MANAJEMEN BUKTI DIGITAL HASIL AKUISISI DFXML

Putry Wahyu Setyaningsih[1], Yudi Prayudi[2] , Bambang Sugiantoro[3]

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

ABSTRAK

Kasus kejahatan yang banyak terjadi di era modern ini adalah kejahatan di dunia maya yang meninggalkan jejak berupa barang bukti elektronik. Barang bukti elektronik tersebut harus diakuisisi terlebih dahulu untuk menemukan bukti didalamnya dengan mengunakan aplikasi. Salah satu hasil dari akuisisi bukti elektronik adalah berupa DFXML. DFXML adalah pengembangan dari bahasa XML yang dirancang untuk berbagai macam informasi forensik dan hasil pengelolaan forensik. Hasil dari DFXML ini berupa file dengan ekstensi XML, dimana file dengan ekstensi XML ini menghasilkan banyak elemen-elemen dari bukti elektronik yang diakuisisi menjadi bukti digital. Banyaknya elemen-elemen yang dihasilkan oleh XML membuat petugas investigator sulit untuk membacanya. Saat ini masih belum banyak pengembangan yang dilakukan untuk memudahkan petugas *investigator* untuk membaca elemen-elemen XML hasil akuisisi bukti elektronik menjadi bukti digital yang berupa DFXML. Oleh karena itu dilakukan penelitian dengan melakukan sebuah pengembangan dengan sebuah wadah yang akan mengubah elemen-elemen XML ke dalam sebuah *form* yang dapat dibaca oleh petugas investigator.

Kata Kunci: *Bukti Elektronik, Bukti Digital, DFXML, Elemen, XML*

ABSTRACT

Cases of crime that many occur in this modern era is a crime in cyberspace that leaves traces of electronic evidence. Electronic evidence must be obtained first to find evidence in it by using the application. One of the results of electronic evidence acquisition is DFXML. DFXML is an XML language development designed for various forensic information and forensic management results. This DFXML result is a file with an XML extension, where XML files generate many elements from each acquisition result. The number of elements generated by XML makes the investigation officer hard to read. Currently there is not much development done to facilitate the investigator to read the XML elements from the acquisition of electronic evidence into digital evidence in the form of DFXML. Therefore, research is done by developing with a system that will transform the XML element into a form that can be read by the investigator.

Keywords: *Electronic evidence, Digital Evidence, DFXML, Elemen, XML*
DOI : 10.15408/jti.v11i1.6680

I. PENDAHULUAN

Kasus kejahatan yang terjadi saat ini banyak melibatkan berbagai macam barang bukti. 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 [1].

Layaknya kejahatan yang dilakukan secara konvensional, kejahatan dunia maya juga meninggalkan jejak atau pun barang bukti yang disita dan dapat memberikan sebuah petunjuk dalam pembuktian sebuah kasus kejahatan. Kegiatan forensika digital bertujuan untuk mencari bukti digital [2]. Forensika digital melibatkan dua jenis barang bukti yaitu barang bukti elektronik dan barang bukti digital. 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 [3]. Sedangkan barang bukti digital merupakan data digital yang tersimpan di dalam perangkat elektronik tersebut dan baru akan muncul setelah barang bukti elektronik tersebut diakusisi.

Bukti digital memainkan peran yang sangat penting dalam hal pengungkapan kasus *cybercrime*. 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 [4].

Digital Forensics XML (DFXML) adalah pengembangan dari bahasa XML yang dirancang untuk mewakili berbagai macam informasi forensik dan hasil pengolahan forensik [5]. 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 [6]. XML atau *eXtensible Markup Language* merupakan suatu format dokumen dengan berbasis teks yang dibuat sebagai salah satu cara untuk membuat data lebih terstruktur, dan dapat digunakan untuk menyimpan dan mengirim informasi menjadi lebih mudah. Struktur bahasa XML yang sederhana, semi-terstruktur (struktur dapat dibuat secara mandiri), dapat dibuat dengan berbagai ekstensi (*extensibility*) [7].

Selama ini sistem yang ada dalam penanganan output DFXML menyulitkan investigator, dimana hasil akuisisi dari satu bukti digital akan menghasilkan satu file bukti digital yang berada di folder tertentu dan akan terus berulang untuk bukti digital yang berikutnya yang pasti akan membuat banyak folder sehingga perlu dibuat suatu mekanisme lain untuk menangani file-file output hasil DFXML. File hasil output DFXML akan dimasukkan ke dalam sistem yang telah dibuat kemudian investigator dapat melakukan manajemen bukti digital.

Manajemen bukti digital yang dimaksud adalah manajemen yang mengakomodir beberapa aktivitas, seperti: melihat bukti digital, membaca bagian terpenting dari tag XML, mengubah data dinamis pada *chain of custody* dan menghapus bukti digital. Akuisisi hasil bukti digital berupa file XML dan file *disk doubler* (dd) kemudian diunggah ke dalam sistem dimana sistem yang dibuat akan menguraikan hasil dari DFXML menjadi sebuah form yang mudah dibaca oleh investigator.

Atas dasar permasalahan tersebut, perlu dilakukan sebuah penelitian mengenai pengembangan manajemen bukti digital hasil akuisisi DFXML untuk manajemen bukti digital untuk memudahkan investigator dalam

mengelola beberapa file DFXML secara bersamaan.

II. TINJAUAN PUSTAKA

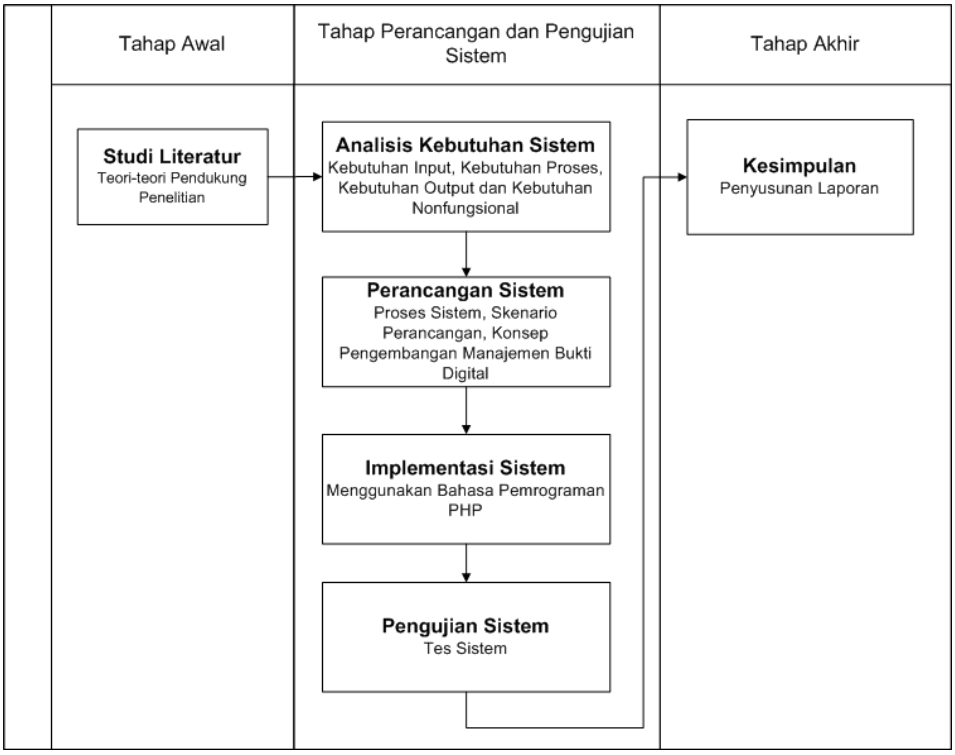
Digital Forensics XML (DFXML) adalah sebuah bahasa XML yang memungkinkan terjadinya perubahan struktur informasi *forensic*. DFMXL dapat mewakili asal subyek data untuk investigasi forensik, mendokumentasikan keberadaan dan lokasi dari *file system* dan informasi teknis lainnya. Penggunaan spesifik untuk DFXML sebagai berikut DFXML mengembangkan kemampuan mengubah dengan menyediakan sebuah bahasa untuk mendeskripsikan proses-proses *forensic* serupa (misal, *hashing* kriptografik), produk kerja forensik (misal, lokasi file pada *hard drive*) dan metadata (misal, nama file dan *timestamp*).

Fiwalk adalah bagian yang digunakan untuk menghasilkan laporan XML. Fiwalk dapat dijalankan melalui Bitcurator.

BitCurator adalah salah satu turunan dari Linux Ubuntu, Bitcurator mengembangkan *software* untuk mengekstrak, menganalisis dan menghasilkan laporan dari sebuah bukti digital. File *object* adalah XML *Forensics* dan XML tag yang digunakan untuk menggambarkan informasi tentang sebuah file. Objek file dapat berisi informasi tentang nama file, lokasi file, ukuran file dan kode *hash* file.

III. METODOLOGI

Secara ringkas metode dan tahapan penelitian yang dilakukan dapat digambarkan seperti pada Gambar 1 di bawah ini.



Gambar 1. Metode penelitian

- Tahap Awal
  Proses ini merupakan tahap awal untuk mengumpulkan teori-teori yang berhubungan dengan DFXML.
- Tahap Perancangan Awal dan Pengujian Sistem
  Proses ini merupakan proses setelah semua literatur terkumpul. Tahap ini melibatkan 4 proses utama.
  1. Analisis kebutuhan sistem
     Proses untuk menganalisis kebutuhan sistem berupa: *input* dan *output.*
  2. Perancangan sistem
     Analisis terhadap proses yang terjadi pada sistem yang berkaitan dengan manajemen bukti digital.
  3. Implementasi sistem
     Proses implementasi sistem menggunakan bahasa PHP berdasarkan perancangan dan

analisis yang telah dilakukan pada proses sebelumnya.

4. Pengujian sistem
   Proses untuk menguji sistem. Proses ini bertujuan untuk menguji fungsionalitas sistem mencakup *input* dan *output* sistem yang dibuat.

- Tahap Akhir
  Tahap ini merupakan tahapan dimana sistem telah diuji dan pembuatan laporan terhadap hasil uji sistem tersebut dilakukan.

IV. HASIL DAN PEMBAHASAN

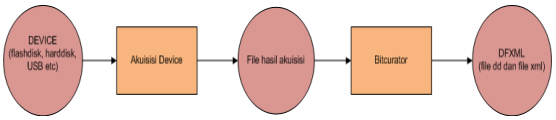
Salah satu hasil akuisisi bukti digital dari *Flashdisk* menggunakan aplikasi dc3dd seperti gambar di bawah ini

```
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 2. Hasil akuisisi bukti digital

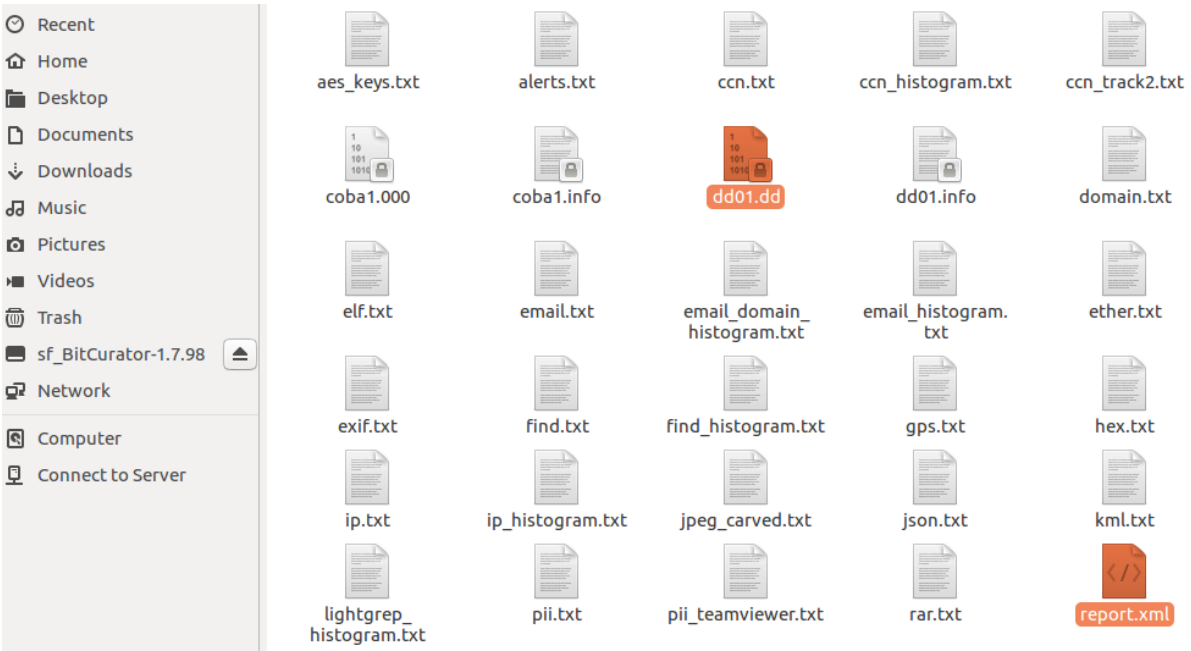
Flashdisk yang diakuisisi terdapat satu file di dalamnya dengan ukuran file 1147142144 bytes. Semakin banyak isi di dalam *Flashdisk* akan semakin banyak elemen yang dihasilkan. Elemen dalam *flashdisk* yang berisi satu file ini menghasilkan kurang lebih mencapai 500 lebih baris.

Pada gambar di bawah menjelaskan bahwa file hasil bukti elektronik yang dapat berupa *Flashdisk*, *Harddisk*, dan lainnya yang akan di akuisisi terlebih dahulu dan akan menghasilkan sebuah file bukti digital. Setelah itu file bukti digital akan diakuisisi dengan menggunakan sebuah *tools* yang bernama Bitcurator. Alurnya seperti pada gambar di bawah ini.



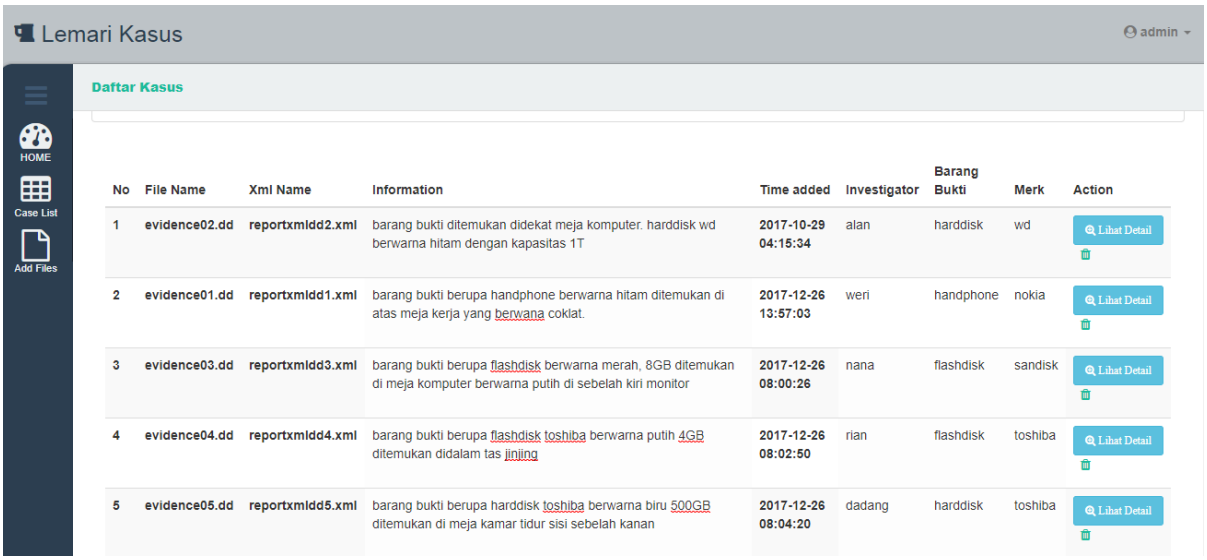
Gambar 3. Alur akuisisi

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 aplikasi 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. Salah satu contohnya seperti gambar di bawah ini.



Gambar 4. Folder hasil akuisisi DFXML

Dalam masalah yang ada, maka dibuatkan sebuah solusi untuk membangun sebuah aplikasi guna menangani file-file hasil akuisisi DFXML untuk dikelola secara bersamaan. Dengan aplikasi tersebut file-file hasil akuisisi DFXML akan mudah dikelola dan mudah ditangani investigator. Gambarnya dapat dilihat seperti gambar di bawah ini



Gambar 5. Manajemen file hasil akuisisi DFXML

Pada aplikasi yang dibuat tidak hanya memudahkan investigator dalam pengelolaan file hasil akuisisi DFXML saja, tetapi investigator dapat menambahakan nama investigator yang sedang menangani kasus, memberikan informasi kasus yang sedang ditanganinya, memberikan informasi barang bukti elektronik yang ditemukan, merk dari barang bukti yang ditemukan. Sistem yang dibangun juga dapat mengubah data jika terjadi kesalahan, sistem juga dapat menghapus file bukti digital tersebut.

Struktur DFXML pada tabel di bawah menampilkan sebagian elemen XML dari hasil akuisisi pada Gambar 2. Semakin banyak file yang ada pada bukti elektronik yang di akuisisi menjadi bukti digital semakin banyak juga elemen yang akan dihasilkan.

Elemen paling tinggi dalam elemen XML adalah DFXML. Elemen XML yang pasti akan

muncul adalah sub elemen *source* yang mempunyai tiga elemen *child* yang paling penting di dalam setiap hasil akuisisi bukti digital yaitu *image_filename*, *image_size*, dan *hashdigest*. *Hashdigest* dengan tipe MD5 adalah pembeda dari satu bukti digital dengan bukti digital yang lainnya. Elemen XML selain yang ada dalam tabel banyak mengalami perulangan dan menggunakan istilah asing yang mungkin bagi sebagian orang yang membacanya akan mengalami kesulitan dan terlalu banyak elemen yang tidak penting.

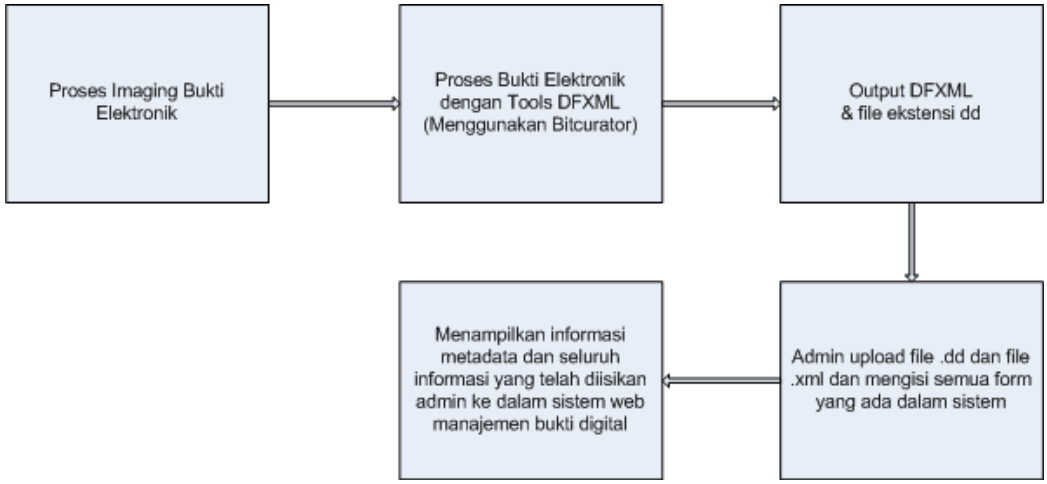
Tabel 1. Struktur DFXML

```
<?xml version='1.0' encoding='UTF-8'?>
<dfxml xmloutputversion='1.0'>
<metadata
   <dc:type>#</dc:type>
    </metadata>
<creator version=' # '>
   <program> # </program>
       <version> # </version>
    </creator>
<execution_environment>
    <os_sysname>Linux</os_sysname>
    <os_release> # </os_release>
    <os_version> # </os_version>
    <host>ubuntu</host>
<command_line>#</command_line>
    <username> # </username>
    <start_time> # </start_time>
</execution_environment>
 <provided_filename>/ #
</provided_filename>
    <source>
    <image_filename> # </image_filename>
    <image_size> # </image_size>
    <hashdigest type='MD5'> #
</hashdigest>
    </source>
```

Gambar di bawah merupakan proses perancangan sistem yang akan dibangun untuk manajemen bukti digital hasil akuisisi DFXML. Penjelasan proses tersebut akan dijabarkan pada poin-poin berikut:

- Proses akuisisi bukti elektronik menjadi bukti digital dengan ekstensi dd.
- Setelah itu, Bitcurator memproses bukti digital yang kemudian menghasilkan file dengan ekstensi DFXML.
- 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 ke dalam sistem yang dibangun.
- 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.
- Setelah selesai ungguh file dd, file xml dan semua data sudah di isi, maka sistem akan menampilkan semua informasi dan membaca metadata dari file yang diunggah oleh pengguna.

Gambar alur tersebut digambarkan pada gambar di bawah ini



Gambar 6. Alur manajemen DFXML

Gambar ketujuh menunjukkan potongan elemen-elemen. DFXML menghasilkan banyak elemen, padahal tidak semua dari elemen-elemen tersebut digunakan. Sehingga sistem hanya akan membaca elemen-elemen yang penting (nama file, lokasi file, ukuran file dan MD5 file).

Struktur DFXML paling tinggi adalah elemen DFXML. DFXML mempunyai sub elemen yang berupa *source*, dimana *source* mempunyai 3 elemen child. Ketiga elemen *child* dari *source* adalah image_filename, image_size, dan hashdigest dengan atribut type.

Pada elemen image_filename terdapat lokasi bukti digital berada. Selanjutnya, elemen image_size terdapat ukuran bukti digital yang diakuisisi dalam satuan *byte*. Terakhir adalah elemen hashdigest dengan atribut type yang berisi kode unik dari bukti digital yang menjadi pembeda antara bukti digital satu dengan bukti digital lainnya.

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

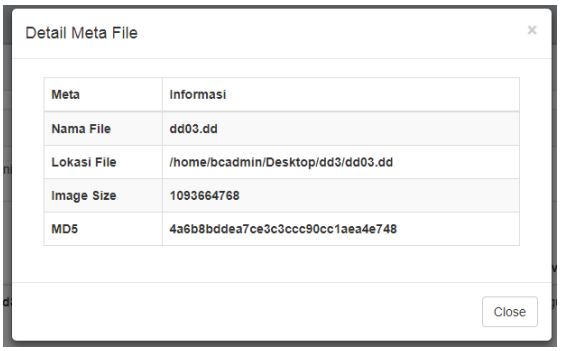
Gambar 7. Sebagian elemen report.xml

Gambar kedelapan menunjukkan file XML yang di ambil untuk dibaca oleh sistem. Banyak elemen yang terdapat pada file hasil akuisisi, tetapi pada sistem ini hanya diambil elemen yang terpenting yang akan dibaca oleh pengguna. Dikarenakan banyaknya elemen dari satu bukti digital tidak memungkinkan untuk dikeluarkan maupun dibaca oleh pengguna. Elemen-elemen yang akan dibaca berupa: nama file, lokasi file, ukuran file dan kode hash dari file bukti digital.

Detail metadata yang akan dibaca pada sistem yang pertama adalah nama file yang berupa nama file bukti digital yaitu dd03.dd. Selanjutnya lokasi file bukti digital hasil akuisisi berada di lokasi /home/bcadmin/Desktop/dd3/dd03.dd.

Metadata yang dibaca selanjutnya adalah ukuran file bukti digital hasil akuisisi yaitu 1093664768 byte. Dan yang paling utama dari file hasil akuisisi bukti digital adalah MD5 yang terdiri atas angka dan huruf.

Dari elemen-elemen yang ada terdapat elemen yang dibutuhkan oleh pengguna di antaranya adalah MD5 dari sebuah bukti digital yang telah diakuisisi. Bukti digital yang diakuisisi akan menghasilkan elemen-elemen yang berbeda-beda. Bukti digital MD5 adalah kode untuk membedakan bukti digital satu dengan bukti digital yang lainnya.



Gambar 8. Hasil baca metadata

V. PENUTUP

Berdasarkan hasil penelitian yang dilakukan, maka didapatkan kesimpulan yang sesuai dengan tujuan yaitu sebuah

wadah yang mampu menangani masalah yang selama ini menyulitkan investigator dalam melakukan penanganan hasil akuisisi DFXML dari sebuah kasus bukti digital. Sebuah wadah yang mampu mengelola hasil akuisisi DFXML dari bukti digital dan mampu membaca elemen XML dari hasil akuisisi bukti digital.

DAFTAR PUSTAKA

[1] POLRI. (2017). Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2014, 1–12

[2] A. Varol and Y. Ulgen Sonmez, "Review of Evidence Analysis and Reporting Phases in Digital Forensics Process," 2017.

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

[4] Prayudi, Y. (2015). Digital Chain of Custody : State of The Art Digital Chain of Custody : State of the Art, (April).

[5] Garfinkel, S. (2011). Digital Forensics XML and the DFXML Toolset, 1-44.

[6] D. Zhao, H. Fu, H. Ren, M. Wei, and J. Chu, "XML Documents Clustering Algorithm Based on Cluster Core And LSPX," pp. 1027–1032, 2017.