Vol. 6 No.2 Tahun 2020, pp. 53-63
Jurnal Teknologi dan Manajemen Informatika
http:// http://jurnal.unmer.ac.id/index.php/jtmi
P-ISSN: 1693-6604 E-ISSN: 2580-8044

Rancang Bangun Sistem untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital

Tino Feri Efendi [1], Ridho Rahmadi [2], Yudi Prayudi [3]

Universitas Islam Indonesia Yogyakarta, Jl. Kaliurang km 14.5, Sleman, Yogyakarta

Info Artikel

Riwayat Artikel
Diterima: 05-06-2020
Direvisi: 22-07-2020
Disetujui: 25-11-2020

Kata Kunci
Bukti Fisik;
Chain of Custody;
Inventori Data;

✉ Corresponding Author
Tino Feri Efendi,
Tel. +62 5642142940
tinoferit@yahoo.co.id

ABSTRAK

Kejahatan komputer memiliki dua jenis barang bukti yaitu bukti fisik dan bukti digital. Penyimpanan bukti fisik membutuhkan ruang khusus yang dapat menampung bukti fisik. Namun diperlukan sistem yang dapat menyimpan dan mengelola bukti fisi. Permasalahannya adalah tidak adanya konsep penyimpanan bukti fisik serta dokumentasi (*Chain of Custody*). Manajemen barang bukti fisik dan konsep pada sistem manajemen bukti fisik dan *Chain of Custody* dengan mengambil analogi sebuah data inventory. Permasalahan pada manajemen barang bukti fisik membutuhkan sistem manajemen untuk barang bukti fisik yang sesuai untuk diterapkan di lingkungan laboratorium forensika digital UII. Hasil dari penelitian ini adalah mengimplementasikan konsep data inventory yaitu konsep manajemen barang bukti fisik melalui kontrol barang bukti fisik dan segala aktivitas yang berkaitan dengan bukti fisik dapat terjaga serta dapat terdokumentasi dengan baik.

PENDAHULUAN

Barang bukti merupakan hal sangat penting, tetapi permasalahannya adalah banyak hal yang dapat melemahkan pembuktian dari barang bukti tersebut. Salah satu diantaranya adalah alat bukti yang ada tidak dapat diterima di pengadilan atau sering disebut *not admissible at court.* Beberapa hal yang dapat menyebabkan barang bukti menjadi tidak diterima adalah proses ekstraksi atau pengambilan barang bukti yang tidak profesional, tidak ada kesesuaian antara perkara dengan alat bukti yang ditampilkan, atau hal lain yang merupakan kesalahan dari penyidik. Keberadaan barang bukti sangat penting dalam investigasi kasus-kasus *computer crime* maupun *computer related crime* karena dengan barang bukti inilah seorang investigator dan analis *forensic* dapat mengungkap kasus-kasus dengan kronologis secara lengkap, untuk kemudian melacak keberadaan pelaku dan menangkapnya. Oleh karena posisi barang bukti ini sangat strategis, seorang investigator dan analis *forensic* harus paham jenis-jenis barang bukti, sehingga ketika datang ke tempat kejadian perkara (TKP) yang berhubungan dengan kasus *computer crime* dan *computer-related crime*, ia dapat mengenali keberadaan barang bukti untuk kemudian diperiksa dan dianalisa lebih lanjut. Supaya barang bukti dapat digunakan di dalam proses penegakan hukum, maka barang bukti tersebut harus terjaga dan sama persis dengan ketika pada saat pertama kali ditemukan. Dalam dunia forensika digital, salah satu pembuktian secara ilmiah adalah dengan tahap dokumentasi bukti digital dan bukti fisik. Menurut [1] juga mengungkapkan bahwa agar bukti digital dan bukti fisik dapat diterima di pengadilan, *Chain of Custody* (dokumentasi barang bukti) dan aspek informasi dari *Chain of Custody* menjadi domain penting yang harus diperhatikan.

Chain of Custody akan mendokumentasikan persyaratan yang terkait dengan tempat, kapan, mengapa, siapa, bagaimana dalam penggunaan bukti pada setiap tahap proses investigasi. Masalah *Chain of Custody* menjadi sangat penting sebagai keaslian bukti yang harus dipertahankan sesuai dengan kondisi ketika pertama kali ditemukan sampai kemudian disajikan di pengadilan. Lingkup *Chain of Custody* mencakup semua individu yang terlibat dalam proses akuisisi, pengumpulan, analisis bukti, catatan waktu serta informasi kontekstual, yang mencakup pelabelan kasus, dan unit dan laboratorium yang memproses bukti. Menurut [2] dalam laporan *National Institute of Justice* dokumen formulir *Chain of Custody* berisi *history* atau kronologi perjalanan barang bukti yang memuat informasi lengkap seperti subyek/obyek yang terlibat dalam aktivitas pengumpulan dan analisis, tanggal/waktu serta tempat pengumpulan dan analisis, nama lengkap dan nama panggilan korban maupun pelaku, nama agensi serta deskripsi lengkap barang bukti. Keterkiatan antara pentingnya bukti fisik dan *Chain of Custody* mendorong penulis untuk meneliti tentang manajemen *Chain of Custody* pada barang bukti fisik. Hal tersebut diharapkan dapat membantu suatu penyelidikan dalam manajemen barang bukti fisik.

Bukti Digital

Bukti digital menurut [3] adalah jejak yang dinginkan maupun tidak diinginkan yang berasal dari perubahan data digital pada perangkat elektronik. Berdasarkan sumbernya, bukti digital terbagi menjadi dua kategori [4] antara lain *closed system* dan *open system*. *Closed system* merupakan sistem yang pernah terkoneksi internet. Artinya, sistem tersebut sangat terisolasi dan hanya terhubung dengan sistem pada komputer yang lain. Berbeda dengan *closed system*, *open system* merupakan sistem yang terhubung dengan internet meskipun sistem tersebut tidak terhubung dengan sistem pada komputer lain, contohnya ketika seseorang menghubungkan laptop pada WiFi.

Menurut [2] terdapat empat prinsip dalam penanganan bukti digital. Berikut adalah empat prinsip penanganan bukti digital menurut ACPO.

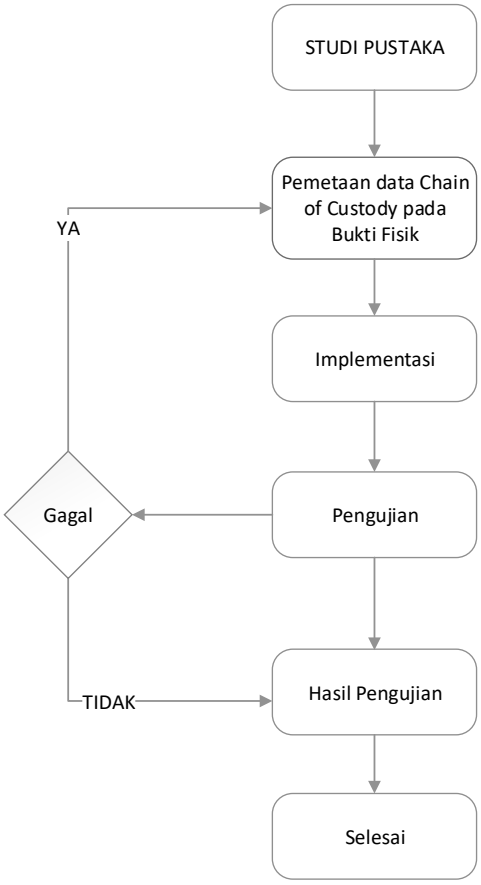
1. Prinsip 1, seorang penegak hukum tidak diperbolehkan untuk mengubah data yang terdapat pada komputer atau media penyimpanan karena hal ini akan dipertanggung jawabkan di pengadilan.
2. Prinsip 2, dalam situasi tertentu dan jika memang diharuskan, seseorang diperbolehkan untuk mengakses data yang asli, namun orang tersebut harus kompeten dan ia harus dapat menjelaskan tentang relevansi terhadap barang bukti serta implikasi terhadap kegiatan yang dilakukan terhadap barang bukti tersebut.
3. Prinsip 3, catatan dan audit yang berisi semua proses dalam penanganan barang bukti elektronik harus dibuat dan ketika pihak ketiga memeriksa catatan dan audit tersebut, hasilnya harus sama dengan yang dimiliki oleh pihak investigator.
4. Prinsip 4, orang yang bertanggung jawab dalam investigasi ini harus memastikan bahwa hukum dan semua prinsip ini dipatuhi oleh orang-orang yang terlibat.

Konsep Lemari Penyimpanan Bukti Fisik

Munculnya konsep lemari penyimpanan bukti fisik didasarkan atas permasalahan dalam penanganan bukti digital yang berkutat dalam beberapa hal yaitu: model bisnis dari bagian-bagian yang berhubungan langsung dengan bukti digital, penyimpanan informasi metadata bukti digital maupun kontrol akses dan kemananan terhadap digital CoC. Konsep ini diperkenalkan oleh [5] dalam penelitiannya yang berjudul *Digital Evidence Cabinets: A Proposed Frameworks for Handling Digital Chain of Custody*. Dalam penelitiannya disebutkan bahwa lemari penyimpanan bukti digital merupakan sistem yang dibuat untuk penanganan CoC dari setiap bukti digital yang telah diperoleh. Konsep ini dibangun atas 3 pendekatan, yaitu: *Digital Evidence Management Frameworks*, kantong bukti digital dan keamanan

METODE

Metode penelitian dengan menjelaskan setiap alur proses penelitian secara struktur dan sistematis. Memilih metode ini guna saat menemukan permasalahan dapat diatasi dengan terstruktur dan sitematis. Apabila terjadi permasalahan saat dilakukannya proses penelitian ini, dapat menemukan solusi yang tepat untuk menyelesaikan permasalahan dan tidak menghambat proses penelitian ini.



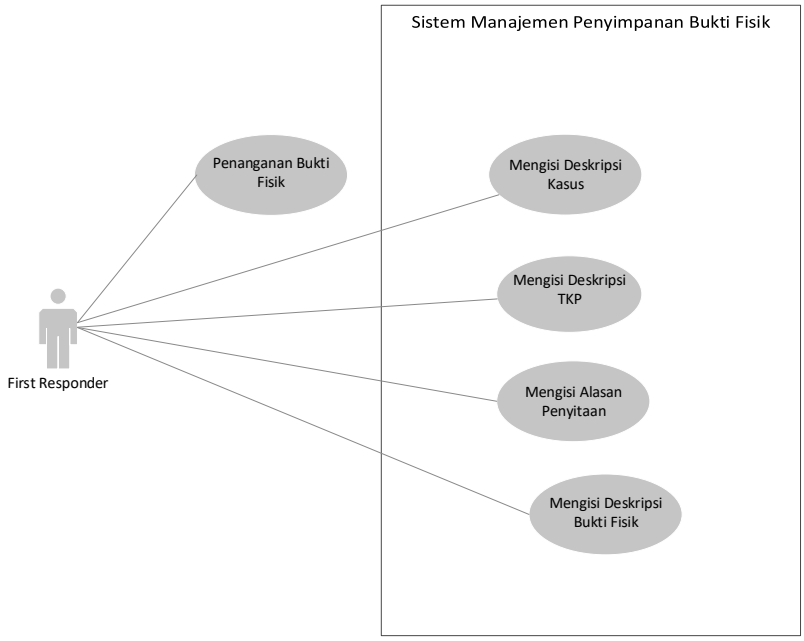
Gambar 1. Metodologi Penelitian

Pembagian Hak Akses terhadap Sistem

Setelah studi pustaka dilakukan dan informasi-informasi dari berbagai sumber yang terkait dengan penelitian ini didapatkan tahapan selanjutnya adalah pembuatan konsep manajemen penyimpanan bukti fisik. Pada konsep ini terdapat tiga *use case* yang digunakan untuk membagi hak otorisasi dari setiap aktor yang terlibat dalam penanganan kasus kejahatan komputer. Pembagian hak otorisasi bertujuan agar setiap aktor pada konsep ini dapat mengatur setiap aktivitas dalam sistem manajemen yang akan dibuat pada penelitian tersebut dengan baik.

Hak Otorisasi *First Responder*

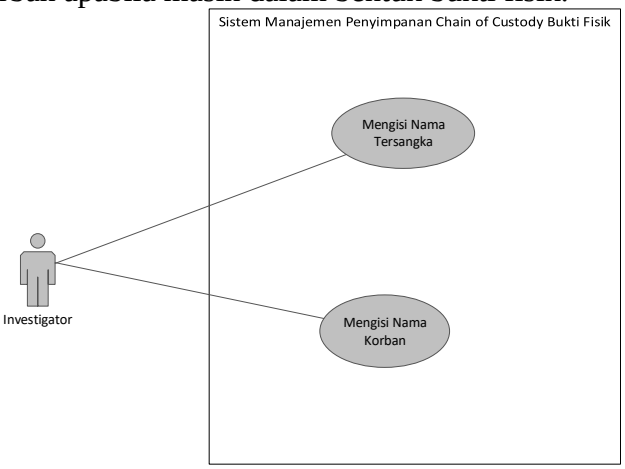
First responder juga dapat mengganti akun dengan akun lain yang sudah terdaftar pada sistem. Akun tersebut digunakan untuk masuk kedalam sistem. Akun tersebut berupa informasi tentang instansi tempatnya bekerja, *username* dan *password*. Investigator adalah orang yang melakukan proses investigasi terhadap bukti bukti digital (hasil dari akuisisi terhadap bukti fisik) pada kasus kejahatan komputer. Pembagian hak otorisasi *first responder* terhadap sistem manajemen terkait dengan penanganan bukti. Dijelaskan melalui *use case* pada gambar 2.



Gambar 2. *Use Case* Pembagian Hak Otorisasi pada *First Responder*

Hak Otorisasi Investigator

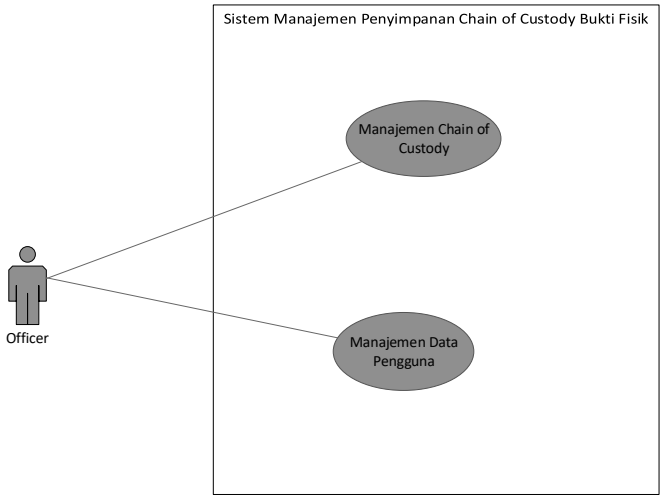
Hak otorisasi investigator terhadap sistem yaitu mengisi nama korban dan nama tersangka ke dalam sistem yang akan dibuat. Nama tersangka dan nama korban akan diisi setelah investigator melakukan analisis terhadap hasil akuisisi dari bukti fisik. Akuisi bukti fisik merupakan aktivitas dari *first responder*, jadi investigator tidak akan menganalisis nama tersangka dan nama korban apabila masih dalam bentuk bukti fisik.



Gambar 3. *Use Case* Pembagian Hak Otorisasi pada Investigator

Hak Otorisasi Officer

Aktor terakhir yang berinteraksi dengan sistem manajemen yang akan dibuat adalah *officer*. Aktor *officer* memiliki tanggung jawab penuh terhadap manajemen data pengguna dan manajemen CoC. Hak otorisasi dari aktor *officer* juga memvalidasi data-data yang dimasukkan ke dalam sistem oleh *first responder* dan investigator, validasi ini masuk ke dalam jenis aktivasi manajemen CoC. Selain itu, *officer* juga dapat merubah dan menambahkan data pengguna yang digunakan untuk mengakses sistem oleh *first responder* maupun investigator. Berikut adalah gambar yang menunjukkan pemberian hak otorisasi antara *officer* dengan sistem.



Gambar 3. *Use Case* Pembagian Hak Otorisasi pada Officer

Gambar 3 menjelaskan bahwa *Officer* memiliki tugas sebagai validator terhadap segala aktivitas yang dilakukan oleh investigator dan *first responder*. Secara umum, aktivitas yang dilakukan oleh *officer* adalah manajemen data CoC dan manajemen data pengguna. *Officer* tidak memiliki hak untuk melakukan analisis maupun penanganan bukti fisik yang merupakan tugas dari *first* responder dan investigator.

Rancangan Desain *Form chain of custody*

Rancangan desain *form chain of custody* yang dihasilkan oleh sistem ini memiliki 3 halaman utama. Halaman pertama adalah halaman yang berisi informasi kasus dan informasi deskripsi bukti fisik. Data-data yang ditampilkan pada halaman pertama merupakan data-data yang sebelumnya telah divalidasi oleh *officer*.

Crime Scene	
Case Name	Jenis Kasus yang dihadapi
Suspect	Nama Tersangka
Victim	Nama Korban
Location	Tempat Olah TKP Dilakukan
Time	Tanggal dan Waktu Olah TKP
First Responder	Nama First Responder
Tools (Live Forensics)	Tools yang Digunakan saat Olah TKP
Tools Description	Spesifikasi dari Perangkat yang Digunakan
Institution	Nama Institusi Tempat First Responder Bekerja
Electronic Evidence	
Register Number	Nomor Inventaris Bukti Elektronik
Type	Tipe Bukti Elektronik
Model	Model Bukti Elektronik
Manufacture	Nama Perusahaan Pembuat Bukti Elektronik
Serial number	Nomor Serial Bukti Elektronik
Foreclosure Reasons	Alasan Penyitaan Bukti Elektronik

Gambar 4. Konsep Desain *Form chain of custody* Halaman Pertama

Gambar 4 berisi tentang kasus kejahatan, bukti elektronik dan metadata hasil *image processing*. Kolom *crime scene* baris pertama yaitu *case name* yang merupakan catatan dari kasus kriminal yang diselidiki dan kejahatan yang yang dilakukan. Suspect berisi nama dari tersangka yang terlibat pada kasus kejahatan. Victim berisi tentang nama korban dari kasus kejahatan ini. Lalu *location* merupakan baris yang berisikan tentang lokasi terjadinya kasus kejahatan. *Time* disini berisikan waktu kapan terjadinya tindak kejahatan, waktu yang dicatatat yaitu jam dan tanggal. *Tool* atau alat apa yang digunakan untuk penyelidikan forensik terdapat pada baris *Tools(live forensic*) dan *Tool Description* berisi tentang hasil dari penyelidikan forensik tersebut.

Tanggal/Waktu		**Validator**
Diajukan	Tanggal dan waktu pengajuan data	Nama Officer
Divalidasi	Tanggal dan waktu validasi	**Pemohon**
Diterima	---	Nama first responder
Aksi	**Mengisi Data Deskripsi Kasus**	

Tanggal/Waktu		**Validator**
Diajukan	---	Nama Officer
Divalidasi	---	
Divalidasi	---	**Pemohon**
Diterima	Tanggal dan waktu diterimanya form Chain of Custody	---
Aksi	**Mencetak Form Chain of Custody**	

Gambar 5. Konsep Desain *Form chain of custody* Halaman Kedua

Berbeda dengan halaman pertama yang jumlah datanya tidak dapat bertambah, halaman kedua memungkinkan untuk memiliki jumlah datanya lebih dari satu halaman. Hal ini karena halaman ini merupakan halaman yang menyimpan semua catatan tentang segala aktivitas pengguna saat berinteraksi dengan sistem. Dalam *form* ini terdapat catatan ketika *officer* melakukan validasi terhadap data yang diinputkan *first responder* maupun investigator. Aktivitas ketika terjadi unduh bukti digital *form chain of custody* nama elemen dari struktur history akan dimunculkan beserta nilai dari setiap elemen tersebut. Simbol "---" artinya *field* tersebut kosong (tidak ada data yang dimunculkan. Halaman ini juga mencatat waktu ketika user berinteraksi dengan sistem. Terdapat beberapa aktivitas yang akan tercatat pada halaman kedua. Aktivitas-aktivitas tersebut adalah: pengisian data deskripsi kasus, pengisian data TKP, pengisian data alasan penyitaan barang bukti fisik, dan deskripsi bukti fisik. Selain itu, halaman ini juga mencatat aktivitas waktu dan tanggal unduh form CoC. Halaman ini dapat melebihi 1 halaman, hal ini dikarenakan aktivitas-aktivitas tersebut dapat lebih dari 1 kali dilakukan terutama apabila terjadi kesalahan data dan data tersebut harus diubah.

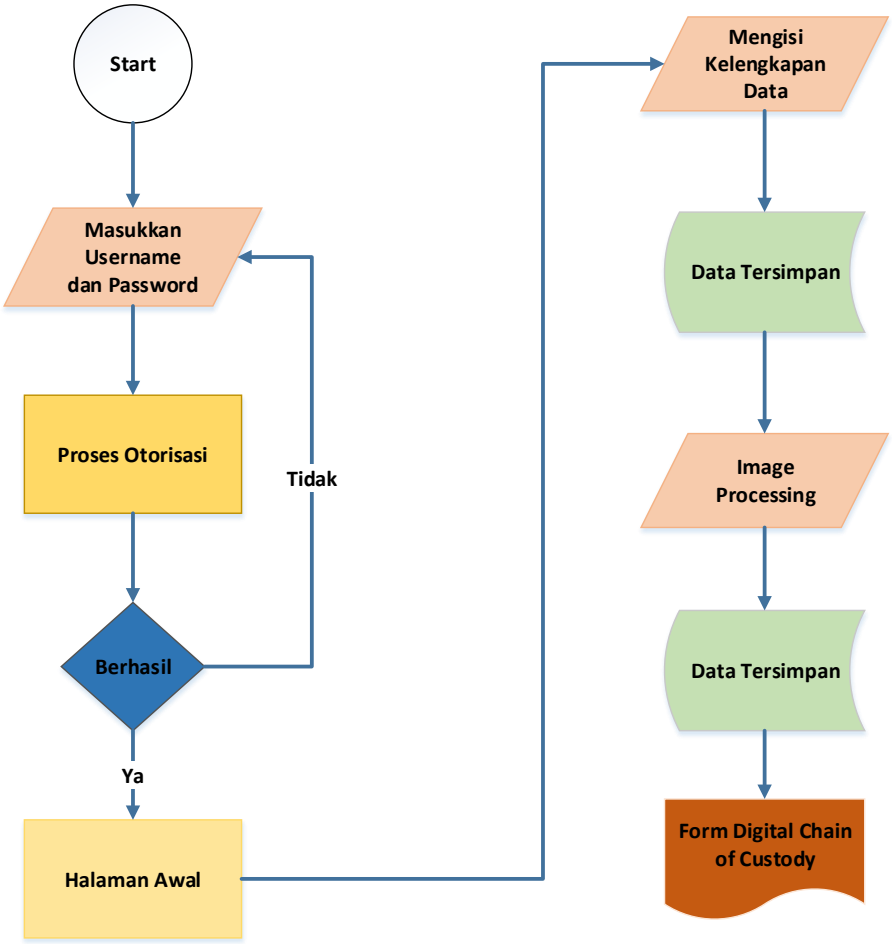
Penyimpanan data pada halaman kedua mencakup tanggal/waktu aktivitas tersebut dilakukan, aksi atau aktivitas yang dilakukan aktor yang melakukan aktivitas tersebut serta nama aktor yang melakukan aktivitas tersebut. Simbol "---" memiliki arti bahwa *field* tersebut kosong (tidak ada data yang dimunculkan). Halaman terakhir atau halaman ketiga adalah halaman validasi dari *officer* terhadap form CoC yang dihasilkan. Validasi form CoC tersebut berisi tandatangan *officer* yang telah dienkripsi menggunakan metode enkripsi MD5. *Officer* dapat memasukkan tandatangan dalam bentuk *string* melalui sistem. Halaman ketiga ini berfungsi sebagai bentuk pengesahan bahwa segala aktivitas yang terkait dengan bukti digital pada *system* telah melalui validasi dari *officer*.

HASIL DAN PEMBAHASAN

Alur Sistem

Alur kerja sistem ini dimulai dengan memasukkan *field username* dan *password.* Pengguna dapat memasukkan *username* dan *password* yang telah dibuat oleh *officer.* Setelah mendapat hak otorisasi, sistem akan menampilkan halaman utama bagi setiap pengguna, namun jika tidak mendapat hak otorisasi, maka sistem akan menampilkan sebuah pesan yang *error* sehingga membuat pengguna diminta untuk mengisi kembali data *username* dan *password.*

Setelah pengguna dapat masuk ke dalam sistem, *First Responder* dan *Investigator* dapat mengisi kelengkapan data. Data tersebut akan tersimpan pada sistem dan akan di proses melalui *image processing* agar menjadi sebuah bukti digital. Data yang sudah di proses otomatis akan disimpan pada sistem, selanjutnya hasil akhir dari proses tersebut adalah *Form chain of custody.*



Gambar 6. Alur Kerja Sistem

Alur Kerja Sistem

Alur kerja sistem ini dimulai dengan memasukkan *field username* dan *password*. Pengguna dapat memasukkan *username* dan *password* yang telah dibuat oleh *officer*. Setelah mendapat hak otorisasi, sistem akan menampilkan halaman utama bagi setiap pengguna, namun jika tidak mendapat hak otorisasi, maka sistem akan menampilkan sebuah pesan yang *error* sehingga membuat pengguna diminta untuk mengisi kembali data *username* dan *password*.

Setelah pengguna dapat masuk ke dalam sistem, *First Responder* dan Investigator dapat mengisi kelengkapan data. Data tersebut akan tersimpan pada sistem dan akan di proses melalui *image processing* agar menjadi sebuah bukti digital. Data yang sudah di proses otomatis akan disimpan pada sistem, selanjutnya hasil akhir dari proses tersebut adalah *Form chain of custody*.

Source Code

Source code yang akan dijelaskan merupakan *source code* yang membangun sistem yang berperan dalam penyimpanan data hingga *source code* tentang pembentukan *Form chain of custody* yang merupakan hasil akhir dari sistem.

Source Code Penyimpanan Data

Source code penyimpanan data di bawah ini menunjukkan potongan *source code* untuk melakukan penyimpanan data. Penyimpanan data pada system ini melibatkan 2 tabel, yaitu: tabel *record* dan tabel *case_data*. Tabel *record* berfungsi sebagai tempat penyimpanan segala aktivitas yang dilakukan oleh pengguna sistem. Sedangkan pada tabel *case_data* digunakan sebagai penyimpanan data kasus hingga data deskripsi bukti fisik.

```
case_name = self.caseName.get()
suspect_name = self.suspectName.get()
```

```
victim_name = self.victimName.get()
try:
  conn = sqlite3.connect("lpbd.db")
  conn.text_factory = str
  cur = conn.cursor()
  now = datetime.datetime.now()
  dateTime = now.strftime("%d-%m-%Y %H:%M")
  sql = """ INSERT INTO record (id_case, desc_record, user_detail, date_record) VALUES
("""+str(self.dropMenu3xy.get())+""","'Updating
Case','"""+str(self.id_user)+""","""+dateTime+""") """
   cur.execute(sql)
   sql2 = """ UPDATE case_data SET case_number = """+str(case_num)+""", case_name =
"""+str(case_name)+""", suspect_name = """+str(suspect_name)+""", victim_name =
"""+str(victim_name)+""" WHERE id_case = """+str(self.dropMenu3xy.get())+""" """
  cur.execute(sql2)
  conn.commit()
  tkMessageBox.showinfo("Success", "Your Case Has Been Updated!")
        except Exception as e:
```

Source Code Pembacaan Data

Code Pembacaan Data menunjukkan potongan *source code* untuk membaca data pada database lpbd.*db* dengan input dari user saat masuk maupun dari investigator saat mengedit kasus. Kemudian menampilkan dalam *listbox* sistem, antara lain:

```
def checklogin(self):
username = self.userName.get()
passwordx = self.passwordName.get()
passx = hashlib.sha1(passwordx).hexdigest()
try:
  conn = sqlite3.connect("lpbd.db")
  conn.text_factory = str
  cur = conn.cursor()
  cur.execute("SELECT * FROM user WHERE user_name = '"+username+"' AND
password_user = '"+passx+"""").rowcount
  rows = len(cur.fetchall())
  if(rows >= 1):
    name = [name[3] for name in cur.execute("SELECT * FROM user WHERE user_name =
'"+username+"' AND password_user = '"+passx+"""")]
        iduser = [iduser[0] for iduser in cur.execute("SELECT * FROM user WHERE
user_name = '"+username+"' AND password_user = '"+passx+"""")]
        now = datetime.datetime.now()
        dateTime = now.strftime("%d-%m-%Y %H:%M")
        sql = """ INSERT INTO session (iduser,date_session)
VALUES("""+str(iduser[0])+""","""+dateTime+""") """
        count = cur.execute(sql)
        conn.commit()
        tkMessageBox.showinfo("Success", "Welcome, "+name[0]+"")
        self.parent.destroy()
        root = Tk()
        menubar = Menu(root)
        aplikasi = Cabinet(root, "Digital Evidence Cabinet")
        root.config(menu=menubar)
        root.mainloop()
      else:
        tkMessageBox.showinfo("Error", "Wrong Username or Password !")
    except Exception as e:
```

Form Chain Of Custody

Form chain of custody merupakan hasil akhir dari sistem ini yang merupakan data-data

yang sudah diinputkan oleh *Investigator* dan *First Responder*. Data-data yang ditampilkan pada halaman pertama merupakan data yang sudah di validasi oleh *officer*. Terdapat 3 halaman dalam *form* ini, halaman pertama berisi data kasus dan data bukti fisik. Halaman kedua berisi data aktivitas yang dilakukan oleh pengguna sistem sedangkan pada halaman terakhir berisi validasi yang dilakukan oleh *officer*.

Halaman Pertama *Form chain of custody*

Halaman pertama berisi 3 informasi utama, yaitu: informasi terkait tempat kejadian perkara (*Crime Scene*), informasi bukti fisik (*Electronic Evidence*) dan informasi metadata dari hasil *image processing.* Halaman pertama ini hanya akan memiliki 1 halaman, hal ini karena data yang ditampilkan tidak dimungkinkan untuk bertambah

CHAIN OF CUSTODY OF PHYSICAL EVIDENCE

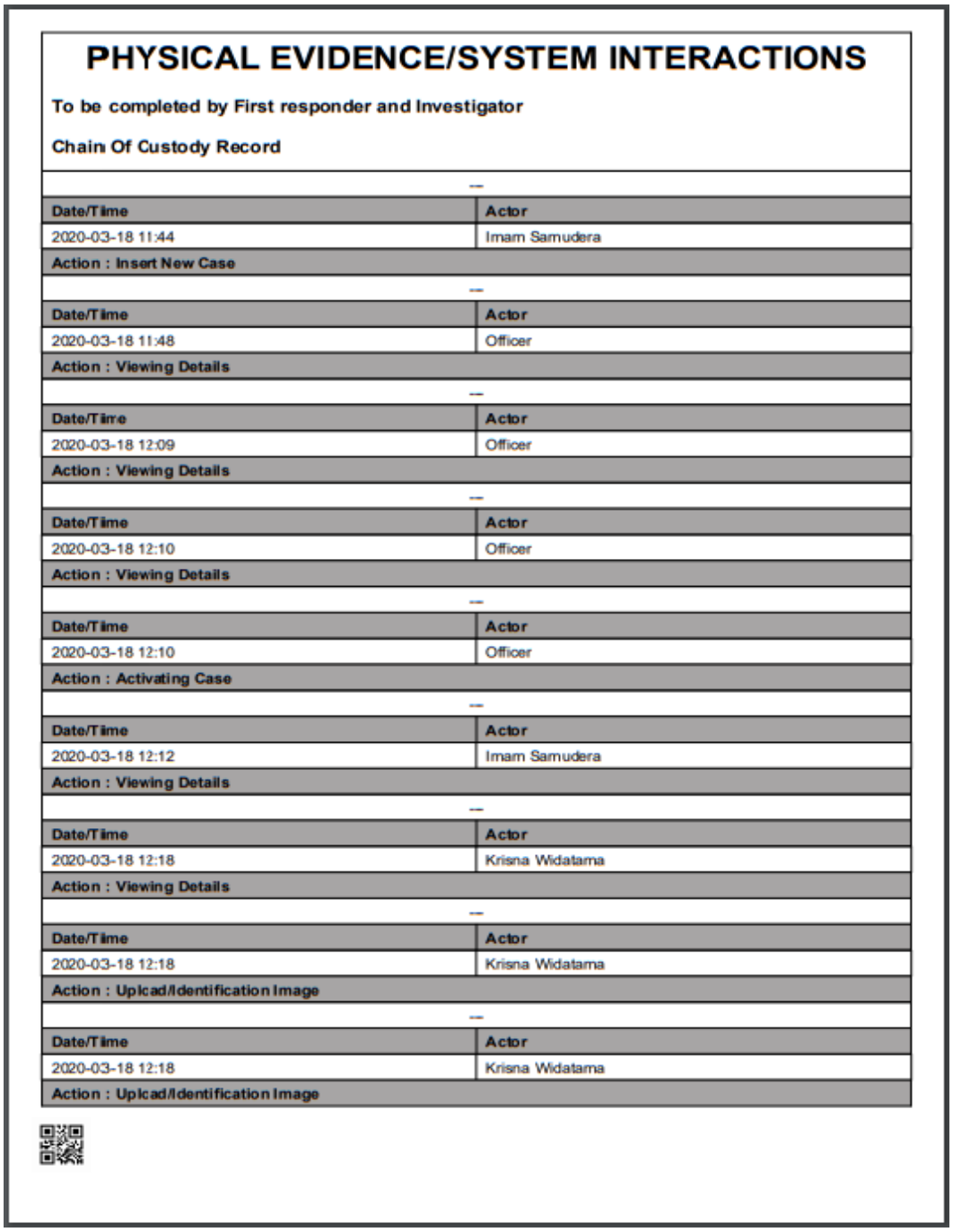
To be completed by First responder and Investigator

Crime Scene	
Case Name	Pembunuhan (Mutilasi)
Suspect:	Aji Notonegoro
Victim:	Basuki Kimono
Location	Pondok Indah, Jakarta Selatan
Time	2020-03-18 16:03
Tools (Live Forensics)	MobilEdit
Tools Description	Akuisisi Handphone
First Responder	Officer
Institution	UII
Electronic Evidence	
Register Number	Redmi 2
Type	Xiaomi Inc.
Model	SN09876567988
Manufacture	16 Gb
Serial Number	Smartphone
Foreclosure Reasons	SMS, Telepon
Metadata of Image Processed	
Evidence Number	180320_1
Case Number	PE18032002
File Name	IMG_0074 - Copy
Size (Byte)	244683
Hashing (SHA1)	c8114ba1fdbb6f4be53d44f0292a388d75cda510
Hashing (MD5)	c57ccf84b15f6704a21c9db2126c8974
Source	/Users/krisnawidatama/Documents/IMG_0074 - Copy.jpg
Cabinet Structure	images/IMG_0074 - Copy
Potential Information	SMS, Telepon
Status	ACTIVE
Validator	officer

Gambar 6. *Form chain of custody*

Halaman Kedua *Form chain of custody*

Dalam form ini terdapat catatan ketika pengguna sistem melakukan interaksi. Hal-hal yang tercatat adalah aktivitas yang dilakukan pengguna, waktu serta pengguna. Aktivitas-aktivitas yang dilakukan terkait dengan sistem adalah: memasukkan kasus baru (*Insert New Case)*, melihat detil kasus (*Viewing Details*), melakukan aktivasi kasus (*Activating Case*), analisis gambar (*Upload/Identification Image*), bukti fisik yang dianalisis (*Analyzed*), bukti fisik yang telah selesai dianalisis (*Returned*). Berikut adalah halaman kedua dari *form chain of custody*.



PHYSICAL EVIDENCE/SYSTEM INTERACTIONS

To be completed by First responder and Investigator

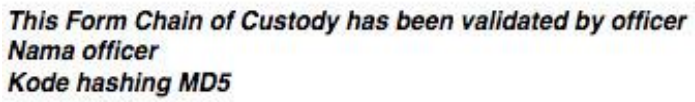
Chain Of Custody Record

Date/Time	Actor
2020-03-18 11:44	Imam Samudera
Action : Insert New Case	
Date/Time	**Actor**
2020-03-18 11:48	Officer
Action : Viewing Details	
Date/Time	**Actor**
2020-03-18 12:09	Officer
Action : Viewing Details	
Date/Time	**Actor**
2020-03-18 12:10	Officer
Action : Viewing Details	
Date/Time	**Actor**
2020-03-18 12:10	Officer
Action : Activating Case	
Date/Time	**Actor**
2020-03-18 12:12	Imam Samudera
Action : Viewing Details	
Date/Time	**Actor**
2020-03-18 12:18	Krisna Widatama
Action : Viewing Details	
Date/Time	**Actor**
2020-03-18 12:18	Krisna Widatama
Action : Upload Identification Image	
Date/Time	**Actor**
2020-03-18 12:18	Krisna Widatama
Action : Upload Identification Image	

Gambar 7. Halaman Kedua *Form chain of custody*

Halaman Ketiga *Form chain of custody*

Halaman terakhir adalah halaman yang berisi tandatangan *officer* yang sudah terenkripsi menggunakan metode enkripsi MD5. *Officer* dapat memasukkan tandatangan dalam dalam tipe data *string* melalui sistem ini. Halaman ini berfungsi untuk pengesahan bahwa aktivitas terkait bukti digital telah melalui proses validasi oleh *officer.*



This Form Chain of Custody has been validated by officer
Nama officer
Kode hashing MD5

Gambar 8. Halaman Validasi *Form chain of custody*

SIMPULAN DAN SARAN

Berdasarkan hasil yang telah diperoleh dari tahapan perancangan hingga implementasi, maka didapat beberapa kesimpulan

1. Terdapat 3 halaman pada formulir digital *Chain of Custody*. Halaman pertama memuat informasi utama terhadap kasus, tanggal penting dan data identitas bukti elektronik. Halaman setelahnya berisi interaksi antara pengguna dengan sistem atau pengguna dengan barang bukti fisik. Halaman terakhir berisi validasi terhadap *Form chain of custody* yang disahkan oleh Officer.
2. Peran utama sistem adalah dapat menyimpan data bukti fisik. Namun, sistem memiliki fitur untuk mengunggah *file* gambar yang langsung dianalisis secara otomatis oleh sistem.
3. Penyimpanan data bukti fisik menggunakan DBMS SQLite. Penyimpanan data menggunakan 4 tabel yang saling berelasi.

Adapun saran-saran yang perlu diberikan dalam hasil penelitian ini adalah penyimpanan data yang ada pada bukti fisik masih menggunakan DBMS sehingga data bukti fisik yang tersimpan masih terlihat. Pengembangan selanjutnya difokuskan terhadap keamanan data yang tersimpan baik menggunakan metode enkripsi maupun metode lainnya.

Penyimpanan bukti fisik masih yang ada pada penelitian ini masih merupakan bagian terpisah dari penyimpanan bukti digital. Diperlukan satu sistem terintegrasi antara sistem penyimpanan bukti fisik dengan bukti digital.

DAFTAR PUSTAKA

[1] J. Ćosić, Z. Ćosić, and M. Bača, "An ontological approach to study and manage digital chain of custody of digital evidence," *J. Inf. Organ. Sci.*, vol. 35, no. 1, pp. 1–13, 2011.

[2] T. F. Gayed, H. Lounis, M. Bari, and DUMMY, "Representing and Publishing Cyber Forensic Data and its Provenance Metadata : From Open to Closed Consumption," *Int. J. Adv. Intell. Syst*, vol. 7, no. 3, pp. 662–688, 2018.

[3] M. Harbawi and A. Varol, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I," *Int. Symp. Digit. Forensic Secur*, pp. 1–6, 2017.

[4] A. M. Marshall, *Digital Forensics : Digital Evidence in Criminal Investigation*. 2018.

[5] Y. Prayudi, A. Ashari, and T. K Priyambodo, "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody," *Int. J. Comput. Appl.*, vol. 107, no. 9, pp. 30–36, Dec. 2014.