa yang terjadi pada objek tersebut. Investigator juga mengalami kesulitan dalam pembacaan metadata hasil dari format XML. Atas dasar permasalahan tersebut, salah satu solusi yang diajukan adalah dengan membuat sebuah sistem yang mampu mengidentifikasi elemen-elemen XML apa saja yang dapat digunakan untuk kepentingan manajemen bukti digital pada fileDFXML yang telah diakuisisi sehingga perlu dilakukan sebuah penelitian mengenai pengembangan *output* DFXML untuk manajemen bukti digital dengan cara mendapatkan file XML dari akuisisi bukti digital kemudian di masukkan ke dalam sistem.		

Agar penelitian ini terarah dan mendapatkan hasil yang maksimal, maka diperlukan metode penelitian menggunakan beberapa tahapan seperti gambar 1.1 di bawah ini.

1.7 Metode Penelitian



Gambar 1.1 Metodologi Penelitian

Pada gambar 1.1 menunjukkan penilitian ini menggunakan 6 tahapan penelitian yakni Studi Literatur, Analisis Kebutuhan Sistem, Perancangan Sistem, Implementasi Sistem, Pengujian Sistem dan Kesimpulan.

1.8 Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian yang dibuat , maka dibuat sistematika penulisan pada penelitian ini :

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, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menjelaskan teori-teori yang digunakan sebagai dasar landasan teoripengembangan *output* DFXML untuk manajemen bukti digital.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian dan gambaran umum langkah penyelesaian. Berisi tentang perancangan sistem yang akan dibangun dan rancangan pengujian sistem.

BAB IV HASIL DAN PEMBAHASAN

Hasil dan pembahasan, berisi tentang hasil implementasi sistem dan hasil pengujian sistem sesuai dengan rancangan pada bab 3.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini menguraikan tentang kesimpulan dari seluruh bab-bab yang telah dibahas yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Forensika Digital

Menurut (Morioka, 2016) forensika digital adalah metode yang dapat dijelaskan secara ilmiah dan dapat dibuktikan. Tujuan dari aktivitas forensika digital ini adalah untuk menjaga, mengumpulkan memvalidasi, mengidentifikasi menganalisis, menafsirkan, mendokumentasikan dan menyajikan bukti digital yang terdokumentasi dalam bentuk *chain of custody* untuk dipresentasikan di pengadilan. Sedangkan menurut (Agarwal, Megha, & Saurabh, 2011) forensik digital adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis,menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekontruksi kejadian serta keabsahan proses peradilan. Ada dua istilah barang bukti yang sering digunakan dalam forensika digital. Yaitu barang bukti elektronik dan barang bukti digital.Kedua istilah ini memiliki arti yang berbeda.

Menurut (Al-Azhar, 2012) barang bukti elektronik yang bisa juga disebut perangkat digital lebih berupa kepada barang bukti yang berwujud secara fisik dan dapat dikenali secara visual yang berupa perangkat elektronik seperti komputer, *handphone*, laptop, dan lain sebagainya yang memiliki bentuk fisik. Sedangkan barang bukti digital merupakan data digital yang tersimpan di dalam perangkat elektronik tersebut dan baru akan muncul setelah barang bukti elektronik tersebut diakusisi. Sebagai contoh, komputer merupakan barang bukti elektronik, setelah diakusisi, maka hasil akuisi tersebut merupakan bukti digital. Setelah adanya barang bukti digital, barang bukti elektronik boleh disimpan ke dalam ruangan penyimpanan barang bukti. Karena yang akan dianalisa adalah barang bukti digitalnya.

Dalam ilmu forensik digital terdapat prinsip – prinsip dasar. Adapun prinsip dasar forensika digital menurut (ACPO, 2011) antara lain :

1. Sebuah lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.

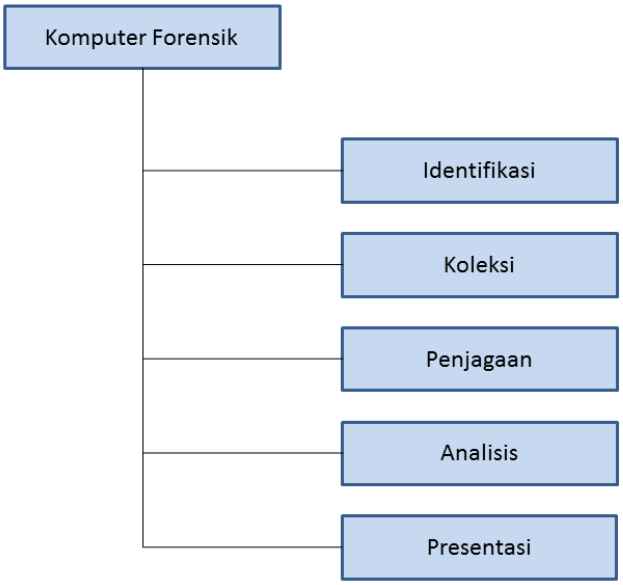
2. Untuk seseorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi, dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Terdapat catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisis berlangsung. Jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama.
4. *Person in charge* dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

2.2 Komputer Forensik

Forensik Komputer adalah ilmu untuk mengidentifikasi, mengekstrak melestarikan, dan menyajikan bukti digital disimpan dalam perangkat digital yang dapat diterima secara hukum di pengadilan karena kejahatan cyber atau penipuan (Rani, 2015).

Tujuan dari teknik forensik komputer adalah untuk mencari, melestarikan dan menganalisa informasi tentang sistem komputer untuk menemukan bukti (Strickland, 2016)

Forensik komputer berdasarkan konsep FBI, ada empat langkah utama dalam proses (Grande & Guadron, 2016). Seperti gambar 2.1 di bawah ini



Gambar 2.1 Langkah Forensik Komputer (Grande & Guadron, 2016)

Langkah yang pertama adalah identifikasi, setelah terjadi kejahatan sebuah identifikasi yang terdiri atas pengetahuan dan verifikasi pidana bertindak harus dimulai. Umumnya dilakukan dengan penilaian sumber daya, ruang lingkup dan tujuan untuk mencapai tujuan investigasi pada kasus kejahatan tersebut, yang harus dilakukan dengan tim yang tepat, dengan batasan, fungsi dan tanggung jawab. Selain itu, penyelidikan sebelumnya harus dilakukan untuk mendeskripsikan situasi saat ini, fakta dan pihak yang terkena dampak, salah satunya adalah tersangka, infrastruktur yang telah dilanggar, untuk memahami situasi dan menentukan jalur tindakan ikuti menurut penyelidikan.

Langkah kedua adalah koleksi barang bukti. Sebuah tim yang sesuai dengan seperangkat pedoman untuk pengumpulan bukti digital dan pengarsipan. Tindakan dalam pengumpulan barang bukti saat terjadi kasus kejahatan sangat penting untuk memenuhi syarat dalam pengumpulan barang bukti.

Langkah ketiga adalah penjagaan, pemeliharaan atau pelestarian barang bukti yang ditemukan. Setelah bukti telah-telah dikumpulkan, dianjurkan untuk memotret peralatan sesuai dengan penemuan barang bukti dengan nomor urut ditampilkan, pemotretan barang bukti nantinya berguna untuk mencocokkan perbandingan. Konfigurasi internal koneksi harus difoto, seluruh proses yang berlangsung juga perlu didokumentasikan, dan mengikuti pedoman dari *Chain of Custody*.

Langkah keempat adalah analisis. Ketika menyelesaikan pengumpulan bukti digital yang diperlukan untuk memecahkan kasus ini, analisis harus dilakukan pada Jaringan terisolasi dengan peralatan yang mampu untuk melaksanakan tugas. Ada hardware dan software yang berbeda, yang akan melakukan analisis forensik untuk memberikan sebuah solusi. Semua tergantung pada teknisi forensik dan lingkungan kerja untuk memilih alat yang digunakan pada analisis bukti. Analisis bukti digital dapat dilakukan dengan 2 cara:

- analisis *post-mortem*: ketika bukti yang dianalisa dengan peralatan khusus dalam komputer forensik. Biasanya ditemukan di laboratorium dan memiliki fitur perangkat keras dan perangkat lunak yang diperlukan untuk analisis.
- analisis TKP: analisis TKP tidak dianjurkan, tetapi jika tidak ada pilihan lain dapat dilakukan. Untuk kasus ini, dianjurkan untuk menggunakan perangkat penyimpanan analisis forensik yang berbeda dan tidak boleh ada yang dirubah dengan cara apapun sistem dikompromikan. Setelah adegan analisis kejahatan, analisis *post-mortem* harus dilakukan.

Langkah yang terakhir adalah presentasi. Presentasi merupakan langkah penting dari semua proses karena itu akan memungkinkan untuk menampilkan data yang akurat, mudah dipahami, jelas dan lengkap dalam laporan tertulis dengan langkah-langkah yang dilakukan dalam proses analisis, penemuan dan interpretasi setiap langkah untuk memberikan kesimpulan untuk masing-masing barang bukti yang ditemukan. Dalam kebanyakan kasus, dokumen ini disajikan untuk lembaga atau pengadilan yang tidak memiliki pengetahuan teknik yang cukup subjek, sehingga harus ditulis dengan cara yang mudah dan dimengerti.

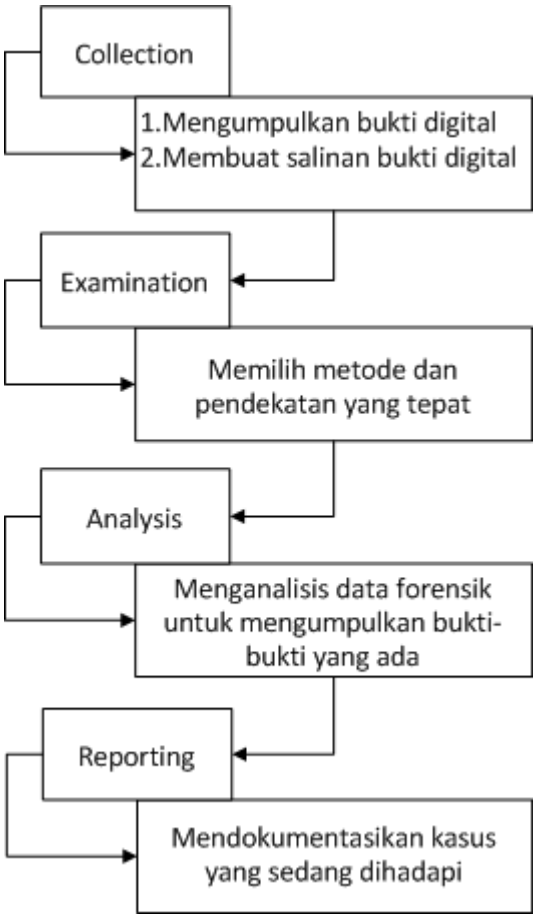
2.3 Manajemen Bukti Digital

Manajemen banyak diartikan dari berbagai sudut pandang, namun semuanya tertuju pada satu maksud yaitu pengambilan keputusan tetapi manajemen dapat juga di artikan dengan mengelola maupun mengatur suatu hal. Manajemen informasi metadata berorientasi dengan implementasi prototipe. Manajemen metadata dalam sistem file terdistribusi merupakan faktor kunci yang mempengaruhi kinerja sistem dan skalabilitas dalam penyimpanan data (Huo & Yi, 2015). Manajemen ini berkaitan dengan interaksi antara manusia dan komputer, dimana manajemen dapat mengelompokkan suatu data atau file-file yang ada pada komputer dan mampu mengatur semua file dari pengguna, manajamen file yang ada pada komputer juga dapat dihapus sesuai keinginan pengguna (Hasan, Anutariya, & Ja, 2012). Manajemen adalah sebuah proses perencanaan, pengorganisasian, pengkoordinasian, dan pengontrolan sumber daya untuk mencapai sasaran secara efektif dan efesien (Griffin, 2012). Efektif berarti bahwa tujuan dapat dicapai sesuai dengan perencanaan, sementara efisien berarti bahwa tugas yang ada dilaksanakan secara benar, terorganisir, dan sesuai.

Definisi bukti digital menurut (Harbawi & Varol, 2017) adalah jejak yang dinginkan maupun tidak diinginkan yang berasal dari perubahan data digital pada perangkat elektronik.

Informasi probabilitas apapun yang disimpan atau dikirim secara digital, yang dapat digunakan oleh pihak yang berwenang dalam persidangan peradilan di pengadilan, disebut sebagai bukti digital (Member,Cattaneo, & Maio, 2013). Bukti digital mencakup informasi tentang komputer, file audio, rekaman video, dan gambar digital (Commitee Joint Technology, 2016).

Prosedur dalam forensika digital, secara umum terdapat 4 proses utama, yaitu: *collection, examination, analysis* dan *reporting* (Dogan & Akbal, 2017), berikut adalah proses dari forensika digital yang ditunjukkan pada gambar 2.2 di bawah ini:



Gambar 2.2 Proses Utama Forensika Digital (Dogan & Akbal, 2017)

Berikut adalah penjelasan proses utama dalam forensika digital pada gambar 2.2.

1. *Collection,* bukti digital dikumpulkan dan dilakukan proses *imaging*.
2. *Examination,* mencari dan menentukan metode yang bertujuan untuk menguji bukti digital.
3. *Analysis,* langkah untuk menganalisis yang bertujuan untuk menemukan bukti digital yang sesuai dengan informasi yang dibutuhkan oleh otoritas yudisial atau keadilan.
4. *Reporting,* fase persiapan dokumentasi untuk diajukan ke otoritas pengadilan.

Dari beberapa referensi yang terkait tentang pengertian manajemen bukti digital, dapat disimpulkan manajemen bukti digital merupakan suatu cara untuk mengelola informasi data mencakup semua informasi tentang file yang ada didalam komputer yang berupa file gambar, file audio, maupun file digital yang lain, dengan menggunakan prosedur yang telah ditentukan untuk mencapai tujuan tertentu dan bukti digital tersebut dapat diterima di pengadilan.

2.4 *Chain Of Custody*

Chain of Custody adalah prosedur dalam penanganan bukti dalam serangkaian penyelidikan (Prayudi, 2015). *Chain of Custody* dalam bahasa indonesia berarti lacak balak, tetapi sangat aneh untuk diartikan seperti itu.

Konsep yang diusulkan kerangka kerja untuk menjamin keamanan berdasarkan 5 W dan 1 H (Ćosić & Bača, 2010).

- *Why* (mengapa) kejahatan telah dilakukan.
- *Who* (siapa) penggunaan biometri untuk tujuan otentikasi dari semua orang yang berhubungan dengan penyelidikan
- *What* (apa) sebuah jejak atau fungsi *hash* (SHA-2) bukti.
- *When* (ketika) menambahkan catatan waktu.
- *Where* (dimana) menggunakan lokasi.
- *How* (cara) menggunakan enkripsi asimetris untuk bukti.

2.5 XML

Salah satu format penyimpanan data yang memiliki struktur hierarkis yang sama dengan database relasional dan mudah dalam pertukaran informasi yaitu XML. Menurut (Tekli & Member, 2016) XML atau *eXtensible Markup Language* sebagai model representasi data semi terstruktur standar pada *web* yang memiliki kemampuan untuk menyaring informasi bentuk bebas dan membentuk ulang terstruktur (data relasional, hierarkis, dan grafik) menjadi format semi terstruktur yang telah terbukti penting dalam memfasilitasi skala pengolahan data otomatis. Dengan menggunakan format dokumen XML, *web service* memungkinkan banyak kemudahan dan perbaikan dalam mendukung integrasi berbagai *platform* sistem dan aplikasi, baik melalui infrastruktur intranet maupun internet, dan informasi yang dibutuhkan tersebut dapat diakses dari mana saja dan dengan *computing device, platform*, atau aplikasi yang kita gunakan.

2.6 Metadata

Metadata adalah data yang menggambarkan, mengidentifikasi dan memperbaiki penyaringan dan pengambilan data lainnya (Zghal, Mnif, Amel, & Amous, 2015). Metadata terdiri dari komponen (*role*) dan elemen. *Role* merupakan *header* dari elemen, elemen berisi informasi mengenai data. Metadata terdiri atas beberapa 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.

Metadata dapat memberikan penyidik dengan kekayaan informasi tentang file yang sedang diselidiki. Selanjutnya, penyidik forensik dapat menggunakan metadata untuk mendapatkan informasi, misalnya: file penulis, tanggal dan waktu penciptaan, berapa kali file yang telah dimodifikasi, termasuk ketika modifikasi mengambil tempat (Alanazi, Lebh, & Jones, 2015)

Kategori metadata file system adalah:

- Informasi tentang ukuran file
- Unit data spesifikdialokasikan dan,
- Waktu akses dalam file.

2.7 DFXML

Digital Forensics XML (DFXML) menurut (Garfinkel, 2011) adalah sebuah bahasa XML yang memungkinkan terjadinya perubahan struktur informasi forensik. DFMXL dapat mewakili asal subyek data untuk investigasi forensik, mendokumentasikan keberadaan dan lokasi dari file sistem dan informasi teknis lainnya. Penggunaan spesifik untuk DFXML mengembangkan kemampuan mengubah dengan menyediakan sebuah bahasa untuk mendeskripsikan proses-proses forensik.

2.7.1 Rancangan DFXML

DFXML dimaksudkan untuk mewakili jenis data forensik berikut (Garfinkel, 2011):

- Metadata yang menggambarkan nama file termasuk informasi lainnya.
- Informasi terperinci tentang alat forensik yang melakukan pemrosesan (misalnya, nama program dan nomor versi, dimana program dikompilasi, perpustakaan terkait).
- Keadaan komputer tempat pemrosesan dilakukan (misalnya, nama komputer).
- Bukti atau informasi yang diekstrak, bagaimana cara diekstraksi, dan dimana letaknya secara fisik.
- Nilai *hash* kriptografi urutan *byte*.
- Informasi spesifik sistem operasi yang berguna untuk analisis forensik.

2.7.2 *Tools* yang menghasilkan DFXML

Bulk extractor adalah salah satu *tools* yang menghasilkan XML dengan menggunakan DFXML untuk melaporkan konfigurasi masing-masing dan asal file *input* (Garfinkel, 2011).

2.7.3 Fiwalk DFXML dan Bitcurator

Fiwalk (Garfinkel, 2011) adalah bagian dari koleksi alat forensik digital *The Sleuth Kit* dan digunakan untuk menghasilkan laporan DFXML tentang isi pada file. Seperti namanya, *fiwalk* akan mengumpulkan informasi (metadata) tentang masing-masing file, termasuk tanggal file terakhir diakses, tanggal dimodifikasi terakhir, jenis file, pengguna yang membuat file, dan banyak lagi. *File object* adalah XML *forensics* dan XML elemen yang digunakan untuk menggambarkan informasi tentang sebuah file. Objek file dapat berisi informasi tentang:

- Nama file
- Kode *hash* file
- Lokasi file pada disk
- Metadata
- Blokir *hash*, *Filter Bloom*, atau Digestitas untuk file

Fiwalk bisa dijalankan melalui *command line* atau dari Bitcurator *Reporting Tool*.

Bitcurator adalah salah satu turunan dari Linux Ubuntu, *Bitcurator* mengembangkan *software* untuk mengekstrak, menganalisis dan menghasilkan laporan dari sebuah bukti digital.

Bitcurator membahas dua kebutuhan mendasar untuk mengumpulkan institusi yang tidak ada dalam perangkat lunak yang dirancang untuk industri forensik digital digabungkan ke dalam alur kerja pengelolaan, dan penyediaan akses publik terhadap data.

Bitcurator mendefinisikan dan menguji dukungan untuk alur kerja kekurangan digital yang dimulai pada titik menghadapi kepemilikan yang berada pada media yang dapat dilepas baik akuisisi baru atau materi yang berada dalam kepemilikan repositori yang ada dan berlanjut sampai pada titik interaksi dengan pengguna akhir.

Fitur *bitcurator* meliputi:

- Triase data pra-pencitraan
- Pencitraan disk forensik
- Analisis dan pelaporan sistem berkas

- Identifikasi informasi pribadi dan identifikasi individu
- Ekspor metadata teknis dan lainnya

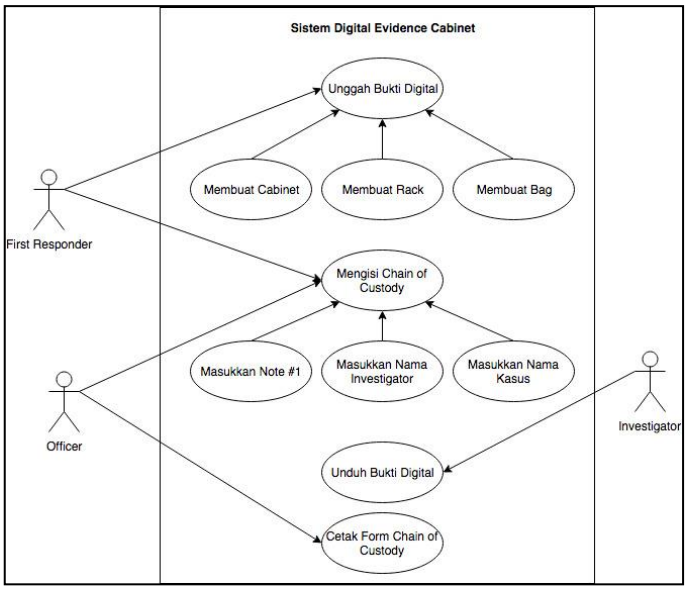
2.8 Sistem Lemari Penyimpanan Bukti Digital

Konsep dasar pada sistem Lemari Penyimpanan Bukti Digital (LPBD) (Widatama, 2017) ini adalah membuat membuat sebuah lemari penyimpanan bukti digital dengan prosedur penyimpanannya sama seperti bukti elektronik seperti halnya sebuah lemari penyimpanan barang bukti pada bukti fisik. Penyimpanan barang bukti pada bukti fisik memerlukan sebuah lemari yang berisi rak-rak untuk menaruh sebuah kantong-kantong yang berisi bukti fisik atau bukti elektronik yang ditemukan saat menangani sebuah kasus. Investigator akan mencatat waktu, jenis bukti elektronik dan siapa yang mengambil bukti elektronik dari lemari penyimpanan tersebut. Konsep ini akan memberikan pembatasan hak akses terhadap bukti dimana tidak semua orang tidak dapat mengaksesnya. Konsep ini juga menyimpan informasi metadata bukti digital pada struktur Bahasa XML saat bukti digital tersebut diunggah pada lemari penyimpanan. Metadata yang ada pada konsep LPBD dijelaskan pada tabel 2.1 di bawah ini

Tabel 2.1 Jenis Metadata (Widatama, 2017)

Tipe Metadata	**Informasi yang Disimpan**
Descriptive Metadata	Nama bukti digital
Technical Metadata	Tipe File (dengan format DD atau AFF)
	Ukuran File (dalam satuan kB)
	Waktu Unggah (masuknya bukti digital ke LPBD)
Preservation Metadata	*Checksum/*fungsi *hash* (SHA1 dan MD5)

Kelebihan pada sistem LPDB ini adalah dapat menyimpan file selain file dd. Dimana sistem LPDB dapat menyimpan file e01 dan AFF (*Advanced Forensics Format*). Konsep LPDB juga dapat menampilkan fungsi *hash* selain MD5 yaitu SHA1. Sistem pada LPBD juga lebih terstruktur karena ada lemari, rak dan kantong bukti digital. Maka pada sistem LPBD dalam penggunaannya dibagi menjadi 3, yaitu *First Responder*, Investigator dan *Officer* yang masing-masing pengguna mempunyai pekerjaan dan hak akses untuk menangani sebuah kasus. Tiga pengguna tersebut digambar kan seperti gambar 2.3di bawah ini



Gambar 2.3 Interaksi Antar Pengguna (Widatama, 2017)

Konsep yang digunakan pada Lemari Penyimpanan Bukti Digital seperti konsep lemari penyimpanan barang bukti secara fisik dimana ada lemari yang berisikan sebuah rak, dan didalam rak berisi beberapa barang bukti elektronik hasil penyitaan sebuah kasus.

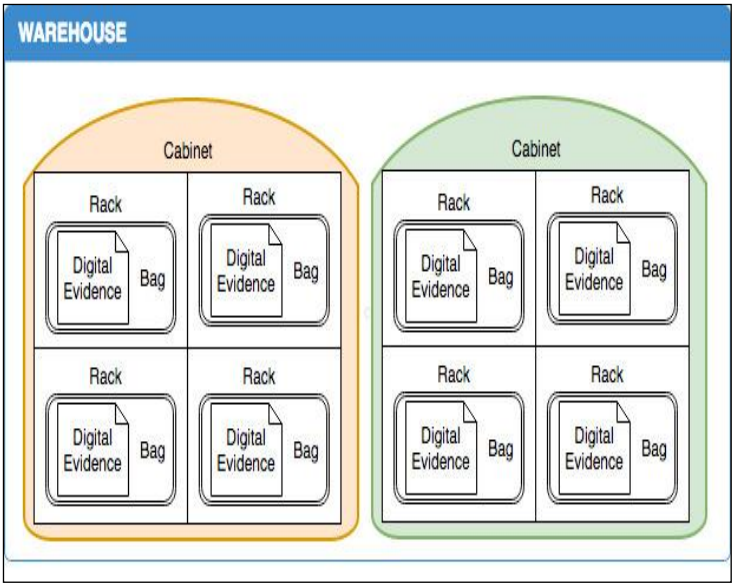
Warehouse merupakan sebuah nama direktori untuk menyimpan semua *file* bukti digital. *Warehouse* tidak memiliki struktur xml, sehingga untuk melihat *file* bukti digital dapat langsung mengakses direktori *warehouse*.

Cabinet merupakan nama direktori yang berada di dalam direktori *warehouse*. Berbeda dengan *warehouse* yang tidak memiliki struktur xml, *cabinet* merupakan struktur elemen xml tertinggi dari LPBD (*Top Root*).*Cabinet* memiliki attribut dengan nama "*name.*" Nilai atribut dari elemen *cabinet* bersifat dinamis yang nantinya akan menyesuaikan dengan nama *cabinet.*

Rack merupakan "anak" (*child*) dari elemen *cabinet.* Sama halnya dengan *cabinet, rack* juga memiliki atribut dengan nama "*rack_name*". Nilai atribut *rack_name* bersifat dinamis yang dapat diberi nama sesuai dengan yang diinginkan pengguna.

Bag adalah sub elemen (*child*) dari elemen *rack. Bag* memiliki atribut yaitu "*bag_name".* Nama *bag* dapat menyesuaikan dengan yang diinginkan oleh pengguna. Pada elemen *bag* inilah terdapat sub elemen *digital_evidence* yang digunakan untuk menyimpan metadata bukti digital.

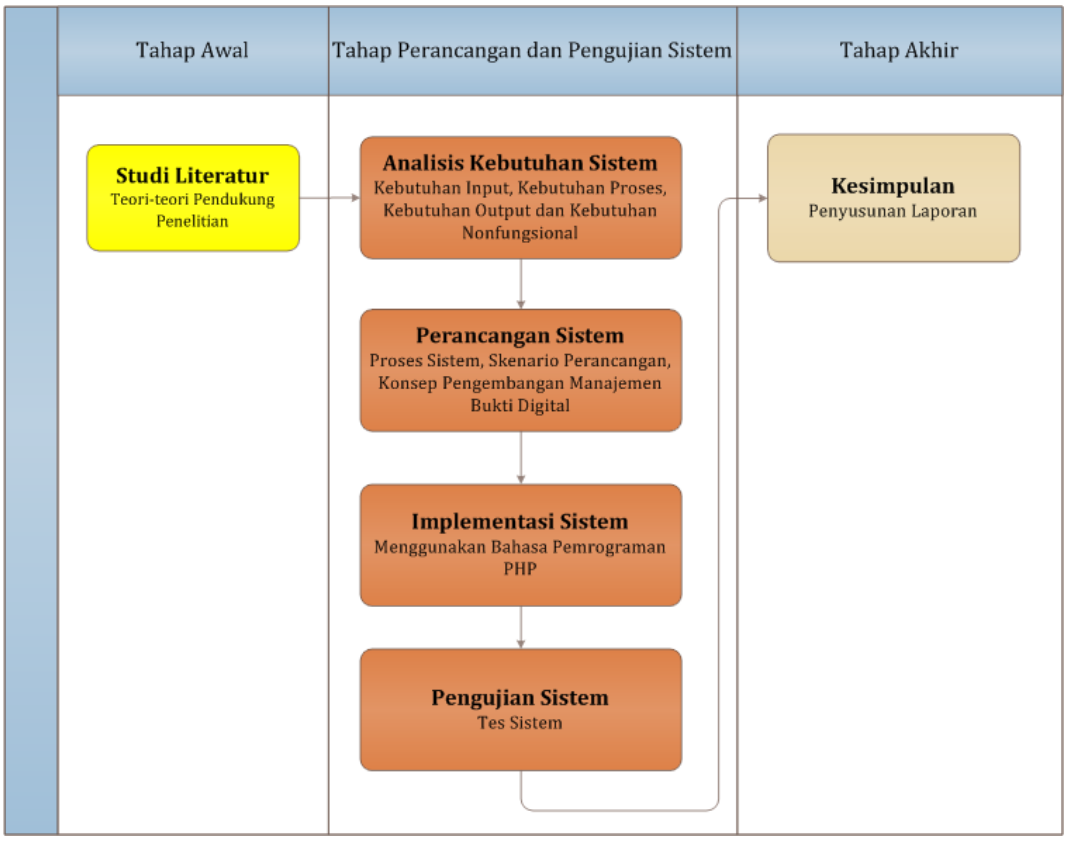
Konsep yang ada dalam sistem Lemari Penyimpanan Bukti Digital (LPDB) digambarkan seperti gambar 2.4 di bawah ini



Gambar 2.4 Struktur Penyimpanan Bukti Digital (Widatama, 2017)

BAB 3
Metodologi Penelitian

Bab ini menjelaskan bagaimana cara penelitian dilakukan dengan mendeskripsikan setiap langkah-langkah yang dibuat secara sistematis sehingga dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, analisis hasil dan kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan – tahapan dalam penyelesaian masalah dapat dilihat pada gambar 3.1.



Gambar 3.1 Metodologi Penelitian

3.1 Studi Literatur

Studi literatur dilakukan sebagai tahapan awal yang mendasar untuk memberikan arahan bagi peneliti.Studi literatur dilakukan untuk mendapatkan informasi mengenai topik penelitian yang dapat bersumber dari buku, artikel atau bahan tertulis lainnya, yang berupa teori atau penemuan sebelumnya, baik bersifat *online source* maupun *offline source*.

Studi literatur dilakukan terhadap penelitian yang terkait pengembangan *output* DFXML untuk manajemen bukti digital, teori-teori tentang digital forensik, teori-teori

tentang bukti digital dan teori-teori tentang DFXML sehingga dapat menunjang tujuan akhir dari penelitian ini.

Berdasarkan pengumpulan data, pertama yang dilakukan adalah mengakuisisi bukti elektronik menjadi file dd, setelah mendapatkan file dd lanjut pada aplikasi *bitcurator* untuk mendapatkan file XML dari file dd yang telah diakuisisi. Setelah mengetahui cara kerja tersebut, maka dapat dilakukan pengajuan pembuatan sistem *output* DFXML untuk manajemen bukti digital.

3.2 Analisis Kebutuhan Sistem

Bukti elektronik akan diproses menggunakan *tools* DFXML yang hasilnya nanti akan berupa file dengan format dd dan format XML. Pada file dengan format XML akan menghasilkan baris-baris *scripting* yang akan menjelaskan tentang informasi bukti elektronik yang menjadi bukti digital (dd). Aplikasi hanya digunakan oleh satu pengguna.

3.2.1 Analisis Kebutuhan Sistem *Input*

Kebutuhan sistem *input* di dalam sistem ini adalah input yang dilakukan pengguna. Kebutuhan *input* tersebut meliputi:

- Input file XML dan dd hasil proses menggunakan *tools* DFXML
- Input informasi tambahan metadata yang ada pada sistem

3.2.2 Analisis Kebutuhan Sistem Proses

Kebutuhan sistem proses yang ada pada sistem ini adalah :

- Proses unggah file dd dan file XML
- Proses isi data informasi pada sistem
- Proses menampilkan *tools* hasil yang telah dimasukkan pengguna
- Proses membaca metadata XML
- Pembuatan sistem menggunakan bahasa PHP

3.2.3 Analisis Kebutuhan Sistem *Output*

Kebutuhan sistem *output* yang terjadi pada sistem ini yaitu menampilkan halaman yang berisi tentang file yang telah di unggah oleh pengguna dan semua informasi data pada sistem yang diisi oleh pengguna. Kebutuhan sistem *output* juga menampilkan hasil metadata file XML yang di unggah oleh pengguna.

3.2.4 Analisis Kebutuhan Nonfungsional

Kebutuhan nonfungsional meliputi perangkat keras dan perangkat lunak yang digunakan untuk menjalankan sistem yang dibangun ini. Perangkat keras yang dibutuhkan untuk membuat sistem ini yaitu Laptop merk Acer Aspire E14 dengan prosesor Core i5 dan RAM 4GB, untuk membangun serta pengujian sistem yang mendukung aplikasi. Sistem ini didukung dengan kebutuhan perangkat lunak untuk membangun sistem ini, diantaranya adalah

- XAMPP PHP

  XAMPP digunakan sebagai *localhost* atau *server* untuk pembuatan *website* yang didukung dengan PHP.
- *Sublime Text* 2

  Sublime text 2 sebagai *editor* teks untuk berbagai bahasa pemrograman, seperti bahasa pemrograman PHP yang digunakan untuk pembuatan sistem ini.
- *Google Chrome* dan *Mozilla Firefox*

  Keduanya digunakan sebagai *browser* untuk mengakses alamat *website* pada *localhost website* yang akan dibangun.

3.2.5 Analisis Kebutuhan Antarmuka

Kebutuhan antarmuka dirancang dengan *user friendly* adalah sebagai berikut:

- Halaman awal adalah halaman selamat datang pada sistem
- Halaman kedua adalah halaman tambah kasus dan informasi kasus
- Halaman ketiga adalah halaman dimana pengguna memasukkan data-data
- Pada halaman tambah kasus akan menampilkan hasil akhir dari data-data yang telah dimasukkan pengguna.

3.3 Perancangan Sistem

Membangun sebuah sistem manajemen bukti digital merupakan tahapan awal sebagai konsep pengembangan *output* DFXML untuk manajemen bukti digital. Konsep ini terinspirasi dari sulitnya untuk pembacaan metadata yang dihasilkan dari *output* DFXML. Bukti elektronik akan diproses pada *tools* DFXML menjadi file dengan format dd dan menghasilkan *report* dengan format XML. Maka perlu dibangun sebuah sistem untuk mempermudah dalam pembacaan metadatanya.

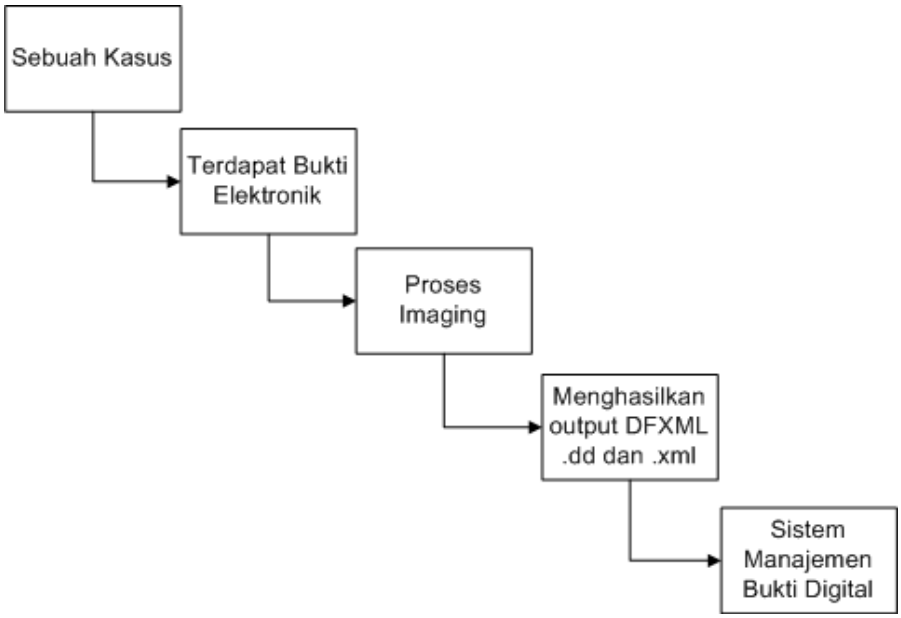
Perancangan sistem untuk pembacaan XML harus menggunakan *bitcurator* untuk menghasilkan file dengan format XML. *Bitcurator* mempunyai kelebihan dibandingkan

dengan aplikasi yang lain, *bitcurator* dapat menghasilkan file dalam bentuk XML, hasil file XML dari *bitcurator* dapat dibaca oleh berbagai jenis *platform* (dapat dibuka pada sistem operasi Windows, Mac maupun Linux). Perancangan sistem yang dibangun akan membaca XML yang dihasilkan oleh *bitcurator*. Pembacaan metadata dengan format XML memudahkan untuk mengidentifikasi dan menyusun informasi.

Perancangan sistem ini dibuat berdasarkan (Garfinkel, 2011) DFXML meningkatkan komposisi dengan menyediakan bahasa untuk menggambarkan proses forensik umum misalnya, *kriptografi hashing*, lokasi file, nama file dan waktu pembuatan maupun waktu perubahan data pada file. Berdasarkan pengalaman dalam mencari file pada sistem memungkinkan beberapa pencari menggunakan dengan nama file, bisa juga mencari dengan ekstensi file maupun menggunakan tanggal untuk mencari file. File juga dapat dicari dengan mengurutkan berdasarkan kapan data dibuat.

Sistem yang akan dibuat menggunakan aplikasi berbasis website. Aplikasi berbasis *website* mempunyai beberapa keunggulan diantaranya adalah mudah digunakan, dapat digunakan dalam berbagai macam sistem operasi apapun (*multi platform*). Kekurangan pada aplikasi berbasis website diantaranya *web server* yang harus di aktifkan terlebih dahulu (jika aplikasi *offline*).

Sebelum membangun sebuah sistem, buat skenario perancangan terlebih dahulu. Gambar skenario perancangan dapat dilihat pada gambar 3.2 di bawah ini

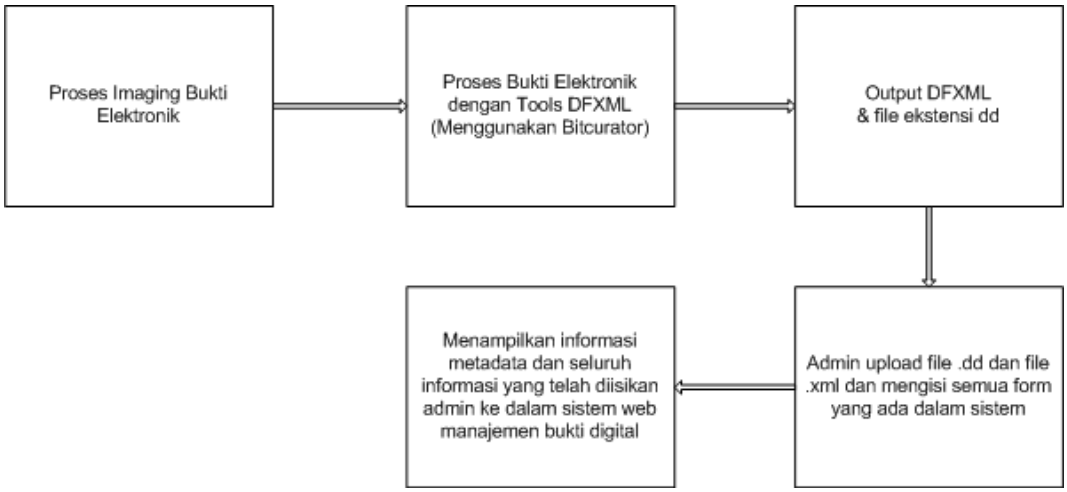


Gambar 3.2 Perancangan Sistem

Penjelasan skenario perancangan yang ada pada sistem pada gambar 3.2, dijelaskan sebagai berikut:

1. Pertama-tama diperlukan suatu kasus yang nantinya akan memberikan sebuah barang yang berupa barang elektronik yang nanti akan menjadi sebuah bukti digital.
2. Bukti elektronik dapat berupa *flashdisk*, *harddisk*, maupun barang elektronik lainnya.
3. Semisal bukti elektronik yang ditemukan sebuah *flashdisk*, *flashdisk* tersebut harus melalui proses *imaging* untuk menemukan bukti yang ada di dalam flashdisk tersebut dan dijadikan sebuah barang bukti digital agar barang bukti aslinya tetap terjaga keasliannya dan tidak terkontaminasi apapun.
4. Setelah ditemukan bukti digital yang ada pada *flashdisk* proses selanjutnya mengekstrak bukti digital dengan *bitcurator* untuk menghasilkan file dengan format XML yang nanti akan dibaca kan metadatanya.
5. Setelah semua proses selesai, maka di bangun sebuah sistem pengembangan *output* DFXML untuk manajemen bukti digital untuk mempermudah pembacaan metadata dari file XML dan dd.

Proses sistem yang akan dibangun seperti gambar 3.3 di bawah ini



Gambar 3.3 Proses sistem yang dibangun

Penjelasan gambar 3.3 alur rancangan umum sistem pengembangan *output* DFXML untuk manajemen bukti digital

1. Proses *imaging* bukti elektronik menjadi bukti digital di jadikan file dengan ekstensi dd.

2. Setelah itu file dengan ekstensi dd di ekstrak di VM *Virtual Box* dengan *tools* DFXML *bitcurator* yang akan menghasilkan file dengan ekstensi XML.
3. Setelah selesai diekstrak dengan *bitcurator*, pilih file yang telah diekstrak tadi pada folder yang diisi file berformat dd dan pilih file dengan ekstensi XML yang nantinya akan diunggah kedalam sistem yang dibangun.
4. Setelah itu masuk ke dalam sistem yang di bangun. Unggah file dengan ekstensi dd dan XML yang tadi telah diekstrak. Isi semua data informasi yang telah tersedia pada sistem.
5. Setelah selesai ungguh file dd, file XML dan semua data sudah diisi, maka sistem akan menampilkan semua informasi dan membaca metadata dari file yang di unggah oleh pengguna.

Pada tampilan hasil metadata yang dibaca, hanya ada beberapa metadata yang ditampilkan dari hasil XML, di antaranya adalah nama file, ukuran file, dan MD5 dari file dd. Pembacaan metadata dapat dilihat dalam bentuk tampilan *pop-up*, pengguna lebih cenderung suka melihat tampilan visual dari pada melihat tampilan yang berupa teks.

Pada konsep pengembangan *output* DFXML untuk manajemen bukti digital terdapat data statis dan data dinamis. Data statis dan data dinamis tersebut dapat dilihat pada tabel 3.1 di bawah ini

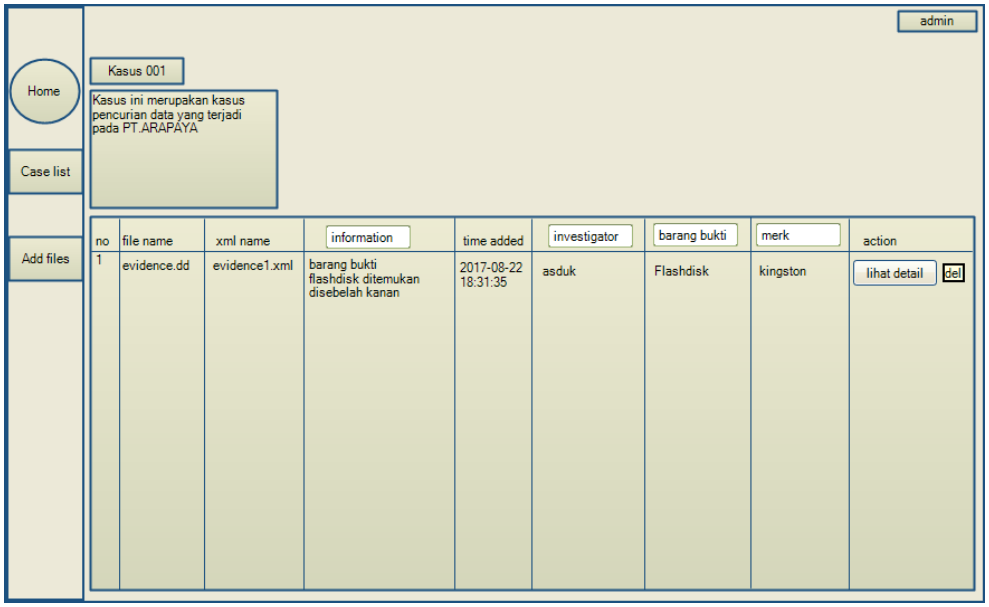
Tabel 3.1 Tabel Data Statis dan Data Dinamis

STATIS	**DINAMIS**
File .dd	Keterangan kasus
File .XML	Informasi barang bukti
Tanggal input kasus	Nama investigator
Action (lihat detail metadata)	Barang bukti
	Merk barang bukti

Tabel statis yang ada pada sistem yang dibangun terdapat 4 data, di antaranya ada file dengan ekstensi dd dimana file ekstensi dd ini merupakan hasil akuisisi bukti elektronik. File dengan ekstensi XML, dimana file dengan ekstensi XML hasil dari *bitcurator*. File selanjutnya adalah tanggal, dimana tanggal ini merupakan tanggal data dibuat. Data yang terakhir adalah metadata dimana pada metadata terdapat beberapa elemen yang diambil dari hasil XML, di antaranya ada nama file, ukuran file dan MD5 dari file dd.

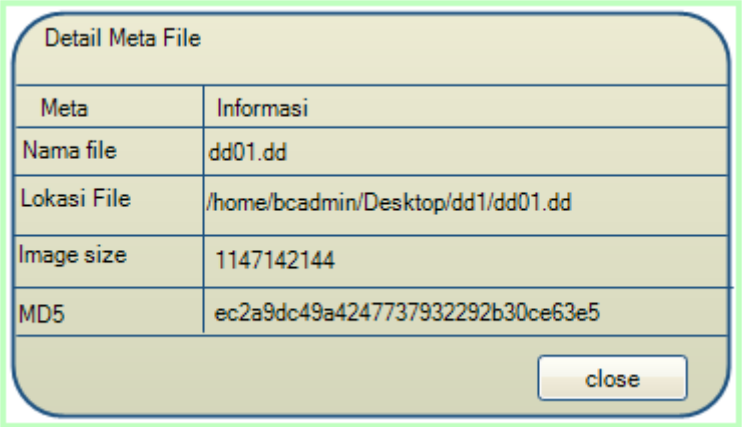
Tabel dinamis terdapat 5 data yang dapat dirubah jika suatu waktu data tersebut ada kesalahan. Data tersebut diantaranya ada keterangan kasus yang berisi informasi kasus yang ditangani. Data selanjutnya yang harus diisi adalah informasi barang bukti dimana berisi informasi tentang barang bukti ditemukan dimana. Data selanjutnya adalah nama investigator dan barang bukti yang ditemukan pada kasus *cybercrime*. Data dinamis yang terakhir adalah merk barang bukti.

Konsep manajemen bukti digital dari hasil *output* DFXML yang akan dibangun nantinya akan menampilkan halaman seperti gambar 3.4 di bawah ini



Gambar 3.4 Hasil *Output* DFXML

Metadata yang dibaca tampilannya menggunakan *pop-up*. Dimana investigator memilih tombol pada *button* lihat detail untuk melihatnya. Tampilan *pop-up* metadatanya seperti gambar 3.5 di bawah ini.



Gambar 3.5 Tampilan metadata

3.4 Implementasi Sistem

Tahap implementasi ini merupakan tahapan untuk merealisasikan dari rancangan sebuah sistem kedalam kondisi yang sebenarnya, sehingga dapat berjalan sesuai dengan rancangan. Pada pembuatan sistem menggunakan *Mozilla firefox, Google Chrome, Sublime Text* 2, XAMPP, PHP *My Admin*, *Oracle* VM *VirtualBox*, dan *bitcuarator*. Jenis file yang di uji hanya file dd dan hanya digunakan oleh satu pengguna. Cara kerja sistem yang dibangun akan dijelaskan lebih detail, sehingga dapat diketahui apakah sistem yang dibangun telah sesuai dengan perancangan. Pada bagian implementasi perangkat lunak akan dijelaskan bagaimana sistem bekerja, dengan memberikan tampilan-tampilan halaman yang dibuat. Kebutuhan perangkat lunak yang digunakan sebagai berikut:

1. Sistem operasi *Windows* 10
2. *XAMPP My*SQL digunakan untuk *database management system*
3. *Microsoft Office Word* 2010 digunakan untuk membuat dokumen laporan tesis
4. *Microsoft Office Visio* 2007 digunakan untuk membuat *flowchart*.

Kebutuhan perangkat keras yang digunakan sebagai berikut:

1. Laptop ACER Aspire E14
2. RAM 4GB
3. *Processor* Intel Core i5-5200U CPU @2.20Ghz
4. *Harddisk* 1000GB

Batasan-batasan asumsi yang mendasari dibuatnya sistem pengembangan *output* DFXML untuk manajemen bukti digital diantaranya:

1. Yang dapat mengakses sistem hanya admin yang mempunyai *username* dan *password*.
2. Sistem hanya dapat dioperasikan pada laptop maupun PC.

Implementasi juga merupakan tahap perancangan perangkat lunak yang direalisasikan dari rancangan sebuah sistem ke dalam kondisi yang sebenarnya, sehingga sistem dipastikan dapat berjalan sesuai dengan rancangan dan memastikan bahwa sistem yang dibangun mudah digunakan oleh pengguna dalam hal ini seorang investigator. Pada tahap implementasi, pembuatan sistem menggunakan *browser google chrome* atau *mozilla firefox, sublime, bitcurator, virtualbox* dan menggunakan bahasa pemrograman PHP. Kebutuhan antarmuka dari program tersebut adalah sebagai berikut:

1. Tampilan *Windows* 8 yang mudah digunakan.

2. Tampilan dalam membaca metadata forensik

3. Terdapat beberapa menu yang mempunyai fungsi masing-masing.

Cara kerja dari sistem yang dibangun akan dijelaskan dengan lebih detail, sehingga dapat diketahui apakah sistem yang dibangun telah sesuai dengan perancangan sistem. Pada bagian implementasi perangkat lunak akan dijelaskan bagaimana sistem bekerja, dengan memberikan tampilan-tampilan halaman yang dibuat.

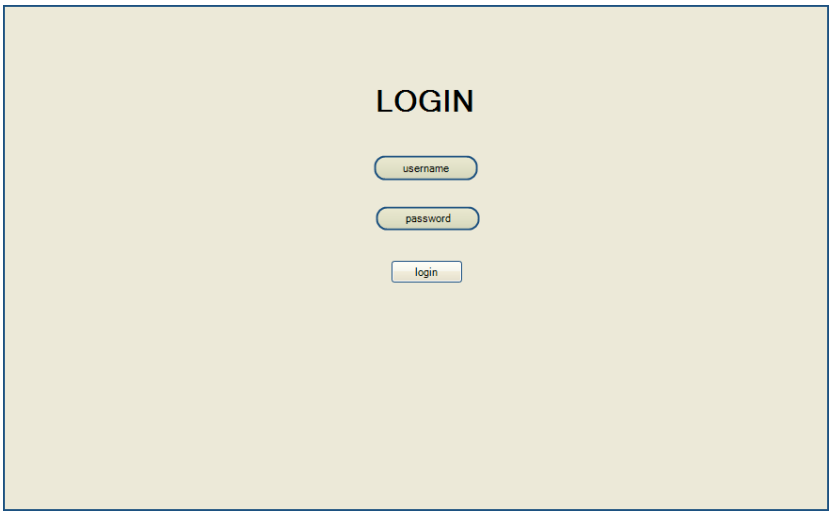
Dengan sebuah teknologi yang berkembang saat ini, maka dibuat sebuah sistem pengembangan *output* DFXML manajemen bukti digital dengan membangun sebuah konsep yang akan memudahkan investigator dalam membaca sebuah metadata. konsep tersebut akan dirancang seperti gambar 3.6 sampai 3.10.

Pada gambar 3.6 akan menunjukkan halaman *login* pengguna, dimana pengguna harus menggunakan *username* dan *password* untuk masuk kedalam sistem.

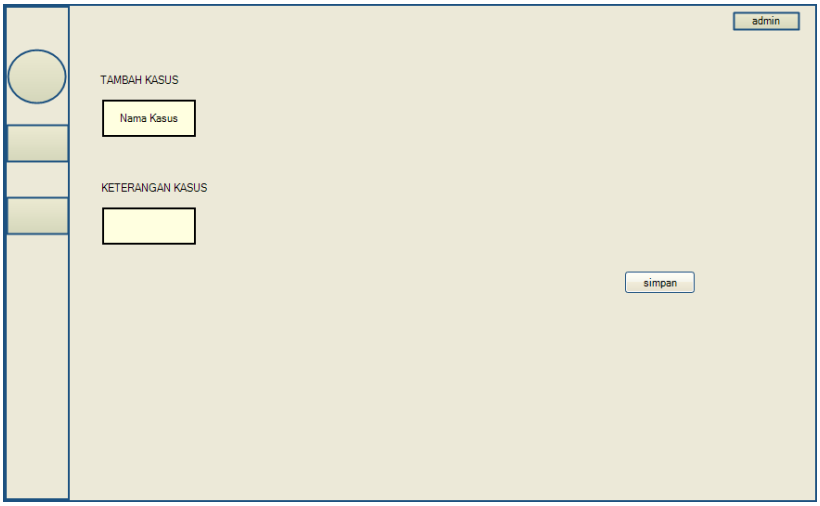
Pada gambar 3.7 akan menunjukkan halaman tambah kasus dan tambah keterangan kasus. Tambah kasus ini nantinya akan diisikan informasi kasus keberapa yang akan ditangani. Tambah keterangan kasus akan diisi tentang informasi kasus yang sedang ditangani.

Pada gambar 3.8 akan menunjukkan halaman kasus, dimana investigator harus memasukkan file dan data kasus yang ditanganinya terlebih dahulu, setelah semua file dan data dimasukkan investigator dapat melihatnya. Pada halaman kasus yang sudah tersimpan ada beberapa data yang dapat diperbarui dan dihapus datanya. Beberapa data yang dapat diperbarui diantaranya adalah informasi kasus, informasi pada barang bukti, nama investigator, barang bukti, dan merk barang bukti.

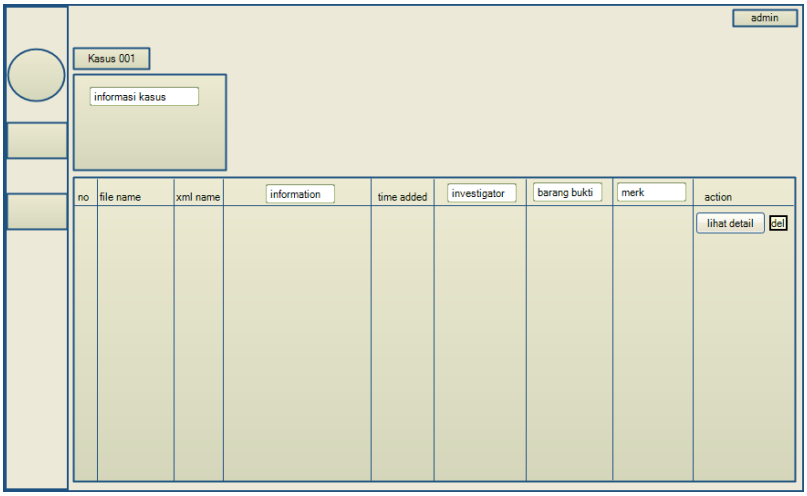
Pada gambar 3.9 menunjukkan halaman *add file* dimana investigator memasukkan semua file dan data kasus yang ditanganinya. *Add file* yang harus diisikan ada nama investigator, barang bukti yang ditemukan, merk barang bukti yang ditemukan, memilih kategori kasus, memberikan informasi mengenai barang bukti yang ditemukan serta memasukkan file XML dan file dd. Gambar 3.6 sampai 3.9 dapat dilihat seperti gambar di bawah ini.



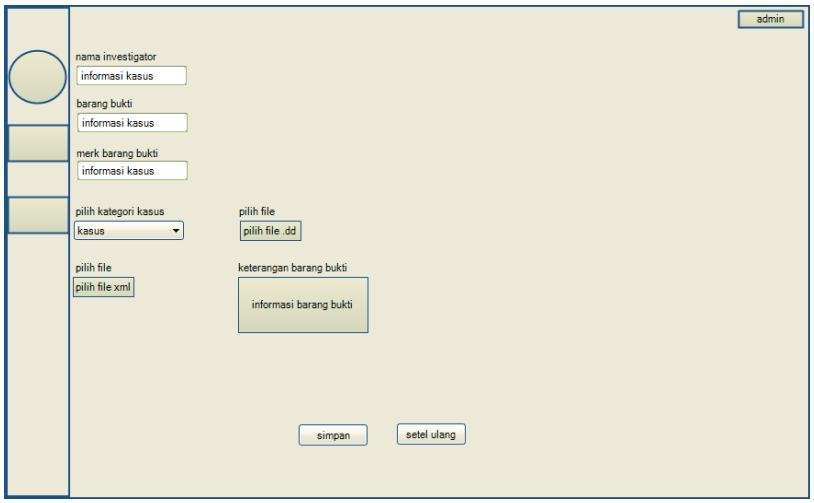
Gambar 3.6 Halaman *Login*



Gambar 3.7 Halaman Tambah Kasus dan Keterangan



Gambar 3.8 Halaman Kasus

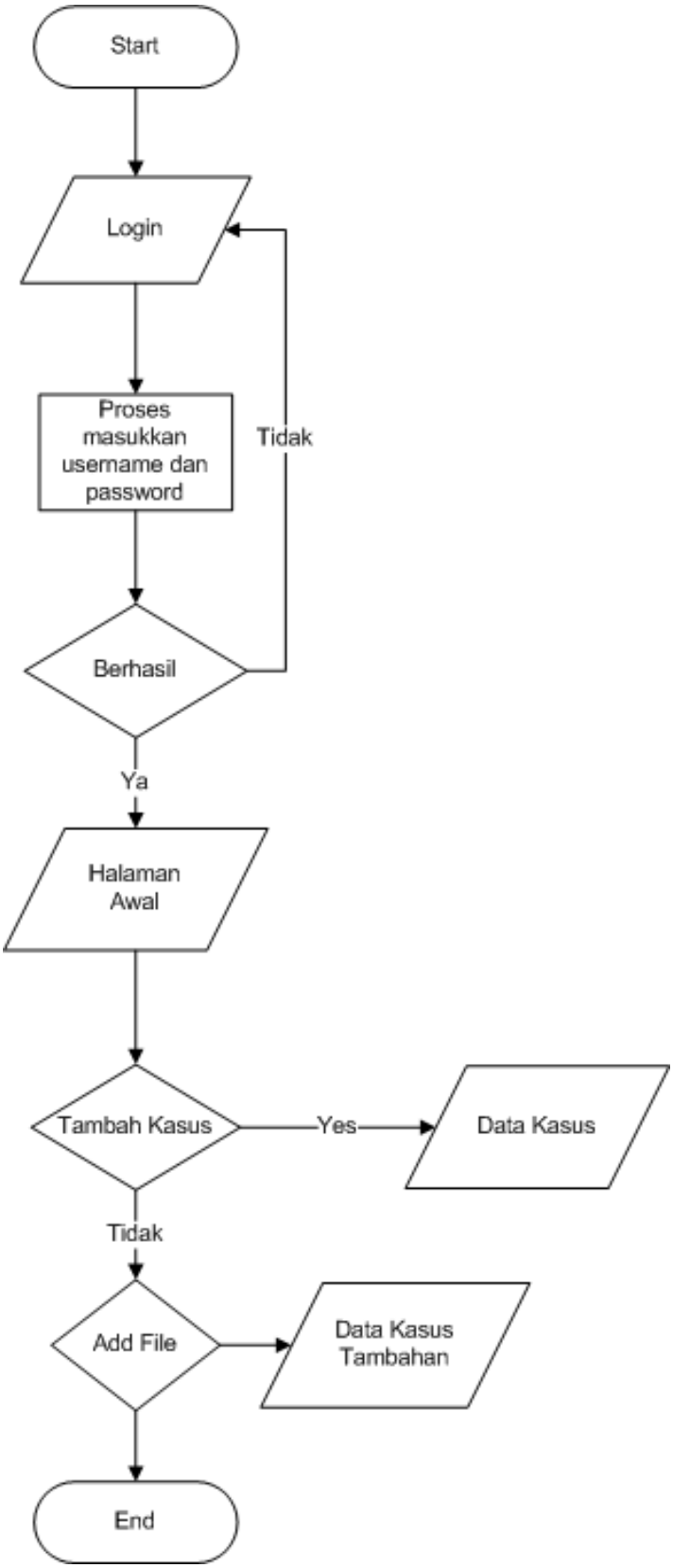


Gambar 3.9 Halaman *Add File*

3.5 Pengujian Sistem

Pada tahapan ini dilakukan pengujian sistem manajemen bukti digital yang bertujuan untuk mendeteksi keberhasilan dan kegagalan dari sistem ini agar dapat diperbaiki terlebih dahulu. Pengujian sistem ini merupakan suatu investigasi yang dilakukan untuk mendapatkan informasi mengenai kualitas dari sistem yang sedang diuji.

Dalam konsep pengembangan manajemen bukti digital ini membutuhkan sebuah *flowchart* untuk model interaksinya. *Flowchart* adalah suatu bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara detail dan hubungan antara suatu proses dengan proses lainnya dalam suatu program. *Flowchart* yang ada pada sistem ini menggambarkan adanya suatu proses permulaan yang akan mengarah pada proses *login* dimana proses *login* ini memasukkan *username* dan *password* sebagai proses awal untuk masuk kedalam sistem. Setelah proses *login* aliran program akan mengarah pada proses pengolahan data *login*, jika *username* dan *password* yang dimasukkan sudah benar maka alur selanjutnya akan mengarah pada pilihan berhasil atau tidak masuk kedalam sistem, jika *username* dan *password* yang dimasukkan tidak sesuai maka akan kembali pada proses awal, dan jika *username* dan *password* yang dimasukkan sudah sesuai maka alur selanjutnya akan mengarah pada informasi halaman awal. Halaman awal akan mengarah ke proses memberikan pilihan ke halaman tambah kasus jika akan menambah kasus maka alur selanjutnya mengarah pada proses memasukkan tambah data kasus, jika tidak alur akan mengarahkan pada proses *add file* dan alur akan mengarah pada proses data kasus tambahan yang tersedia pada sistem yang. Alur dari *flowchart* akan digambarkan seperti gambar 3.10 di bawah ini



Gambar 3.10 *Flowchart*

Penjelasan alur dalam *flowchart* pada gambar 3.10 adalah sebagai berikut:

Pada alur yang pertama pada sistem dimulai dengan *login*, dimana *login* ini mengharuskan investigator untuk memasukkan *password* dan *username* dimana jika *password* dan *username* yang dimasukkan sudah benar maka sistem akan memproses masuk ke dalam halaman awal sistem, jika investigator memasukkan *username* dan *password* yang salah maka sistem tidak akan memprosesnya.

Setelah investigator berhasil masuk kedalam sistem, maka sistem akan menampilkan halaman awal. Dalam sistem ini selain halaman awal, ada halaman tambah kasus, dan halaman *add file.*

Pada halaman tambah kasus invetigator akan memasukkan nama kasus yang sedang ditanganinya. Tambah kasus ini harus diisi dengan nama kasus yang sedang ditangani investigator. Karena kasus ini nantinya akan dipilih pada saat *add file*. Jika telah mengisi tambah kasus maka halaman akan masuk kedalam data kasus, jika investigator tidak akan menambah kasus lagi maka bisa langsung ke halaman *add file*.

Dalam halaman tambah kasus jika investigator tidak ingin menambah kasus bisa langsung ke halaman *add file*, dimana dalam halaman *add file* hal yang paling utama adalah mengunggah file dd dan file XML, investigator juga harus mengisi informasi data-data tentang kasus yang sedang ditanganinya. Dalam data kasus terdapat beberapa form yag telah ada pada sistem, diantaranya adalah nama investigator yang menangani kasus tersebut, barang bukti yang ditemukan, merk barang bukti yang ditemukan, dan informasi tentang barang bukti yang ditemukan. Jika semua data yang ada pada sistem telah selesai dimasukkan maka investigator bisa keluar dari sistem dengan cara *logout* dari sistem tersebut.

BAB 4
Hasil dan Pembahasan

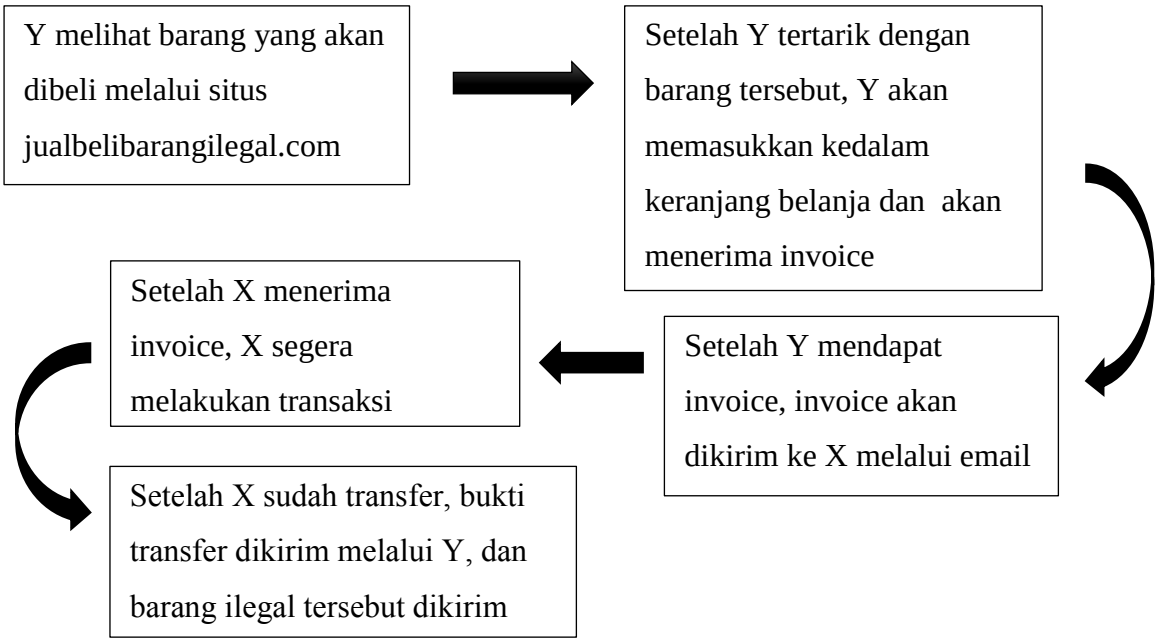
Bab ini akan membahas tentang jawaban dari rumusan masalah yang telah dilakukan dalam pengujian pengembangan *output* DFXML untuk manajemen bukti digital. Berdasarkan hasil pengujiannya sistem tersebut berjalan sesuai dengan rancangan. Rancangan sistem tersebut akan mendapatkan sebuah hasil implementasi dari sistem manajemen bukti digital.

4.1 Skenario Kasus

X dan Y adalah penjual barang ilegal yang berupa *handphone*, *laptop* dan barang elektonik yang lainnya. Barang yang dijual, mereka dapatkan dari luar negeri. Dengan adanya teknologi mereka memanfaatkannya untuk membeli barang ilegal dan menjualnya kembali di Batam.

Pada hari Senin 5 Juni 2016 si X mendapatkan email dari Y berisi *invoice* transaksi dari Y membeli barang-barang ilegal tersebut. Dengan teknologi yang semakin canggih dan mudah digunakan membuat X dan Y mudah bertransaksi lewat jaringan internet maupun media sosial.

Berikut alur transaksi Y untuk mendapatkan barang ilegal tersebut



Tabel 4.1 Tabel Barang Bukti

No	Jenis Kasus	Tanggal Kejadian	Lokasi	Jenis Barang Bukti	
				Bukti Elektronik	Bukti Digital
1	Jual beli barang ilegal	5 Juni 2016	Rumah Ilegal Jl.Jalak No 23	Handphone X	Evidence01.dd
				Handphone Y	Evidence02.dd
				Laptop	Evidence03.dd

4.2 Masalah Manajemen Bukti Digital

Selama ini sistem yang sudah ada dalam penanganan *output* DFXML menyulitkan investigator karena harus membuka bukti digital satu persatu. Sehingga perlu dibuat suatu mekanisme lain untuk menangani *output* hasil DFXML. Perlu beberapa langkah yang diperlukan untuk mempermudah investigator dalam pengelolaan hasil bukti digital dan pembacaan metadata dari bukti digital hasil akuisisi.

Langkah pertama yang harus dilakukan, mengakuisisi bukti elektronik menggunakan dc3dd *tool imager* dengan sistem operasi Linux. Dc3dd *tool imager* adalah salah satu *tools* untuk mengakuisisi bukti elektronik yang ada pada sistem Kali Linux. Bukti elektronik yang akan diakuisisi berupa *flashdisk*. Bukti elektronik yang dapat diakuisisi tidak hanya *flashdisk*, dapat berupa *harddisk*, telepon genggam dan laptop. Hasil akuisisi menggunakan dc3dd *tool imager* berupa file dd. Gambar dapat dilihat pada gambar 4.1 di bawah ini

Gambar 4.1 Langkah 1

Tahapan akuisisi bukti elektronik menggunakan dc3dd

1. Siapkan bukti elektronik yang ditemukan (*flashdisk*)
2. Buka kali linux, lalu tancapkan bukti elektronik tersebut. Kemudian mulai akuisisi bukti elektronik tersebut.
3. Setelah selesai akuisisi bukti elektronik, hasilnya akan berupa file bukti digital.

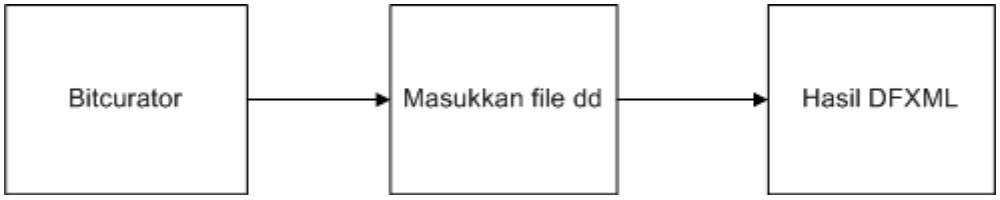
Hasil dari akuisisi bukti elektronik *flashdisk* dengan dc3dd akan menghasilkan seperti gambar 4.2 di bawah ini

```
root@kalilinux:~# dc3dd if=/dev/sdb1 of=/home/putry/evidence01.dd hash=md5

dc3dd 7.2.641 started at 2016-12-10 11:32:21 +0700
compiled options:
command line: dc3dd if=/dev/sdb1 of=/home/putry/evidence01.dd hash=md5
device size: 2240512 sectors (probed),    1,147,142,144 bytes
sector size: 512 bytes (probed)
  1147142144 bytes ( 1.1 G ) copied ( 100% ),   15 s, 71 M/s

input results for device `/dev/sdb1':
   2240512 sectors in
   0 bad sectors replaced by zeros
   ec2a9dc49a4247737932292b30ce63e5 (md5)

output results for file `/home/putry/evidence01.dd':
   2240512 sectors out

dc3dd completed at 2016-12-10 11:32:37 +0700
```

Gambar 4.2 Hasil Akuisisi dc3dd

Dalam hasil akuisisi dengan menggunakan dc3dd *tool imager* mendapatkan hasil MD5ec2a9dc49a4247737932292b30ce63e5. Dalam gambar diatas perintah dc3dd diketikan pada terminal, diikuti dengan if=/dev/sdb1 yang merupakan *flashdisk* yang akan diakuisisi, kemudian of=/home/putry/evidence01.dd adalah tempat direktori mana yang akan menampung hasil akuisisi tersebut, lalu /evidence01.dd adalah nama file hasil akuisisi, selanjutnya hash=md5 adalah jenis *hash* yang digunakan adalah MD5.

Langkah kedua adalah mengakuisisi bukti digital hasil dari dc3dd menggunakan aplikasi *bitcurator* seperti gambar 4.3 di bawah ini

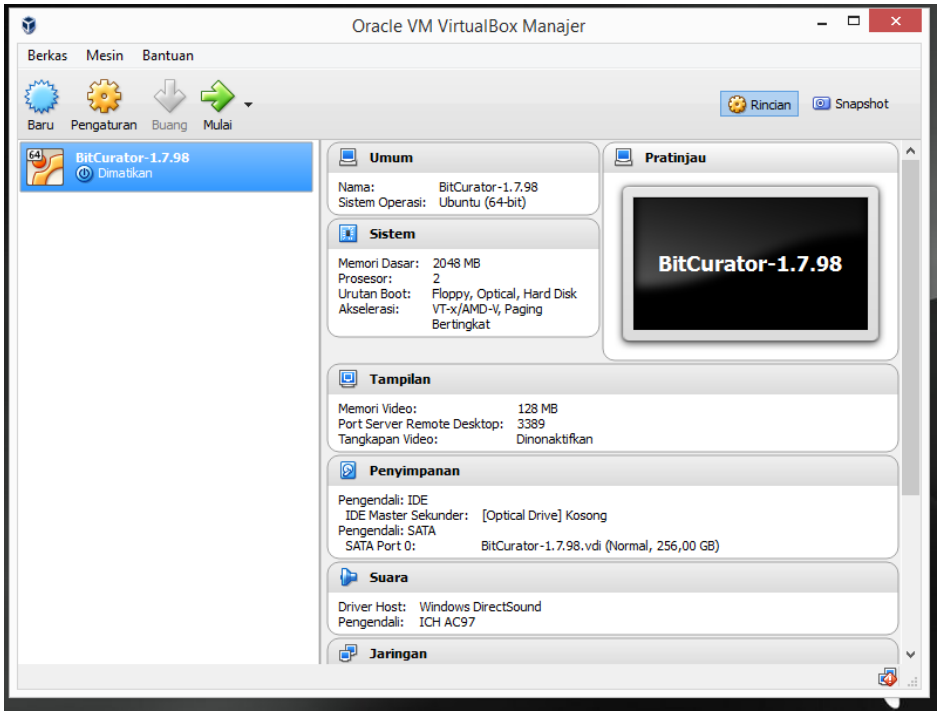


Gambar 4.3 Langkah 2

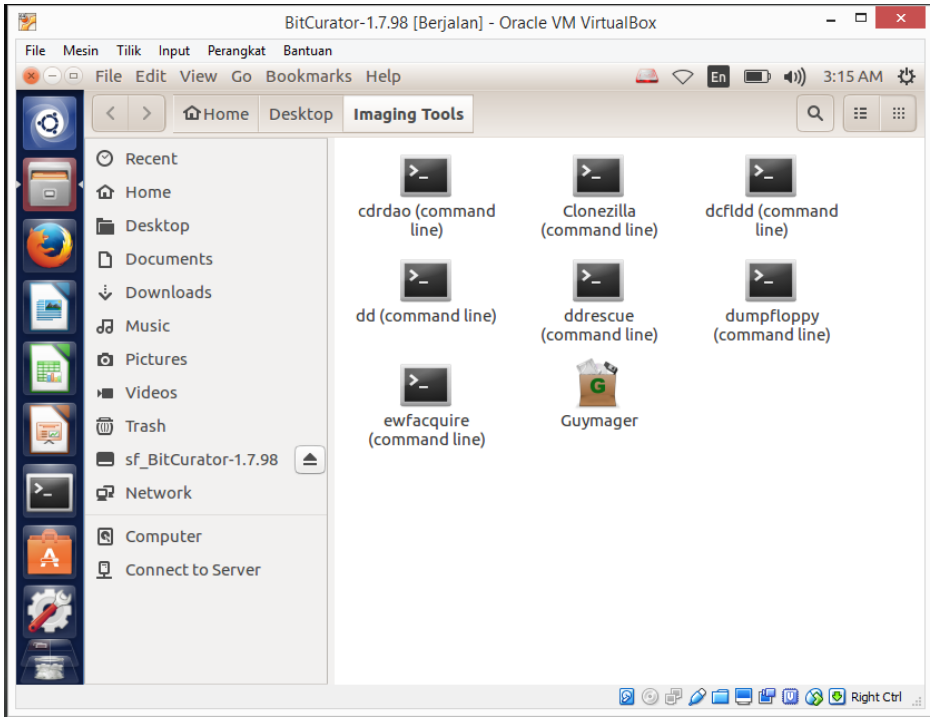
Langkah selanjutnya adalah menakuisisi bukti digital menggunakan *bitcurator*.

1. Siapkan *Oracle* VM *VirtualBox*, kemudian nyalakan aplikasi *bitcurator*.
2. Masukkan file dd dari hasil bukti digital ke aplikasi *bitcurator*, lalu mulai akuisisi.
3. Buka folder *imaging tools* dan pilih *guymager*.
4. Pada *guymager* pilih file bukti digital yang akan di akuisisi.
5. Selanjutnya *Acquire Image* pada file bukti digital.
6. Beri nama file bukti digital.
7. File bukti digital berhasil diakuisisi.
8. Hasil bukti digital dari DFXML adalah file dd dan file xml yang ada dalam sebuah folder bersama hasil file yang lainnya.

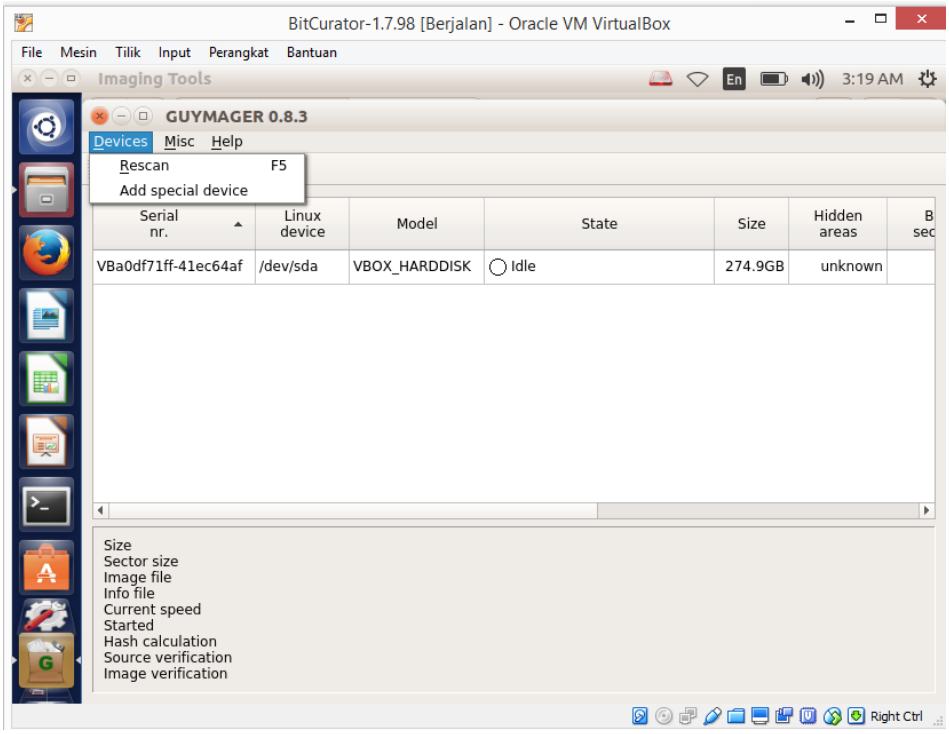
Pada tahap ini, file dd hasil akuisisi dari dc3dd *tool imager* akan diproses untuk menghasilkan *output* DFXML. Berikut proses menggunakan *bitcurator* dapat dilihat pada gambar 4.4 sampai 4.10 gambar di bawah ini



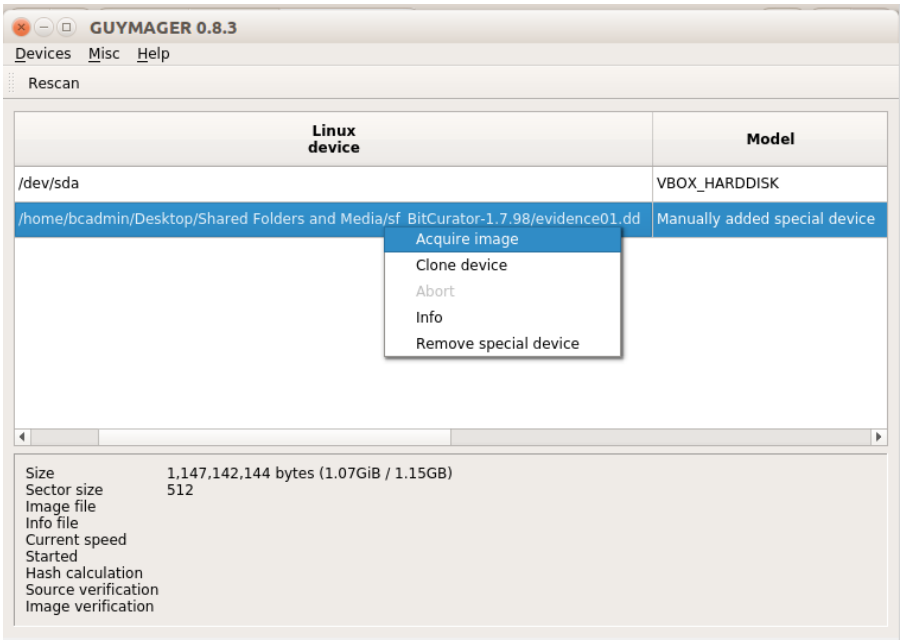
Gambar 4.4 Halaman Awal VM *VirtualBox*



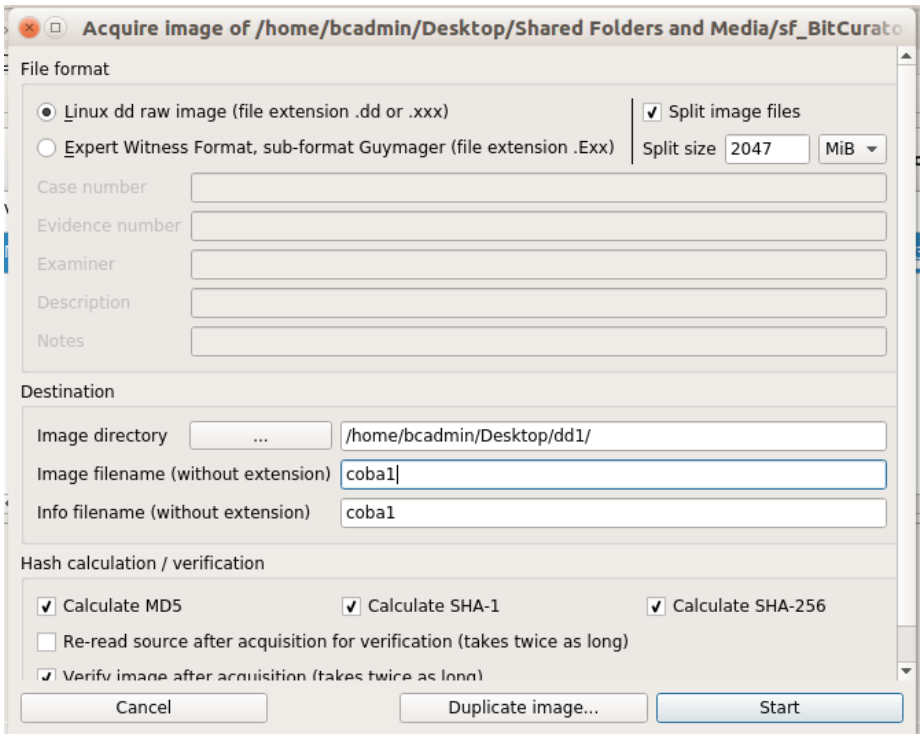
Gambar 4.5 Halaman *Imaging Tools*



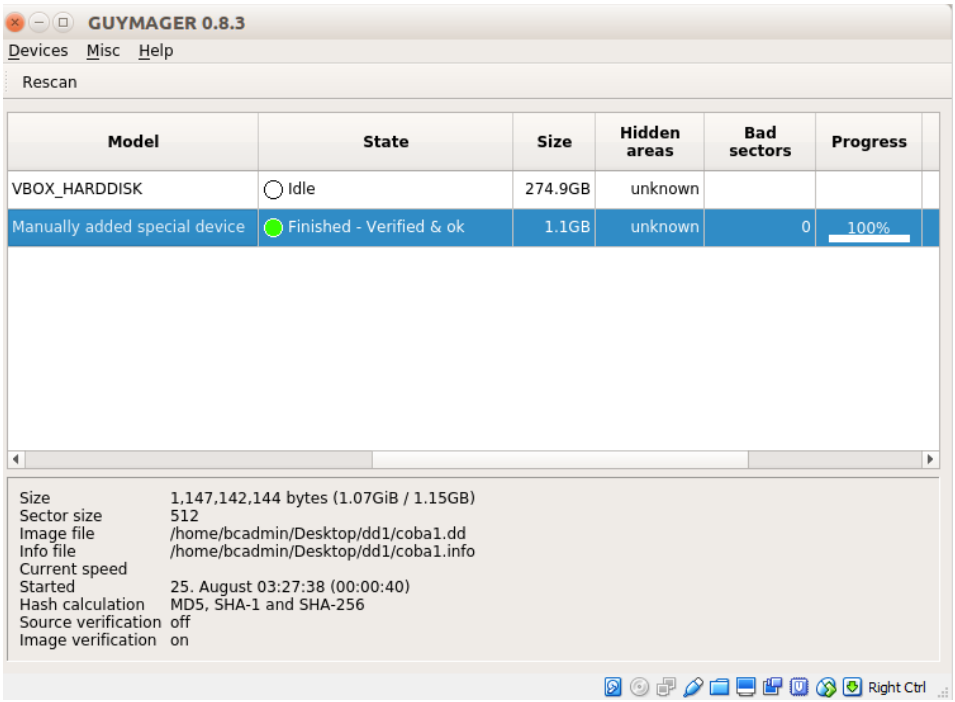
Gambar 4.6 Pilih File Bukti Digital



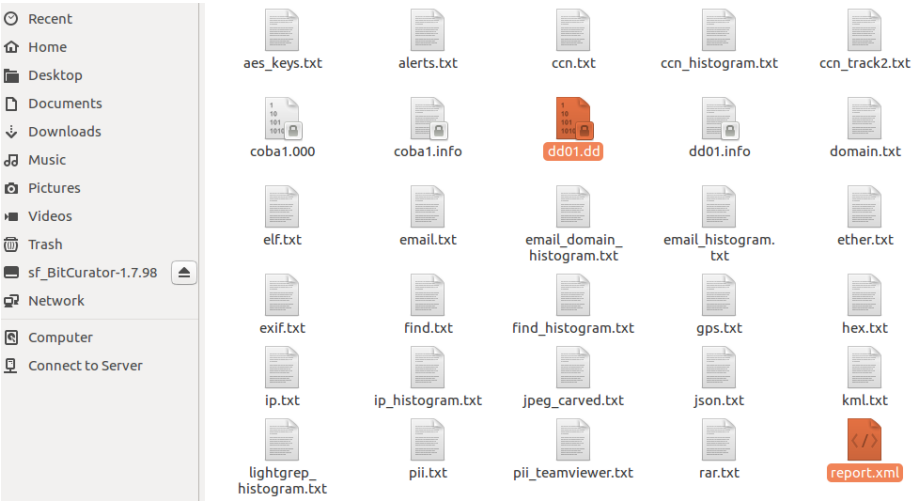
Gambar 4.7 Mulai Akuisisi Bukti Digital



Gambar 4.8 Nama File Bukti Digital



Gambar 4.9 Sukses Akuisisi

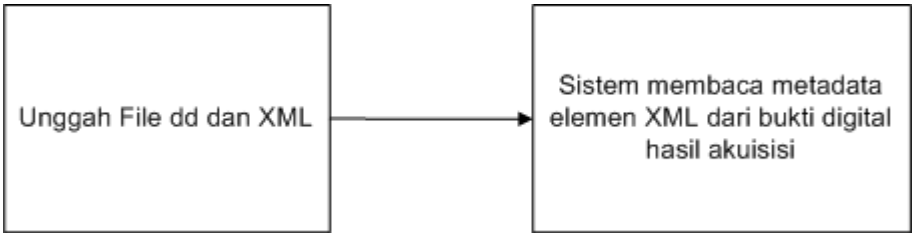


Gambar 4.10 *Output* DFXML

Pada masalah ini belum ada sistem yang mampu menangani masalah hasil akuisisi DFXML untuk dikelola secara bersama-sama. Pada gambar di bawah akan memberikan penjelasan, tanpa sistem yang dibangun file hasil akuisisi DFXML akan menghasilkan file dd dan XML dalam satu folder dan akan berulang setiap ada file hasil akuisisi DFXML yang baru, jika ada 10 atau lebih file akuisisi DFXML juga akan menghasilkan 10 atau lebih folder akuisisi DFXML.

Dalam sistem yang akan dibuat ini proses yang pertama kali harus dilakukan adalah menguraikan dengan cara mengakuisisi satu persatu bukti elektronik menjadi bukti digital dengan aplikasi DFXML yang akan menghasilkan file dengan ekstensi dd dan file dengan ekstensi XML. Hasil DFXML yang berupa file dengan ekstensi XML akan menghasilkan elemen-elemen. Dari elemen-elemen ini terdapat elemen yang dibutuhkan oleh investigator diantaranya adalah MD5 dari sebuah bukti digital yang telah diakuisisi. Bukti digital yang diakuisisi akan menghasilkan elemen-elemen yang berbeda-beda.

Langkah berikutnya adalah mengunggah file dd dan file XML kedalam sistem yang telah dibangun. Seperti gambar 4.11 di bawah ini



Gambar 4.11 Langkah ke 3

Langkah ketiga ini adalah mengunggah hasil *output* DFXML. File yang di unggah ada 2 file, yaitu file dd dan file XML, selain kedua file tersebut tidak dapat diunggah.

Setelah berhasil mengunggah dan mengisi semua data pada sistem, maka sistem akan menampilkan file yang telah di isi dan akan membaca file xml yang diambil beberapa elemen xml yang penting dalam bentuk *pop-up*

Hasil dari akuisisi bukti digital dengan menggunakan *bitcurator* seperti gambar di bawah ini. Sebagian dari elemen XML yang ada pada gambar di bawah ini akan di baca oleh sistem yang di bangun. Seperti gambar 4.12 di bawah ini


```
-<source>
   <image_filename>/home/bcadmin/Desktop/dd1/dd01.dd</image_filename>
   <image_size>1147142144</image_size>
   <hashdigest type="MD5">ec2a9dc49a4247737932292b30ce63e5</hashdigest>
 </source>
-<feature_files>
  -<feature_file>
```


Gambar 4.12 *Report* XML

Script coding yang berhubungan dengan aktivitas dalam sistem ini salah satunya pada *coding* untuk pembacaan XML. Dalam pembacaan XML yang akan keluar dalam sistem diperlukan *Tools Sublime Text* 2. *Sublime Text* adalah aplikasi *editor* untuk kode dan teks yang dapat berjalan diberbagai *platform operating system* dengan menggunakan teknologi *Phyton* API. *Sublime Text* mendukung berbagai bahasa pemrograman dan mampu menyajikan fitur *syntax highlight* hampir di semua bahasa pemrograman yang didukung ataupun dikembangkan. Untuk lebih jelasnya dapat dilihat pada gambar 4.13 di bawah ini

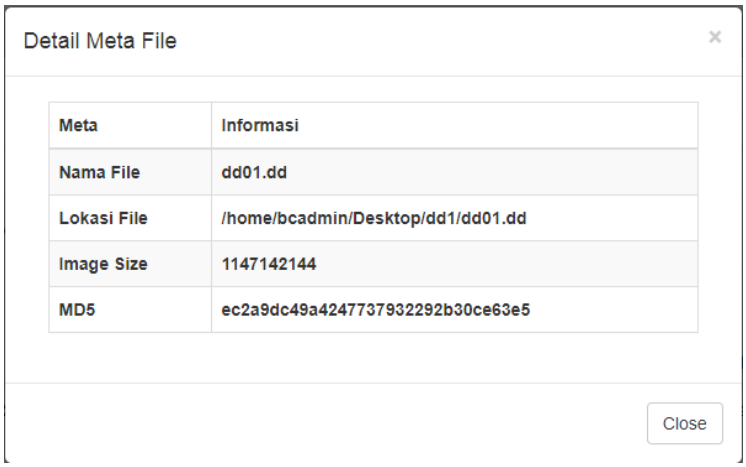
```
1   <?php
2   if (isset($_REQUEST['id'])) {
3       $file_xml = $_REQUEST['id'];
4       $doc = new DOMDocument();
5          $doc->load('../files/xml/'.$file_xml);
6
7          echo ("<table class='table table-bordered jambo_table' >");
8          echo ("<thead><tr class='headings'><th>Meta</th><th>Informasi</th></tr></thead>");
9
10          $df = $doc->getElementsByTagName("source");
11         foreach($df as $bd)
12         {
13          $ifile = $bd->getElementsByTagName("image_filename");
14          $ifile_name = $ifile->item(0)->nodeValue;
15          $test = explode("/", $ifile_name);
16          $ifile = $bd->getElementsByTagName("image_filename");
17          $ifile_name = $ifile->item(0)->nodeValue;
18          $isize = $bd->getElementsByTagName("image_size");
19          $isizeFile = $isize->item(0)->nodeValue;
20          $md5 = $bd->getElementsByTagName("hashdigest");
21          $md5Text = $md5->item(0)->nodeValue;
22
23          echo ("<tbody><tr><th>Nama File</th><th>$test[5]</th></tr>
24             <tr><th>Lokasi File</th><th>$ifile_name</th></tr>
25             <tr><th>Image Size</th><th>$isizeFile</th></tr>
26             <tr><th>MD5</th><th>$md5Text</th></tr></tbody>");
27         }
28         echo ("</table>");
29     }
30  ?>
```

Gambar 4.13 *Script Coding* Pembacaan XML

Script coding ini hanya mengidentifikasi beberapa file dari hasil XML, beberapa diantaranya adalah: nama file, lokasi file, *image size* dan yang paling penting adalah MD5. MD5 akan memberikan perbedaan pada setiap bukti digital yang telah diakuisisi.

Pada baris ke 1 menjelaskan tentang bahasa pemrograman yang dipakai untuk membangun sistem. Sistem di bangun menggunakan bahasa pemrograman PHP. Pada baris ke 2 sampai baris ke 3 menjelaskan tentang data yang diminta dalam *database* jika masuk kedalam sistem adalah id, karena dengan id dapat membedakan file satu dengan yang lain (unik). Pada baris ke 4 adalah membaca sebuah dokumen. DOM (*Document Object Model*) adalah *object* model standar untuk HTML dan XML yang bersifat *platform independent*. Fungsi DOM salah satunya adalah untuk mencari sebuah *tag* HTML berdasarkan id. Dalam kasus ini DOM berfungsi sebagai pemanggil id dari file XML. Pada baris ke 5 berdasarkan id yang ada dalam *database,* sistem akan membaca nama file XML yang di ambil dari database. Pada baris ke 10 sampai baris ke 18 untuk membaca file yang dipanggil dengan menggunakan elemen XML yang dipanggil di antaranya adalah *image_filename, image_size* dan *hashdigest.* Pada baris ke 20 sampai baris ke 24 untuk menampilkan *elemen* XML ke dalam sistem dengan memunculkan nilai dari *elemen* XML.

Gambar di bawah ini adalah pembacaan elemen XML hasil akuisisi bukti digital. Elemen XML yang dibaca oleh sistem hanya diambil beberapa bagian saja tidak semua elemen XML akan dibaca oleh sistem yang dibangun. Elemen XML yang dapat dibaca ada 4 elemen, diantaranya adalah nama file yang ada pada gambar diatas menunjukan nama file dd01.dd. Selanjutnya lokasi file terdapat pada /home/bcadmin/Desktop/dd1/dd01.dd. Elemen XML berikutnya adalah *image size*, dimana ukuran file juga dapat dibaca oleh sistem, ukuran file pada dd01 adalah 1147142144. Elemen XML yang terakhir yang dapat dibaca oleh sistem adalah MD5 dari file dd01.dd, dimana MD5 dalam sebuah hasil akuisisi bukti digital berupa angka dan nomor, MD5 dari bukti digital dd01.dd adalah ec2a9dc49a4247737932292b30ce63e5. Gambar untuk baca metadata dapat di lihat pada gambar 4.14 di bawah ini



Gambar 4.14 Baca Metadata

4.3 Membangun Sistem Untuk Manajemen Bukti Digital

Membangun sebuah sistem diperlukan beberapa tahapan, tahap pertama adalah membuat sebuah rancangan untuk membangunnya. Konsep ini terinspirasi dari sulitnya untuk pembacaan metadata yang dihasilkan dari *output* DFXML. Bukti elektronik akan diproses pada *tools* DFXML menjadi file dengan format dd dan menghasilkan *report* dengan format XML. Maka perlu dibangun sebuah sistem untuk mempermudah dalam pengelolaan manajemen bukti digital dan pembacaan metadatanya.

Perancangan sistem untuk pembacaan XML memerlukan *tools* yang bernama *bitcurator* untuk menghasilkan file dengan format XML. *Bitcurator* mempunyai kelebihan dibandingkan dengan aplikasi yang lain, hasil file XML dari *bitcurator* dapat dibaca oleh berbagai jenis *platform* (dapat dibuka pada sistem operasi *windows*, *mac* maupun *linux*).

Perancangan sistem ini dibuat berdasarkan (Garfinkel, 2011) DFXML meningkatkan komposisi dengan menyediakan bahasa untuk menggambarkan proses forensik umum misalnya, *kriptografi hashing*, lokasi file, nama file dan waktu pembuatan maupun waktu perubahan data yang ada pada file.

Sistem yang akan dibuat menggunakan XAMPP PHP yang mendukung sistem berbasis *website* yang mempunyai beberapa keunggulan diantaranya adalah mudah digunakan, dapat digunakan dalam berbagai macam sistem operasi apapun (*multi platform*). Kekurangan pada sistem berbasis *website* diantaranya *web server* yang harus di aktifkan terlebih dahulu (jika aplikasi *offline*).

Proses yang dilakukan sebelumnya adalah proses akuisisi. Proses akuisisi adalah proses tahap pertama yang dilakukan dalam pengujian ini. Proses pengujian menggunakan dc3dd *tool imager*. Proses ini sangat penting dalam tahapan analisis forensik karena

tahapan ini adalah proses penggandaan yang hasilnya sama. Tujuan *imaging* ini adalah untuk menjaga keutuhan barang bukti tersebut. Setelah selesai proses *imaging* baru dilakukan proses *output* DFXML. Berikut adalah diagram *output* DFXML yang dapat dilihat pada gambar 4.15 di bawah ini.

Gambar 4.15 *Output* DFXML

Bitcurator adalah salah satu turunan dari Linux Ubuntu, *bitcurator* mengembangkan *software* untuk mengekstrak, menganalisis dan menghasilkan laporan dari sebuah bukti digital. *Bitcurator* termasuk rangkaian digital *open source* forensik dan alat analisis data untuk membantu mengumpulkan institusi proses digital. *Bitcurator* didistribusikan sebagai VM yang bisa jalankan di *VirtualBox*, dan sebagai *Live* ISO yang bisa digunakan untuk menginstal *bitcurator* pada mesin khusus.

Sistem yang dibangun terdiri atas dua data, yaitu data statis dan data dinamis. Data statis pada penelitian ini diartikan sebagai data yang asli dari hasil bukti digital dan tidak dapat dirubah, seperti hal nya file dd, file XML, dan tanggal unggah kedua file kedalam sistem yang dibangun. Sedangkan data dinamis diartikan sebagai data tambahan untuk kebutuhan informasi yang belum ada pada data statis dan dapat dirubah, data dinamis terdiri dari keterangan kasus yang sedang ditangani, nama investigator yang sedang menangani kasus, informasi barang bukti elektronik dan merk barang bukti yang ditemukan pada saat ditempat kejadian perkara. File bukti digital yang pernah diunggah dapat dihapus.

Pada gambar 4.16 menjelaskan elemen XML untuk mengetahui sistem operasi yang digunakan dan mengetahui posisi bukti digital berada dimana. Dalam elemen XML tertulis sistem operasi yang digunakan adalah Linux. Dan bukti digital ada di posisi home/bcadmin/Desktop/dd1/dd01.dd. Gambar dapat dilihat seperti gambar 4.16 di bawah ini.

```
25    <execution_environment>
26      <os_sysname>Linux</os_sysname>
27      <os_release>4.4.0-57-generic</os_release>
28      <os_version>#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016</os_version>
29      <host>ubuntu</host>
30      <arch>x86_64</arch>
31      <command_line>bulk_extractor -o /home/bcadmin/Desktop/dd1 /home/bcadmin/Desktop/dd1/dd01.dd</command_line>
32      <uid>1000</uid>
33      <username>bcadmin</username>
34      <start_time>2017-04-06T10:26:11Z</start_time>
35    </execution_environment>
```

Gambar 4.16 Elemen XML Sistem Operasi

Pada gambar 4.17 menjelaskan tag XML untuk mengetahui nama file, ukuran file, dan MD5 file dd. Nama file pada elemen XML adalah dd01.dd, ukuran file 1GB lebih dan MD5 ec2a9dc49a4247737932292b30ce63e5. Gambar dapat dilihat seperti gambar 4.17 di bawah ini.

```
218   <source>
219     <image_filename>/home/bcadmin/Desktop/dd1/dd01.dd</image_filename>
220     <image_size>1147142144</image_size>
221     <hashdigest type='MD5'>ec2a9dc49a4247737932292b30ce63e5</hashdigest>
222   </source>
223   <feature_files>
```

Gambar 4.17 Elemen XML Metadata File

4.4 Kinerja Sistem

Sistem yang telah dibangun ini hanya dapat membaca file dd saja. File dd digunakan sebagai uji coba, karena file dd adalah file dari bukti digital yang sering terjadi didalam dunia forensik digital.

Disk Image atau sering disebut *imaging* dalam dunia digital forensik adalah suatu proses dari file tunggal atau suatu perangkat media penyimpanan seperti *flashdisk*, *harddisk* dan lain-lain yang mengandung isi lengkap dengan strukturnya yang kemudian diperbanyak atau penggandaan dengan isi dan struktur yang sama dengan yang asli tanpa selisih ukuran se-bit pun di dalamnya. Mudahnya *disk image* itu proses memetakan penggandaan barang bukti dengan metode *bit by bit copy*.

Sistem yang dibangun ini hanya dapat mengunggah hasil *output* DFXML, yaitu file dd dan file XML. Sistem akan menolak jika bukan file dd dan file XML yang diunggah kedalam sistem yang dibangun.

Penanganan untuk file bukti digital yang berekstensi dd mempunyai ukuran file yang berbeda-beda dari file yang kecil sampai yang terbesar, tetapi dalam penelitian ini menggunakan file berukuran 1GB sampai dengan 1,2GB. Kedua file dd yang berbeda-beda ternyata berpengaruh dalam waktu unggah file dd tersebut kedalam sistem.

Ukuran file bukti elektronik yang ada dalam kasus *cybercrime* tidak mungkin kecil, bisa melebihi dari 1GB, tetapi ukuran file yang di uji coba pada sistem ini hanya file berkapasitas 1GB sampai dengan 1,2GB dengan membutuhkan waktu unggah kurang lebih 1menit hingga 3menit. Ukuran file yang diunggah sangat mempengaruhi waktu unggah.

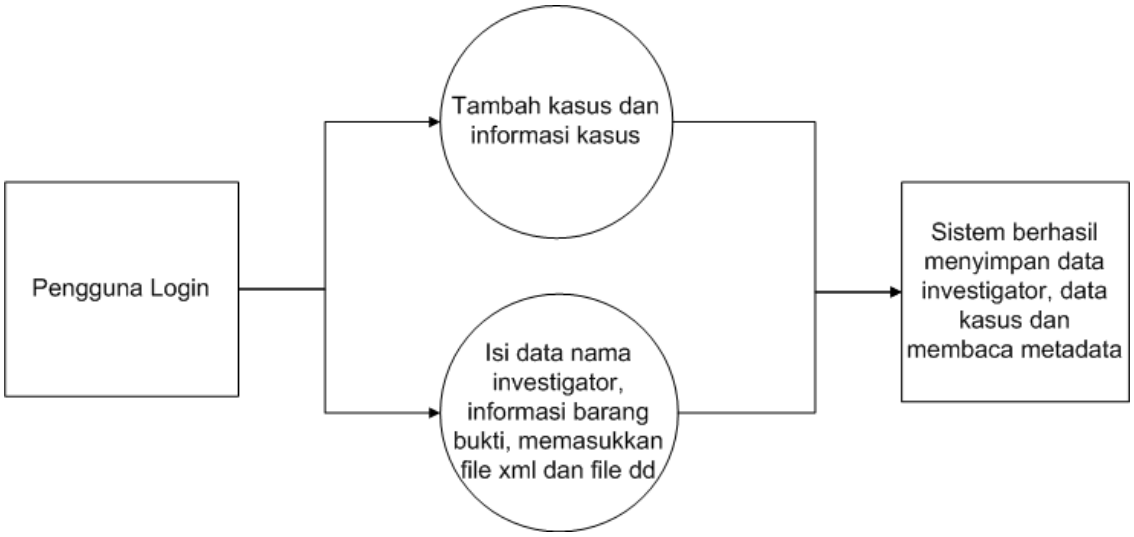
Kinerja pada sistem selain waktu unggah untuk file dd dan file xml, sistem dapat memberikan data-data selain file dd dan file xml, yaitu keterangan kasus yang sedang ditangani, nama investigator yang sedang menangani kasus tersebut, barang bukti elektronik yang ditemukan dan merk barang bukti yang ditemukan.

Kemudahan yang ada pada sistem ini adalah, kemudahan dalam mengelola hasil *output* DFXML menjadi satu folder dan mudah dalam pembacaan metadata hasil akuisisi bukti digital. Dalam pembuatan sistem, terdapat keterbatasan-keterbatasan juga diantaranya adalah file dd yang ada hanya file dengan kapasitas kecil (1GB-1,2GB). Tidak dapat membaca file bukti digital selain file dd dan file XML.

4.5 Solusi Masalah Manajemen Bukti Digital

Pada gambar 4.18 terdapat sebuah gambar skenario pengujian, dimana langkah pertama pengguna akan melakukan proses *login* terlebih dahulu. Proses ini akan memasukkan *username* dan *password* setelah berhasil akan masuk kedalam halaman awal sistem ini. Langkah kedua adalah memberi nama kasus dan informasi kasus yang sedang ditanganin. Langkah ketiga adalah memasukan data nama investigator, barang bukti yang ditemukan, merk barang bukti yang ditemukan, informasi dari barang bukti dan yang terpenting adalah memasukkan file dd dan file XML. Setelah semuanya selesai di unggahmaka sistem akan menyimpan semua data yang telah dimasukkan oleh pengguna dan sistem akan mebaca metadata dari bukti digital tersebut.

Sistem ini memberikan beberapa tambahan untuk data dinamis yang berada pada sistem yang dibangun seperti nama investigator, informasi keterangan untuk kasus yang sedang ditangani, informasi tentang barang bukti yang ditangani dan merk barang bukti. Namun dalam hal penambahan data dinamis belum dapat dilakukan penambahan kedalam elemen pada hasil file XML. Berikut adalah diagram dari skenario pengujian dari sistem yang telah dibuat, gambar 4.18 dapat dilihat pada di bawah ini



Gambar 4.18 Skenario Pengujian

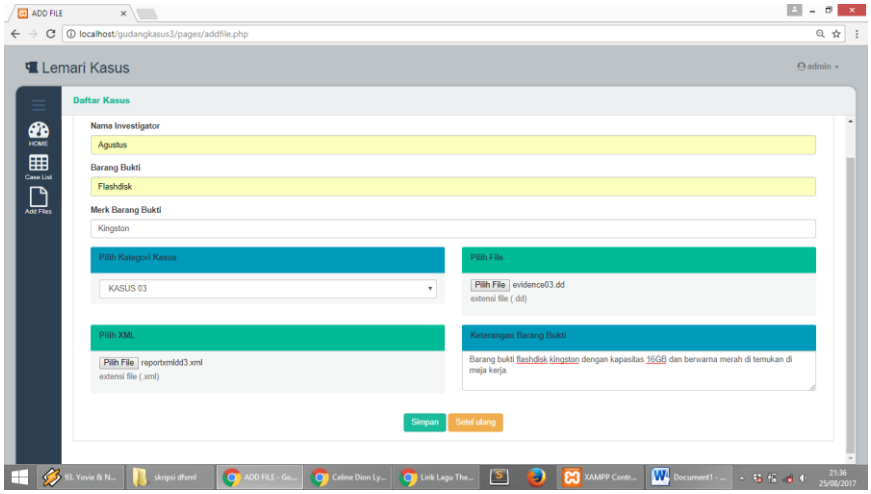
4.6 Pengujian Sistem

Setelah melakukan tahapan-tahapan yang dilakukan, langkah selanjutnya adalah melakukan pengujian terhadap sistem yang dikembangkan oleh penulis. Hasil pengujian ini merupakan sarana yang diguanakan sebagai interaksi antara manusia dan komputer atau laptop agar mudah dalam melakukan perintah-perintah terhadap sistem. Rancangan antarmuka Pengembangan *Output* DFXML Untuk Manajemen Bukti Digital.

Dalam pengujian sistem yang dibangun diperlukan XAMPP dan PHP *MyAdmin* untuk menjalankan sistem. XAMPP merupakan perangkat lunak yang mendukung untuk banyak sistem operasi, yang merupakan kompilasi dari beberapa program. Fungsi XAMPP adalah sebagai *server* yang berdiri sendiri (*localhost*), yang terdiri beberapa program antara lain: *Apache* HTTP *Server*, MySQL *database*, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP. Sedangkan PHP *MyAdmin* adalah sebuah perangkat lunak bebas yang ditulis dalam bahasa pemrograman PHP digunakan untuk menangani administrasi MySQL melalui *World Wide Web*.

4.6.1 Pengujian Sistem Unggah File

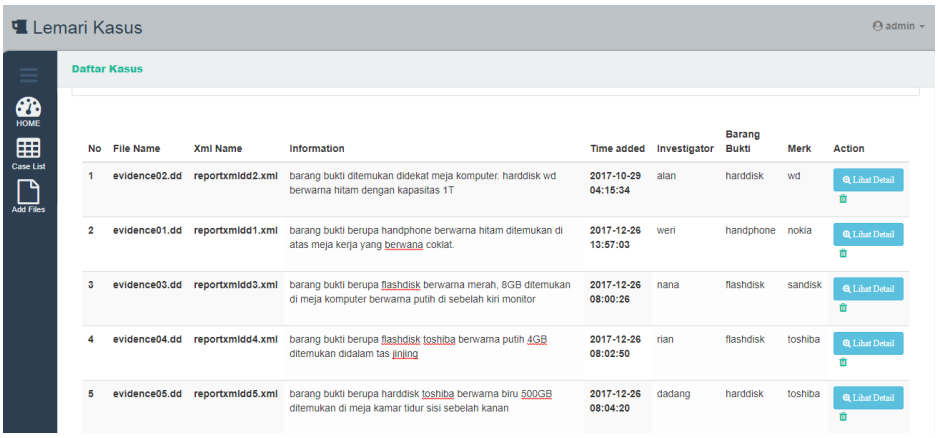
Halaman di bawah ini adalah tampilan dari halaman *add files*, dimana investigator harus melakukan *input* semua yang dibutuhkan oleh sistem. *Input* yang harus dimasukkan dapat dilihat pada gambar 4.19di bawah ini.



Gambar 4.19 Unggah File

4.6.2 Pengujian Manajemen Bukti Digital

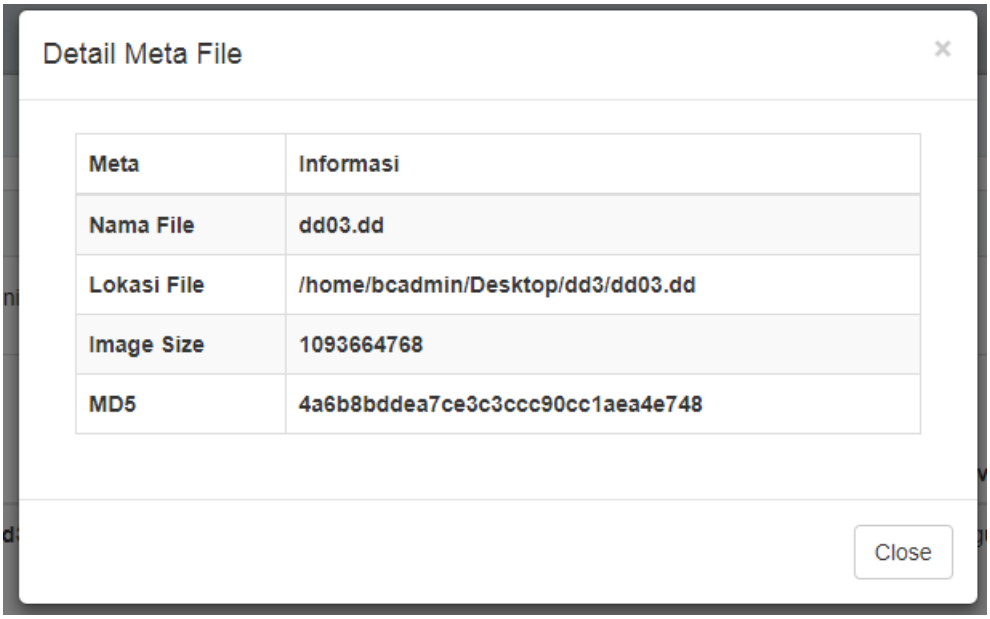
Setelah semua data masuk maka tampilan halaman tadi akan menjadi satu informsi dalam halaman daftar kasus. Untuk lebih jelas dapat dilihat pada gambar 4.20 di bawah ini.



Gambar 4.20 Manajemen Bukti Digital

4.6.3 Baca Metadata Hasil Akuisis DFXML

Setelah semua data yang dimasukkan lengkap, maka metadata akan dapat dibaca dengan memilih tombol pada bagian lihat detail. Untuk lebih jelasnya dapat dilihat pada gambar 4.21 di bawah ini.



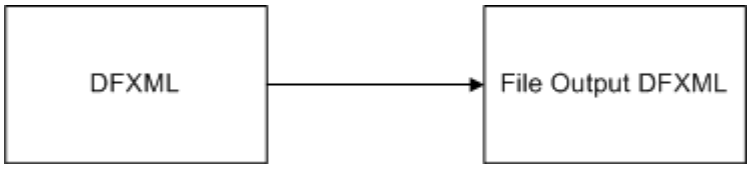
Gambar 4.21 Baca Metadata

Sistem yang dibuat ini mengharuskan investigator terlebih dahulu untuk mengakuisisi satu-persatu bukti elektronik menjadi bukti digital. Setelah itu bukti digital diakuisisi dengan aplikasi *bitcurator* dan menghasilkan file dengan ekstensi dd dan file dengan ekstensi XML. Setelah mendapat file dd dan file XML investigator masuk kedalam sistem dan mengunggah kedua file tersebut dan mengisikan beberapa data yang tertera didalam sistem yang dibuat. Investigator akan mengulang pekerjaan seperti itu setiap akan memasukkan bukti digital yang baru. Sistem ini dibuat untuk mengelola hasil DFXML dengan baik, di sistem ini hasil DFXML yang berupa file dd dan file XML dikelola

menjadi satu kesatuan bersama data dan keterangan tambahan yang tertera dalam sistem yang diisikan oleh investigator. Dalam sistem ini investigator dapat mengubah data yang telah dimasukkan kecuali file dd dan file XML, karena kedua file tersebut statis. Investigator dapat membaca hasil file yang telah diunggah, salah satunya file XML yang diambil hanya beberapa elemen terpenting. Investigator dapat menghapus file bukti digital yang telah diunggahnya.

4.7 Analisis Manajemen *Output* DFXML

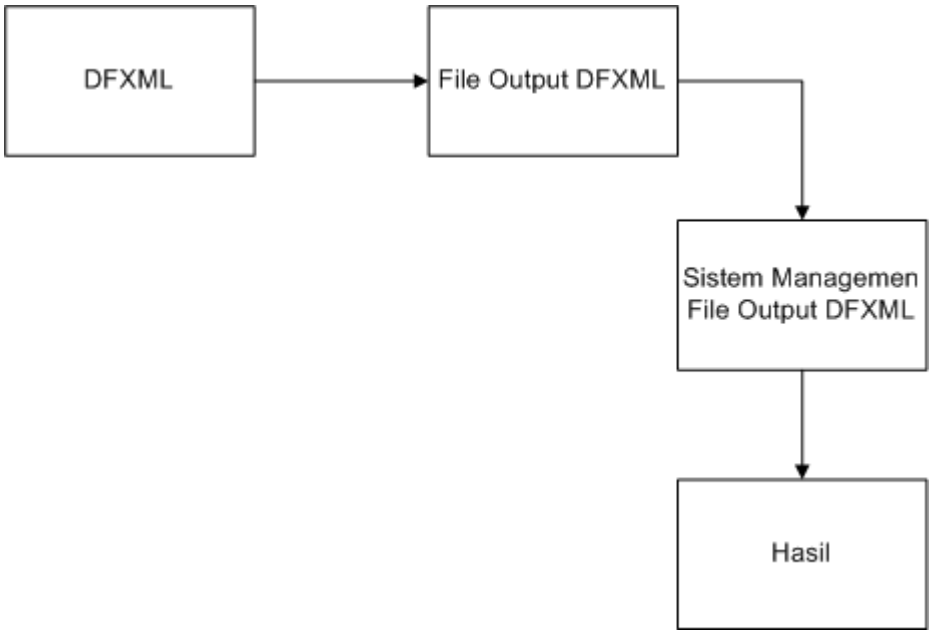
Sebelum dibangun sebuah sistem manajemen untuk *output* DFXML, dalam pengelolaan hasil *output* DFXML terdapat beberapa file dalam satu folder hasil akuisisi bukti elektronik menjadi bukti digital. Sistem sebelumnya digambarkan seperti gambar 4.22 dibawah ini



Gambar 4.22 Sebelum Sistem Dibangun

Pada gambar 4.22 digambarkan pada *tools* DFXML menghasilkan file *output* DFXML, dimana hasil *output* DFXML akan berada di dalam satu folder yang terdapat beberapa file yang dihasilkan disetiap akuisisi bukti digital, salah satunya adalah file dd dan file xml. Dimana file dd dan file xml adalah dua file yang penting diantara file-file lainnya hasil akuisisi DFXML. File dd adalah file bukti digital sedangkan file xml berisi informasi tentang bukti digital. File XML dalam hasil akuisisi bukti digital terdapat banyak elemen, salah satu elemen yang penting adalah MD5, dimana MD5 adalah nomor unik yang menjadi pembeda bukti digital satu dengan yang lainnya. Sistem yang akan dibangun juga akan memudahkan investigator dalam pembacaan file XML, dimana file XML yang terdiri banyak elemen-elemen akan dibaca bagian terpenting saja diantaranya adalah nama file, lokasi file, ukuran file dan MD5 dari bukti digital.

Banyaknya folder pada setiap hasil akuisisi bukti digital, membuat investigator merasa kesulitan dalam pengelolaan hasil *output* DFXML. Tidak hanya itu saja, elemen-elemen yang ada pada file xml juga memberikan kesulitaan kepada investigator dalam pembacaannya. Pada sistem yang dibangun juga akan ada informasi tentang sebuah kasus yang sedang ditangani investigator. Maka solusi yang diberikan adalah membuat sistem yang akan membuat investigator mudah dalam mengelola file-file dan membaca XML dari hasil *output* DFXML. Sistem yang akan dibangun, akan digambarkan seperti gambar 4.23 di bawah ini



Gambar 4.23 Sesudah Sistem Dibangun

Pada sistem yang dibangun memberikan sebuah wadah yang mampu mengelola file-file hasil *output* DFXML, sistem juga mampu membaca bagian terpenting yang diambil dari beberapa elemen XML bukti digital, dan sistem mampu memberikan informasi selain file dd dan file XML yang harus diunggah ke dalam sistem.

Perbedaan yang ada pada sistem sebelum dan sesudah dibangun adalah dimana pada sistem sebelumnya hasil akuisisi bukti digital berada dalam satu folder bersama file-file lainnya. Dalam pembacaan file xml hasil akuisisi bukti digital, file XML harus dibuka dengan *browser*, dan sistem DFXML tidak memberikan informasi tentang akuisisi bukti digital dari sebuah kasus apa yang sedang ditangani investigator. Sedangkan sistem manajemen o*utput* DFXML yang dibangun membuat file hasil akuisisi bukti digital menjadi satu folder bersama dengan beberapa informasi yang diisi investigator pada waktu mengunggah file dd dan file XML, dan sistem manajemen *output* DFXML ini dapat membaca file XML yang diambil dari beberapa elemen XML yang penting (nama file, lokasi file, ukuran file, MD5 file bukti digital).

Keuntungan dan manfaat yang didapat dalam sistem manajemen *output* DFXML ini adalah tersusun rapi file-file *output* DFXML tidak bercampur dengan file-file DFXML yang lainnya. Dapat membaca file XML tanpa menggunakan *browser*, dan file XML yang dibaca tidak banyak karena sistem hanya membaca bagian elemen XML yang terpenting. Sistem manajemen *output* DFXML juga memberikan sebuah informasi tentang kasus yang sedang ditangani investigator.

Dari hasil dalam membangun sebuah sistem untuk manajemen *output* DFXML, sistem yang dibangun mampu menyelesaikan masalah dalam pengelolaan hasil akuisisi bukti digital dan mampu melakukan pembacaan bagian terpenting dari file XML.

4.8 Struktur DFXML

Elemen XML sangatlah banyak, bisa mencapai kurang lebih 500 baris elemen, dalam struktur DFXML yang ada pada file ini mencapai 500 lebih baris elemen. Struktur DFXML ini akan menjelaskan beberapa bagian terpenting elemen-elemen XML yang ada.

Elemen tertinggi dalam elemen adalah DFXML. DFXML mempunyai banyak sub elemen, beberapa sub elemen diantaranya adalah metadata, *creator*, *execution environment*, *provided filename*, dan *source*. Beberapa sub elemen ini mempunyai banyak turunan yang disebut sebagai elemen *child*. Elemen *child* diantaranya adalah program, *version*, OS *sysname*, OS *release*, OS *version*, *command line*, *username*, *starttime*, *image filename*, *image size*, *hashdigest*.

Pada elemen DFXML terdapat atribut XML *output* version, atribut lainnya berada pada elemen *creator* dengan atribut *version*, dan yang terakhir berada pada elemen *child hashdigest* dari sub elemen *source* dimana atributnya berisi *type*.

Pada elemen DFXML terdapat atribut XMLversion=”1.0”. Elemen XML ini memberikan gambaran versi yang dipakai oleh DFXML. Elemen DFXML mempunyai sub elemen yang pertama adalah metadata. Metadata mempunyai isi dari sub elemen yaitu dc:*typeFeatureExtraction* yang memberikan sebuah informasi bahwa yang diekstraksi adalah metadata dari bukti digital.

Sub elemen selanjutnya adalah *creator*, dimana *creator* mempunyai atribut yang berupa version=”1.0”. Versi yang sama dengan atribut DFXML. Dalam sub elemen terdapat dua elemen *child* yaitu program dan *version*. Pada elemen *child* program memberikan sebuah keterangan bahwa yang digunakan untuk mengekstrak bukti digital menggunakan program *bulk extractor*, sedangkan *version* memberikan keterangan versi yang dipakai program *bulk extractor* adalah versi 1.6.0-dev.

Execution environment adalah sub elemen yang mempunyai banyak elemen *child* dibandingkan dengan sub elemen yang lainnya. Elemen *child* yang pertama adalah OS *sysname* yang memberikan sebuah informasi sistem operasi yang digunakan adalah Linux. OS *release* adalah elemen *child* yang kedua, isi dari elemen *child* ini adalah 4.4.0-57-*generic* yang memberikan informasi sistem operasi rilis versi berapa. Elemen *child* selanjutnya adalah os *version* #78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016 yang

memberikan keterangan tentang versi ubuntu yang dipakai. Elemen *child* keempat adalah *command line* yang memberikan keterangan bahwa bukti digital di ekstrak pada program *bulk extractor* dan terdapat file bukti digital dapat dibuka pada folder *home* yang berlokasi didesktop dengan nama file dd01.dd yang berisikan bulk_extractor -o /home/bcadmin/Desktop/dd1 /home/bcadmin/Desktop/dd1/dd01.dd. *Username* yang berisi bcadmin adalah elemen *child* yang kelima. Elemen *child* yang terakhir adalah *starttime* yang berisi 2017-04-06T10:26:11Z dimana elemen *child* start time ini memberikan sebuah informasi waktu yang digunakan untuk mengekstrak sebuah bukti digital.

Provided filename adalah sub elemen selanjutnya, dimana sub elemen ini memberikan keterangan lokasi file bukti digital dan nama file bukti digital isi sub elemen ini adalah /home/bcadmin/Desktop/dd1/dd01.dd.

Source adalah sub elemen yang terakhir. Sub elemen *source* ini adalah bagian terpenting dari sub-sub elemen yang lainnya. Elemen *child* dari sub elemen *source* ada tiga, /home/bcadmin/Desktop/dd1/dd01.dd adalah isi dari elemen *child* yang pertama dari *imagefilename*, elemen *child* ini memberi informasi dimana file bukti digital berada dan nama dari file bukti digital yang diekstrak. Elemen *child* yang kedua adalah *image size* yang berisi ukuran file bukti digital yang diekstrak yaitu 1147142144. Elemen *child* yang terakhir adalah elemen *child* yang paling unik dan paling penting untuk membedakan file bukti digital satu dengan yang lainnya, yaitu *hashdigest* dengan atribut *type* yang berisi angka ec2a9dc49a4247737932292b30ce63e5.

Untuk mengetahui hasil yang didapat dari kemampuan sistem yang dibangun, perlu adanya pengujian metode tersebut. Berikut adalah hasil pengujian dan analisa sistem yang diuji cobakan.

File pertama yang akan di uji coba dengan sistem ini adalah file evidence01.dd. kemudian dari hasil pengujian tersebut didapatkan hasil analisa metadatanya sebagai berikut.

Tabel 4.2 Tabel Evidence01.dd

Bukti Digital	**Jenis Metadata**	**Value**
Evidence01.dd	Program	BULK_EXTRACTOR
	Version	1.6.0-dev
	OS Sysname	Linux
	OS Release	4.4.0-57-generic

Tabel Lanjutan 4.3 Tabel Evidence01.dd

	OS Version	#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016
	Command Line	bulk_extractor -o /home/bcadmin/Desktop/dd1 /home/bcadmin/Desktop/dd1/dd01.dd
	Username	Bcadmin
	Start Time	2017-04-06T10:26:11Z
	Provided_filename	/home/bcadmin/Desktop/dd1/dd01.dd
	Image_filename	/home/bcadmin/Desktop/dd1/dd01.dd
	Image_size	1147142144
	MD5	ec2a9dc49a4247737932292b30ce63e5

File yang kedua yang akan di uji coba dengan sistem ini adalah file evidence02.dd. kemudian dari hasil pengujian tersebut didapatkan hasil analisa metadatanya sebagai berikut.

Tabel 4.4 Tabel Evidence02.dd

Bukti Digital	**Jenis Metadata**	**Value**
Evidence02.dd	Program	BULK_EXTRACTOR
	Version	1.6.0-dev
	OS Sysname	Linux
	OS Release	4.4.0-57-generic
	OS Version	#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016
	Command Line	bulk_extractor -o /home/bcadmin/Desktop/dd2 /home/bcadmin/Desktop/dd2/dd02.dd
	Username	Bcadmin
	Start Time	2017-04-06T10:35:45Z
	Provided_filename	/home/bcadmin/Desktop/dd2/dd02.dd
	Image_filename	/home/bcadmin/Desktop/dd2/dd02.dd
	Image_size	1093664768
	MD5	8c8dbeadb1c35e1f0cb265aa7d16f50e

File ketiga yang akan di uji coba dengan sistem ini adalah file evidence03.dd. kemudian dari hasil pengujian tersebut didapatkan hasil analisa metadatanya sebagai berikut.

Tabel 4.5 Tabel Evidence03.dd

Bukti Digital	**Jenis Metadata**	**Value**
Evidence03.dd	Program	BULK_EXTRACTOR
	Version	1.6.0-dev
	OS Sysname	Linux
	OS Release	4.4.0-57-generic

Tabel Lanjutan 4.6 Tabel Evidence03.dd

	OS Version	#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016
	Command Line	bulk_extractor -o /home/bcadmin/Desktop/dd3 /home/bcadmin/Desktop/dd3/dd03.dd
	Username	Bcadmin
	Start Time	2017-04-06T10:37:40Z
	Provided_filename	/home/bcadmin/Desktop/dd3/dd03.dd
	Imaage_filename	/home/bcadmin/Desktop/dd3/dd03.dd
	Image_size	1093664768
	MD5	4a6b8bddea7ce3c3ccc90cc1aea4e748

File keempat yang akan di uji coba dengan sistem ini adalah file evidence04.dd. kemudian dari hasil pengujian tersebut didapatkan hasil analisa metadatanya sebagai berikut

Tabel 4.7 Tabel Evidence04.dd

Bukti Digital	**Jenis Metadata**	**Value**
Evidence04.dd	Program	BULK_EXTRACTOR
	Version	1.6.0-dev
	OS Sysname	Linux
	OS Release	4.4.0-57-generic
	OS Version	#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016
	Command Line	bulk_extractor -o /home/bcadmin/Desktop/dd4 /home/bcadmin/Desktop/dd4/dd04.dd
	Username	Bcadmin
	Start Time	2017-04-06T10:40:00Z
	Provided_filename	/home/bcadmin/Desktop/dd4/dd04.dd
	Image_filename	/home/bcadmin/Desktop/dd4/dd04.dd
	Image_size	1093664768
	MD5	de0a9587ff931edee15f4f24c17044ee

File kelima yang akan di uji coba dengan sistem ini adalah file evidence05.dd. kemudian dari hasil pengujian tersebut didapatkan hasil analisa metadatanya sebagai berikut

Tabel 4.8 Tabel Evidence05.dd

Bukti Digital	**Jenis Metadata**	**Value**
Evidence05.dd	Program	BULK_EXTRACTOR
	Version	1.6.0-dev
	OS Sysname	Linux
	OS Release	4.4.0-57-generic
	OS Version	#78-Ubuntu SMP Fri Dec 9 23:50:32 UTC 2016
	Command Line	bulk_extractor -o /home/bcadmin/Desktop/dd5 /home/bcadmin/Desktop/dd5/dd05.dd
	Username	Bcadmin
	Start Time	2017-04-06T10:42:11Z
	Provided_filename	/home/bcadmin/Desktop/dd5/dd05.dd
	Image_filename	/home/bcadmin/Desktop/dd5/dd05.dd
	Image_size	1093664768
	MD5	28a2c859f0e649929ccc5f2d21b9ba43

Dari hasil beberapa file dd yang di uji coba, semua hasil analisa dari file dd yang sudah ditampilkan dalam tabel-tabel diatas, di dapatkan sebuah metadata file yang dibaca secara umum yang tidak terlalu spesifikan dalam pembacaaan metadatanya. Metadata yang terbaca antara lain untuk mengetahui posisi bukti digital berada di lokasi mana dan mengetahui sistem operasi yang digunakan. Penjelasan dari elemen-elemen XML seperti tabel 4.2 sampai 4.6 adalah

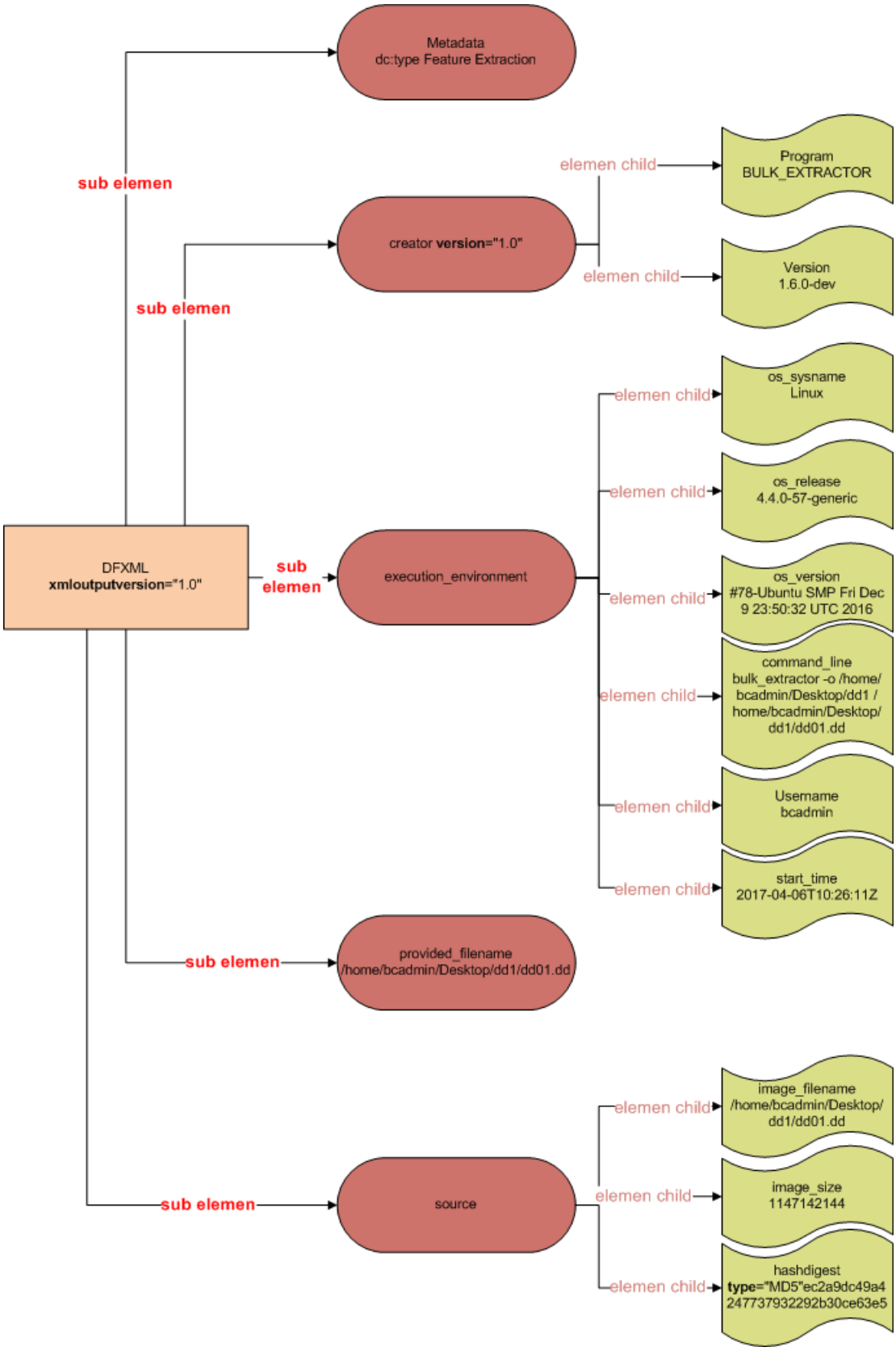
- Program ini merupakan aplikasi forensik yang digunakan untuk mengekstrak file.
- *Version* merupakan versi aplikasi forensik yang digunakan untuk mengekstrak file.
- OS *Sysname* merupakan sistem operasi yang digunakan pada aplikasi forensik.
- OS *Release* merupakan rilisnya sistem operasi yang digunakan aplikasi forensik.
- OS *Version* merupakan versi sistem operasi aplikasi forensik yang digunakan.
- *Command line* merupakan aplikasi yang digunakan serta memberikan informasi letak file dd.
- *Username* merupakan nama pengguna pada aplikasi forensik yang digunakan.
- *Startime* adalah waktu dimana pengguna sedang menggunakan aplikasi forensik untuk mengekstrak file.
- *Provided filename* dan *image filename* merupakan lokasi file dd dan nama file dd.

- *Image size* merupakan ukuran file dd yang diekstrak pada aplikasi forensik.
- MD5 merupakan ciri khas masing-masing file dd.

Dalam analisa pembacaan metadata ini yang ditampilkan sama semua yaitu pembacaan metadata file secara umum dan beberapa file dalam proses korelasi metadata file tersebut dari tampilan hasil korelasi yang dimunculkan itu adalah nama file, lokasi file, ukuran file dan MD5.

Dalam sistem ini terdapat informasi tambahan yang tidak dihasilkan *output* DFXML. Informasi tambahan itu terdiri dari nama investigator, barang bukti, merk barang bukti, memberikan nama pada kasus yang ditangani investigator, memberikan keterangan kasus yang ditangani dan keterangan untuk barang bukti yang ditemukan. Pada sistem yang dibangun ini, data tambahan tersebut dapat diubah jika ada kesalahan dan file yang ada juga dapat dihapus oleh sistem.

Struktur DFXML pada gambar 4.24 hanya mengambil beberapa bagian terpenting saja. Penambahan informasi data dinamis dalam sistem belum ada pada elemen hasil file XML, maka diperlukan penambahan elemen pada hasil file XML. Struktur DFXML akan digambarkan seperti gambar 4.24 struktur DFXML dibawah ini.



Gambar 4.24 Struktur DFXML

4.9 Perbandingan Dengan Sistem Sebelumnya

Sebagai perbandingan yang ada pada sistem ini dengan sistem sebelumnya, maka dibuat tabel untuk perbandingan diantara sistem LPBD (Lemari Penyimpanan Bukti Digital) dan sistem MBD (Manajemen Bukti Digital) tersebut. Perbandingan kedua sistem tersebut dapat dilihat pada tabel 4.9 di bawah ini.

Tabel 4.9 Tabel Perbandingan Sistem

SISTEM LPBD	SISTEM MBD
Sistem mampu menyimpan file selain file dd, yaitu file e01 dan AFF	Sistem MBD hanya membaca file dd
Dapat menampilkan fungsi *hash* selain MD5 yaitu SHA1	Hanya menampilkan fungsi *hash* MD5
Sistem lebih terstruktur	Sistem tidak terstruktur
Pengguna dibagi menjadi tiga	Pengguna hanya satu
Sistem tidak menggunakan database	Sistem menggunakan database
Sistem ini membuat file XML sendiri	Sistem ini mengunggah file XML
ChainOfCustody dapat disesuaikan dengan kebutuhan dan menghasilkan *Output* dalam bentuk XML	*Chain Of Custody* pada sistem MBD sudah ada dan menghasilkan sebuah *database*

Pada sistem LPBD dan sistem MBD maka dapat memberikan sebuah informasi tentang perbandingan terhadap kedua sistem tersebut.

Dalam sistem LPBD terdapat file selain file dd, yaitu file e01 dan AFF dimana file tersebut juga file hasil bukti digital. Sedangkan sistem MBD hanya mampu menyimpan file dd.

Sistem LPBD dapat menampilkan fungsi *hash* selain MD5 yaitu SHA1 dimana SHA1 enkripsinya lebih panjang daripada MD5. Sedangkan sistem MBD hanya menampilkan MD5 saja dimana enkripsinya lebih sedikit dibandingkan SHA1.

Sistem LPBD dalam penyimpanan informasi lebih terstruktur, dimana LPDB terdapat tiga bagian penyimpanan, yaitu lemari, rak dan kantong bukti digital. Sedangkan MBD tidak terstruktur karena hanya ada satu tempat penyimpanan.

Pada sistem LPBD terdapat tiga pengguna dimana tiga pengguna mempunyai peran masing-masing. *First responder* berperan sebagai orang yang pertama mengunggah bukti digital ke dalam LPBD, *investigator* adalah orang yang melakukan investigasi bukti digital

terhadap kasus yang sedang dihadapi, dan yang terakhir *officer* memiliki peran sebagai pengatur hak akses terhadap LPBD. Selain itu, ia memiliki akses untuk mencetak *formchain of custody*. Sedangkan pada sistem MBD hanya ada satu pengguna, dimana pengguna bisa mengunggah file dd dan file XML serta memberikan data-data tentang kasus yang sedang ditanganinya.

Sistem LPDB tidak menggunakan database untuk penyimpanan informasi bukti digital tetapi menggunakan XML dalam membentuk sebuah informasi sedangkan pada sistem MBD menggunakan *database* untuk penyimpanan informasi bukti digital.

BAB 5
Kesimpulan Dan Saran

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan oleh penulis mengenai pembuatan sistem pengembangan *output* DFXML untuk manajemen bukti digital, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Sistem yang dibangun mampu mengelola file-file DFXMLsecara bersamaan yang dapat melakukan manajemen terhadap file bukti digital dan lebih memudahkan dalam pengelolaan bukti digital hasil *output* DFXML.
2. Dalam kinerja sistem ini hanya dapat menambahkan file dd, file xml, dan menambahkan beberapa data yang sudah ada pada sistem. Sistem dapat merubah data selain file xml dan file dd, serta menghapus data bukti digital.

5.2 Saran

Hasil dari penelitian dan pengujian sistem yang dibangun terdapat keterbatasan serta kekurangan. Oleh karena itu, beberapa saran yang diusulkan dapat membantu mengembangkan penelitian dimasa yang akan datang yaitu adanya mekanisme atau prosedur yang lebih baik untuk penyimpanan hasil akuisisi bukti digital agar dapat memudahkan investigator dalam pengelolaan file hasil akuisisi hasil bukti digital.

DAFTAR PUSTAKA

ACPO. (2011). ACPO Good Practice Guide for Digital Evidence, (March), 41.

Agarwal, A., Megha, & Saurabh. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–134.

Alanazi, F., Lebh, L., & Jones, A. (2015). The Value of Metadata in Digital Forensics, *8*(2011), 161174. http://doi.org/10.1109/EISIC.2015.26

Al-Azhar, M. N. (2012). *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek.

Cohen, M., Garfinkel, S., Schatz, B., Cohen, M., Garfinkel, S., & Schatz, B. (2009). Extending the Advanced Forensic Format to Accommodate Multiple Data Sources , Logical Evidence , Arbitrary Information and Forensic Workflow By multiple data sources , logical evidence , arbitrary information and forensic workflow. http://doi.org/10.1016/j.diin.2009.06.010

Commitee Joint Technology. (2016). Managing Digital Evidence in Courts, *1*, 10.

Ćosić, J., & Bača, M. (2010). A Framework to (Im)Prove „Chain of Custody“ in Digital Investigation Process.

Dogan, S., & Akbal, E. (2017). Analysis of Mobile Phones in Digital Forensics. *International Convention on Information and Communication Technology, Electronics and Microelectronics*, 1241–1244.

Garfinkel, S. (2011). Digital Forensics Tool Integration 7 DEC 2011.

Garfinkel, S. (2011). Digital Forensics XML and the DFXML Toolset, 1–44.

Grande, C. L., & Guadron, R. S. (2016). when crime makes use of technology.

Griffin, R. W. (2012). Towards Finding the Balance of Art and Science in Management: A Market Approach to Valuing Management Research.

Harbawi, M., & Varol, A. (2017). An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I : *International Symposium on Digital Forensic and Security*, 1–6.

Hasan, M., Anutariya, C., & Ja, M. Z. (2012). A Metadata-orientated Integrated Approach to Personal File Management, 459–464.

Huo, L., & Yi, R. (2015). Research on Metadata Management Scheme of Distributed File System. http://doi.org/10.1109/CSA.2015.25

Levine, B. N., & Liberatore, M. (2009). DIGITAL FORENSIC RESEARCH CONFERENCE DEX : Digital Evidence Provenance Supporting Reproducibility and Comparison By Brian Levine and Marc Liberatore DEX : Digital evidence provenance supporting reproducibility and comparison. http://doi.org/10.1016/j.diin.2009.06.011

Member, A. C., Cattaneo, G., & Maio, G. D. E. (2013). Automated Production of Predetermined Digital Evidence, *1*.

Morioka, E. (2016). Digital Forensics Research on Cloud Computing : An investigation of Cloud Forensics Solutions.

POLRI. (2017). PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA NOMOR 8 TAHUN 2014, 1–12.

Prayudi, Y. (2015). Digital Chain of Custody : State of The Art Digital Chain of Custody : State of the Art, (April). http://doi.org/10.5120/19971-1856

Rani, D. R. (2015). An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots, *00*(c).

Simbolon, G., Albisar, M., Mulyadi, M., & Leviza, J. (2016). ANALISIS HUKUM ATAS PENETAPAN TERSANGKA TINDAK PIDANA KORUPSI DALAM KAITAN DENGAN WEWENANG LEMBAGA PERADILAN. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. http://doi.org/10.1017/CBO9781107415324.004

Strickland, J. (2016). How Computer Forensics Works. http://doi.org/10.2495/SDP-V11-N3-355-364

Tekli, J., & Member, I. (2016). An Overview on XML Semantic Disambiguation Background , Applications , and Ongoing Challenges, *4347*(c), 1–20. http://doi.org/10.1109/TKDE.2016.2525768

Turner, P. (2005). Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags).

Vries, A. De, Alink, W., Bhoedjang, R. A. F., Boncz, P. A., & Vries, A. P. De. (2006). DIGITAL FORENSIC RESEARCH CONFERENCE XIRAF - Ultimate Forensic Querying By XIRAF – XML-based indexing and querying for digital forensics. http://doi.org/10.1016/j.diin.2006.06.016

Widatama, K. (2017). Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML.

Zghal, R., Mnif, F., Amel, C., & Amous, I. (2015). Adaptive global schema generation from heterogeneous metadata schemas. *Procedia - Procedia Computer Science*, *60*, 197–205. http://doi.org/10.1016/j.procs.2015.08.119