MANAJEMEN BARANG BUKTI FISIK DAN *CHAIN OF CUSTODY (COC)* PADA PENYIMPANANAN LABORATORIUM FORENSIKA DIGITAL

Tino Feri Efendi
16917119

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2020

Lembar Pengesahan Pembimbing

MANAJEMEN BARANG BUKTI FISIK DAN *CHAIN OF CUSTODY (COC)* PADA PENYIMPANANAN LABORATORIUM FORENSIKA DIGITAL

Tino Feri Efendi
16917119

Yogyakarta, 9 Juni 2020

Pembimbing I	Pembimbing II
Dr. Ing. Ridho Rahmadi, M.Sc	Dr. Yudi Prayudi,M.Kom

Lembar Pengesahan Pembimbing

MANAJEMEN BARANG BUKTI FISIK DAN *CHAIN OF CUSTODY (COC)* PADA PENYIMPANANAN LABORATORIUM FORENSIKA DIGITAL

Tino Feri Efendi
16917119

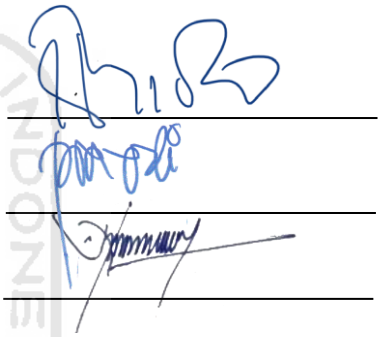
Yogyakarta, 9 Juni 2020

Tim Penguji,

Dr. Ing. Ridho Rahmadi, M.Sc
Ketua

Dr. Yudi Prayudi,M.Kom
Anggota I

Dr. Imam Riadi,M.Kom
Anggota II



Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

MANAJEMEN BARANG BUKTI FISIK DAN *CHAIN OF CUSTODY (COC)* PADA PENYIMPANANAN LABORATORIUM FORENSIKA DIGITAL

Kejahatan komputer memiliki 2 jenis barang bukti, yaitu: bukti fisik dan bukti digital. Penyimpanan pada bukti fisik membutuhkan sebuah ruang khusus yang dapat menampung bukti fisik tersebut. Namun dibutuhkan sebuah sistem yang dapat menyimpan dan mengelola bukti fisik tersebut. Permasalahan yang ada saat ini adalah tidak adanya konsep penyimpanan bukti fisik serta dokumentasinya (*Chain of Custody*). Manajemen barang bukti fisik diusulkan sebagai solusi untuk memecahkan masalah tersebut. Konsep ini berupa sebuah Sistem Manajemen Bukti Fisik dan *Chain of Custody* dengan mengambil analogi sebuah Data Inventory. Thesis ini memberikan solusi manajemen barang bukti fisik yang dibangun dan diimplementasikan di lingkungan Laboratorium Forensika Digital UII. Diharapkan dengan adanya konsep Manajemen Barang Bukti Fisik ini kontrol barang bukti fisik dan segala aktivitas yang berkaitan dengannya dapat terjaga serta terdokumentasi dengan baik.

Kata kunci

bukti fisik, *chain of custody*, data inventory

Abstract

MANAGEMENT OF PHYSICAL AND *CHAIN OF CUSTODY (COC)* OF EVIDENCE ON DIGITAL FORENSICS LABORATORY

Computer crime has 2 types of evidence, namely: physical evidence and digital evidence. Storage on physical evidence requires a special space that can hold physical evidence. However, a sistem that can store and manage physical evidence is needed. The current problem is the absence of a concept of storing physical evidence and its documentation (Chain of Custody). Physical Evidence Management is proposed as a solution to solve the problem. This concept is in the form of a Physical Evidence Management Sistem and Chain of Custody by taking the analogy of a Data Inventory. This research has successfully implemented the concept of Data Inventory for Management of Physical Evidence Sistem and Chain of Custody. It is expected that with the concept of Physical Evidence Management the control of physical evidence and all activities related to it can be maintained and well documented.

Keywords: digital forensics, physical evidence, chain of custody, inventory data

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 cipta yang 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, April 2020

Tino Feri Efendi, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari Bab 3

Sitasi publikasi 1

Kontributor	**Jenis Kontribusi**
Tino Feri Efendi	Mendesain eksperimen (60%) Menulis *paper* (70%)
Ridho Rahmadi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)
Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Halaman Kontribusi

Beberapa pihak yang berkontribusi dalam penyelesaian penyusunan tesis ini adalah:

1. Bapak Dr. Ing Ridho Rahmadi, S.Kom., M.Sc, Ph.D selaku pembimbing I dan Bapak Dr. Yudi Prayudi, S.Si., M.Kom selaku pembimbing II yang telah memberikan arahan, sehingga penyusunan tesis ini dapat terselesaikan.
2. Krisna Widatama, S.Kom., M.Kom., CEH., CHFI sebagai teman diskusi dalam penyusunan tesis ini.

Halaman Persembahan

Tesis ini kupersembahkan kepada orang-orang yang aku cintai karena Allah:

1. Orang tua.
2. Istri dan Saudara, terima kasih karena sudah ikut membantu merawat saya hingga menjadi seperi saat ini, semoga amal ibadahmu diterima Allah SWT.
3. Kawan kawan

Kata Pengantar

Syukur Alhamdulillah penulis ucapkan kepada kehadirat Allah SWT yang telah memberikan rahmat serta hidayahnya sehingga penulis dapat menyelesaikan laporan tugas akhir ini. Shalawat serta salam tidak lupa penulis ucapkan kepada Baginda Rasulullah SAW beserta keluarga dan para sahabatnya yang telah membawa ummat Islam menjadi sebuah peradaban yang mulia.

Laporan tugas akhir dapat disusun berkat adanya dukungan dan bantuan dari berbagai pihak. Melalui kesempatan ini penulis ucapkan terima kasih kepada pihak – pihak yang telah memberikan dukungan serta bantuannya yaitu:

1. Allah SWT atas segala limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir ini.
2. Kedua orangtuaku yang sangat aku sayangi dan banggakan: Bapak Sularwan dan Ibu Harti yang selalu memberikan doa dan dukungannya. Istriku Dewi Muliasari, S.Pd., M.Pd serta adikku Mayasari yang selalu setia menemani dan memberikan support.
3. Dr. Ing Ridho Rahmadi, M.Sc selaku pembimbing I dan Dr. Yudi Prayudi M.Kom, selaku pembimbing II, penulis ucapkan terima kasih atas kesabarannya membimbing penulis untuk menyelesaikan laporan tesis ini.
4. Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D. selaku ketua program pascasarjana Fakultas Teknologi Industri dan seluruh dosen pengajar yang telah memberikan ilmu, bimbingan dan arahan kepada penulis selama menimba ilmu di sana.
5. Semua pihak yang telah ikut membantu penulis untuk menyelesaikan penyusunan laporan tugas akhir ini.

Penulis menyadari bahwa dalam penyusunan laporan tugas akhir ini masih jauh dari sempurna. Dengan segala kerendahan hati penulis mengharapkan kritik dan saran agar bisa berguna untuk masa yang akan datang. Akhir kata semoga laporan tugas akhir ini dapat bermanfaat bagi kita semua.

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

APJII	- Asosiasi Penyedia Jasa Internet Indonesia
CoC	- Chain of Custody
DEMC	- Digital Evidence Management Framework
LPBD	- Lemari Penyimpanan Bukti Digital
PPBB	- Pejabat Pengelola Barang Bukti
RC4	- Rivest’s Chiper Version 4
XML	- eXtensible Markup Language
XHTML	- eXtensible Markup Language

BAB 1
Pendahuluan

1.1 Latar Belakang

Penyelidikan dan penyidikan tindak pidana merupakan suatu tanggung jawab yang besar yang diemban oleh seorang penyidik. Muaranya adalah terbuktinya sebuah tindak pidana di pengadilan dan memperoleh keputusan yang memiliki kekuatan hukum tetap. Namun permasalahan timbul ketika pembuktian tindak pidana tersebut tidak kuat, dan tidak dapat membentuk keyakinan Hakim bahwa telah terjadi suatu tindak pidana, yang bagi Hakim akan menjadi dasar adanya penjatuhan hukuman terhadap terdakwa.

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 bisa menyebabkan barang bukti menjadi tidak diterima yaitu proses ekstraksi atau pengambilan barang bukti yang tidak profesional, tidak ada kesesuaian antara perkara dengan alat bukti yang ditampilkan, atau hal - 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 tersebut 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 (documentation) bukti digital dan bukti fisik. Cosic, (2017) 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. Dalam hal ini, 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 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. Peraturan Kepala Kepolisian Republik Indonesia (Perkap) No. 10 Tahun 2009 Paragraf 3 telah mengatur segala hal yang berkaitan dengan barang bukti elektronik dan barang bukti digitaldi Indonesia. Paragraf tersebut berisi informasi tentang pemeriksaan barang bukti elektronik, telekomunikasi, komputer (Bukti Digital dan Bukti Fisik) dan penyebab proses elektrostatis.

Paragraf tersebut juga mengatur bahwa dalam tata cara pemeriksaan barang bukti, setelah barang bukti diperoleh, barang bukti kemudian dibungkus, diikat, disegel, diberi label dan dilakukan dokumentasi untuk kepentingan pengelolaan dan audit barang bukti. Sedangkan peraturan yang menjelaskan tentang tata cara pengelolaan barang bukti tertuang pada Perkap (Peraturan Kepala Kepolisian Indonesia) No. 10 Tahun 2010.

Salah satu klasifikasi barang bukti digital forensic yaitu Barang bukti elektronik. Barang bukti ini bersifat fisik dan dapat dikenali secara visual, sehingga investigator dan analis forensic harus sudah memahami barang bukti tersebut ketika sedang melakukan proses pencarian barang bukti di TKP. Jenis barang bukti elektronik ini berupa computer PC, laptop, notebook, tablet, handphone, flashdisk, floppydisk, hardisk, CD/DVD, route, switch, hub, kamera video, CCTV, kamera

digital, digital recorder, video player dan bukti fisik lainnya. Di antara perangkat yang tersedia, ponsel adalah salah satu perangkat yang paling sering digunakan. Ponsel memenuhi kebutuhan umum orang seperti komputer dengan lebih murah dan luas penggunaan internet. Dalam hal forensik digital, ponsel yang orang tidak terpisah dari diri mereka sendiri dapat berisi bukti penting (Casey, 2011). Dalam studi ini, bukti yang dapat diperoleh dengan memeriksa ponsel yang berisi data penting dalam forensik digital disajikan.

Pentingnya peran bukti fisik tersebut maka harus dibarengi dengan keamanan informasinya agar bisa diterima di pengadilan. Keamanan informasi merupakan ranah multi disiplin dalam konsentrasi pengembangan dan pelaksanaan dari berbagai mekanisme yang ada untuk menjaga informasi sesuai pada tempatnya. Mulai dari informasi tersebut dibuat, diproses, disimpan, dikirim, dan dihancurkan harus sesuai dengan haknya (Cherdantseva & Hilton, 2013). Secara umum, unsur keamanan informasi terdiri dari ketersediaan, integritas, dan kerahasiaan informasi tersebut. Keamanan informasi erat kaitannya dengan konsep manajemen resiko karena potensi ancaman yang diberikan akan menimbulkan kerentanan bagi aset organisasi tersebut. Kegagalan dalam mengamankan informasi dapat menimbulkan dampak bagi organisasi (Prayudi et al., 2019). Manajemen resiko dalam ranah keamanan informasi adalah serangkaian proses yang dilakukan untuk mengelola resiko mulai dari proses identifikasi sampai penanganan resiko (Basyarahil et al., 2017).

Salah satu hal terkait bukti fisik yaitu Chain of Custody. Chain of Custody adalah merupakan proses kronologi dan dokumentasi suatu kejadian, pengamanan, pengendalian, penahanan, dan pemindahan barang bukti fisik maupun elektronik. Chain of Custody (CoC) adalah sebuah barang bukti yang harus dijaga tingkat keasliannya sesuai dengan kondisi ketika pertama kali ditemukan. Dalam kasus hukum ketika dalam proses persidangan diperlukan untuk menunjukkan secara fisik barang bukti, maka pihak penegak hukum harus dapat menunjukkannya secara fisik barang bukti, maka pihak penegak hukum harus dapat menunjukkannya dengan kondisi yang sesuai dengan penjelasan pada materi dalam tuntutan.

Dalam sistem ini juga menggunakan metode Proses Image Recognition Based on Deep Learning menggunakan API Clarifai. Deep Learning adalah algoritma pembelajaran jaringan saraf multilayer yang muncul dalam beberapa tahun terakhir. Hasil percobaan menunjukkan bahwa pembelajaran yang mendalam memang memiliki kemampuan belajar fitur yang sangat baik. Tidak perlu mengekstrak fitur secara manual. Algoritma deep learning akan menggunakan API Clarifai untuk mendukung proses pengenalan gambar atau image recognition yang dibutuhkan pada identifikasi bukti.

Lebih lanjut Chain of Custody merupakan salah satu tahapan penting dari serangkaian proses investigasi terkait dengan dokumentasi barang bukti. Berdasarkan Ashcroft, Daniels, & Hart, (2004) 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.

Keterkaitan 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.

Hasil akhir dari penelitian ini adalah terciptanya sebuah sistem informasi manajemen yang dapat menyimpan data kasus dan data bukti fisik maupun file image yang diperoleh dari TKP. Sistem ini tidak membutuhkan web server untuk menggunakan database sehingga alokasi memori yang digunakan RAM menjadi lebih kecil. Karena masih menggunakan DBMS, data yang tersimpan masih dapat dilihat dan dipindahkan secara illegal sehingga manajemen keamanan masih perlu dievaluasi kambali pada penelitian yang akan datang.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan masalah yaitu: Bagaimana membangun sistem aplikasi yang bisa mengelola barang bukti fisik

seperti pada perpustakaan dan sistem tersebut dapat memberikan hasil berupa Chain of Custody sebagai salah satu penguat keabsahan barang bukti fisik di Pengadilan.

1.3 Batasan Masalah

Batasan-batasan masalah pada penelitian ini adalah:

1. Proses pengelolaan transaksi peminjaman dan pengembalian barang bukti fisik yang masih dilakukan secara manual.
2. Proses kontrol bukti fisik yang masih dilakukan secara manual.
3. Proses pencarian bukti fisik yang masih dilakukan secara manual.
4. Proses Image Recognition Based on Deep Learning menggunakan API Clarifai.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu:

1. Membangun sistem manajemen yang dapat menyimpan data kasus dan data bukti fisik yang diperoleh dari TKP.
2. Membangun sistem yang mampu menampilkan output berupa `dokumen chain of custody antara bukti fisik dan kasus.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini adalah sebagai berikut:

1. Membantu pihak-pihak terkait untuk menyimpan bukti fisik secara sistematis.
2. Membantu pihak-pihak terkait untuk mendokumentasikan bukti fisik sehingga dapat dipertanggungjawabkan secara hukum di pengadilan.

BAB 2
Tinjauan Pustaka

2.1 Pendahuluan

Terdapat beberapa penelitian yang telah dilakukan berkaitan dengan *CoC.* Penelitian pertama yang dilakukan oleh (Giova, 2011) yang mengangkat permasalahan tentang perlunya pengembangan *CoC* pada investigasi forensik sistem digital elektronik. Dalam penelitiannya ia menulis bahwa saat ini jumlah data yang tercipta semakin banyak dan tersebar melalui berbagai macam perangkat elektronik baik melalui komputer, server, jaringan publik dan pribadi, ponsel dan berbagai macam teknologi tinggi. Hal ini membuat investigator harus mengakuisisi dan menganalisa bukti digital dalam jumlah besa

Penelitian kedua dilakukan oleh (Gayed, Lounis, & Bari, 2012) yang mengangkat isu tentang menyajikan dan meningkatkan *CoC* menggunakan *Semantic Web* yang berkaitan tentang penulisan informasi yang lengkap pada *CoC* terhadap bukti digital dalam rangka memecahkan masalah yang dihadapi. Penelitian ketiga dilakukan oleh (Ćosić, Ćosić, & Bača, 2011) mengangkat isu tentang pengelolaan *CoC* pada dengan pendekatan ontologis pada bukti digital. Penelitian keempat dilakukan oleh (Prayudi & Azhari, 2015) yang mengangkat isu tentang tantangan yang akan dihadapi dalam *CoC* serta cakupan penelitian yang dapat dilakukan terhadap masalah pada *CoC*. Penelitian kelima dilakukan oleh (Prayudi, Ashari, & Priyambodo, 2014) yang mengangkat isu tentang pembuatan *digital evidence cabinet* sebagai pendekatan baru dalam penanganan barang bukti digital. Rangkuman dan perbandingan terhadap penelitian yang dilakukan sebelumnya dapat dilihat pada tabel 2.1.

Tabel 2.1 Perbandingan Penelitian Terdahulu

No.	Paper	Isu	Solusi	Metode	Hasil
1.	(Prayudi et al., 2014)	Penanganan pada bukti digital.	Pembuatan model Digital Evidence Cabinet.	Pembuatan Digital Evidence Cabinet menggunakan 3 pendekatan, yaitu: *digital evidence management frameworks, digital evidence bags* dan *secure communication*.	Tersimpannya bukti digital pada digital evidence cabinet dan pembatasan akses terhadap bukti digital.
2.	(Prayudi, 2014)	Penanganan *chain of custody* pada bukti digital.	Penggunaan *tools* tertentu.	1. Pendekatan *evidence oriented design* yaitu *tools* yang mampu mendukung aktifitas proses investigasi. 2. Pemodelan yang telah digunakan dalam forensika umum yaitu kantung barang bukti digital (*sealed digital evidence bag*).	Tools yang memiliki kemampuan untuk proses investigasi.
3.	(Prayudi & Azhari, 2015)	Kesenjangan penanganan bukti fisik dan bukti digital.	Membuat framework yang mampu menangani bukti fisik dan bukti digital.	1. Penggunaan konsep DEMC (Digital Evidence Management Framework). 2. Penerapan UML dan UMML dengan tujuan untuk menyajikan data proses perencanaan (*planning*), *performing* dan aktivitas forensika yang terjadi.	Integritas dan kredibilitas prosedur dalam penanganan *chain of custody* pada bukti digital.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
				3. Pendekatan terhadap format forensik yang digunakan saat ini. Pendekatan ini ditujukan untuk memberikan solusi penyimpanan dan metadata terhadap format tersebut.	
4.	(Giova, 2011)	Standar kualitas bukti digital untuk diajukan ke pengadilan.	Pengembangan format AFF4 (*Advanced Forensic Format*) sebagai *tool* forensika dan penggunaan RDF (*Resource Description Format*).	RDF digunakan untuk membaca metadata pada bukti digital berformat AFF4 dalam bentuk struktur bahasa XML. Sehingga metadata pada bukti digital dapat dibaca oleh pengguna. Struktur XML yang terbentuk dalam RDF disusun dengan menggunakan format Subject, Attribute, Value.	Bukti digital dapat diterima di pengadilan, karena struktur XML yang dibuat dapat menyesuaikan dengan kebutuhan peraturan hukum di negara tertentu.
5.	(Gayed, Lounis, & Bari, 2012)	Transformasi *chain of custody* dari bentuk dokumen ke bentuk digital.	Penggunaan *semantic web* untuk merepresentasikan informasi *chain of custody*.	*Semantic web* digunakan untuk mengatur format struktur XML pada RDF.	Informasi *Chain of custody* bukti digital dapat dilihat pada halaman web.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
6.	(Ćosić et al., 2011)	Pengelolaan pada bukti digital dengan *tools investigator*.	Pendekatan ontologis terhadap *bukti digital.*	Membuat hirarki pada bukti digital, berikut adalah penjelasannya: 1. *Characteristic*, yaitu sumber dan tipe. Sumber berupa: a. *Personal Computer*, yaitu: Laptop, Netbooks, Notebooks, Server, Desktop. b. Cloud (penyimpanan virtual), yaitu: *magnetic*, *flash, optical*. c. LSDD (*Large Scale Digital Devices*): kamera digital, telepon, dll. d. *Device* yaiut : *input device dan output device.* e. SSDD*(Small Scale Digital Devices)* yaitu: *flashdisk,memory card.* Sedangkan *type* berupa: *Original, best copy, working copy*.	Pemahaman terhadap pengelolaan bukti digital yang melibatkan 2 domain, yaitu: *forensic investigator* terhadap bukti digital dan *forensic investigator* terhadap *tools* yang digunakan untuk memperoleh bukti digital.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
				2. Dynamics (hal-hal apa saja yang berpengaruh serta jenis bukti digital), dibagi menjadi 3 yaitu: *equipment* (*hardware and software*) dan *human* dan *natural dynamics.* *3. Human dynamics* (orang terlibat secara langsung maupun tidak langsung terhadap kasus yang sedang dihadapi) yaitu: a. *First responder.* b. Investigator. c. *Prosecution* (pihak penuntut). d. *Court* (pihak pengadilan). e. *Victim* (korban). f. *Suspect* (Tersangka). *g. Court expert witness*(saksi ahli pengadilan) h. *Law personal* *Natural dynamics* (hal-hal yang dapat merusak bukti digital): a. *Earthquake* (gempa bumi). b. *Fire* (kebakaran). c. *Weather* (Cuaca).	

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
				4. *Factors* (jawaban atas pertanyaan *what, where, who, why, when* dan *how* terhadap bukti digital). a. *What,* jenis bukti digital yang diperoleh. b. *Where,* dimana lokasi bukti digital. c. *Who,* siapa saja yang terlibat pada bukti digital tersebut. d. *When,* kapan bukti digital tersebut diperoleh. e. *How,* bagaimana bukti tersebut diperoleh. 5. *Institutions,* tempat diperolehnya bukti digital. 6. *Integrity,* penjelasan mengenai *tools* dan metode yang digunakan untuk memperoleh bukti digital.	

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
7.	(Widjaja & Kalabadzi, 2017)	Penerapan metode enkripsi untuk pengamanan pengiriman informasi pada Perusahaan Packet Sistems Indonesia	Penggunaan metode algoritma RSA dan RC4 dengan menggunakan bahasa pemrograman PHP	Implementasi algoritma RSA dan RC4 kedalam bentuk bahasa pemrograman PHP. Pengiriman teks maupun *file* harus melalui enkripsi terlebih dahulu, setelah terenkripsi, *file* maupun teks dapat dikirim melalui email.	*File* hasil enkripsi dalam bentuk ekstensi .psi. Terdapat 9 jenis *file* yang berhasil dienkripsi, yaitu: .rar, .docx, .mp3, .pdf, .png, .jpg, .xlsx, .vsd, .mp4.
8.	Tesis : Konsep XML untuk Mendukung Digital Chain of Custody (Widatama, 2018)	1. Penyimpanan bukti digital pada perangkat komputer. 2. Penyimpanan metadata bukti digital.	1. Penyimpanan secara terstruktur dengan model lemari. 2. Pembagian 3 aktor dalam interaksi dengan bukti digital (Officer, First Responder, Investigator) 3. Penyimpanan metadata bukti digital dengan bahasa XML. 4. Enkripsi XML tersebut.	1. Menggunakan bahasa pemrograman Python dalam pembuatan sistem penyimpanan bukti digital. 2. Penyimpanan bukti digital terstruktur menggunakan 3 tingkatan : Cabinet, Rack, Bag. 3. Menggunakan XML sebagai bahasa utama dalam penyimpanan metadata bukti digital serta pengguna. 4. Menggunakan algoritma ARC4 sebagai metode untuk melakukan enkripsi metadata bukti digital maupun data pengguna.	1. Penyimpanan bukti digital berdasarkan kasus. 2. Metadata bukti digital serta data pengguna terenkripsi dan menjadi sulit terbaca maupun diubah jika tidak mengetahui ‘kunci’ pembuka enkripsinya.

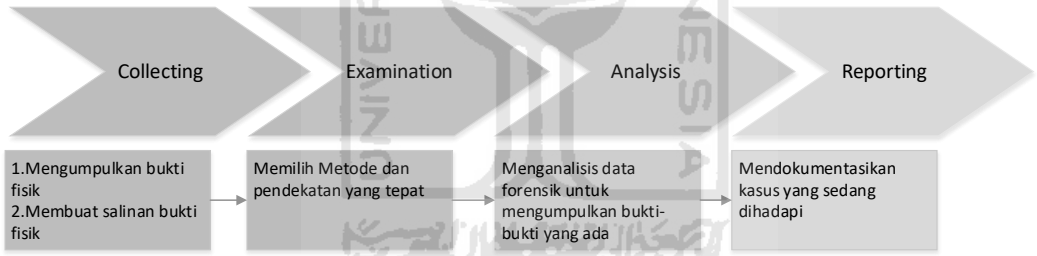
Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
9.	Konsep Penelitian	Manajemen Barang Bukti Fisik Dan Chain of Custody (CoC) Pada Penyimpananan Laboratorium Forensika Digital	Membangun sistem informasi yang dimodelkan seperti data inventory pada bukti fisik. Serta pembatasan	Penyimpanan bukti elektronik dimana informasi bukti fisik dan *chain of custody* disimpan pada sistem informasi manajemen.	Sistem informasi dapat menambah, mengontrol dan memberikan laporan *CoC.*
		Penyimpanan bukti fisik hingga saat ini masih belum terpusat pada sistem tertentu. Hal ini membuat bukti fisik untuk dimanipulasi yang dapat membuat bukti fisik tersebut tidak bisa dijadikan sebagai bukti dalam persidangan. Hingga saat ini, belum ada manajemen pengelolaan dan kontrol bukti fisik yang terpusat pada sebuah sistem untuk mendukung form *chain of custody*. Berdasarkan permasalahan-permasalahan ini, saya mengusulkan sebuah sistem informasi manajemen yang dapat menyimpan data kasus dan data bukti fisik yang diperoleh dari TKP. Selain dapat menyimpan data dan mengontrol bukti fisik, sistem informasi manajemen ini juga dapat menampilkan output berupa dokumen *chain of custody* antara bukti fisik dan kasus yang sedang ditangani.			

2.2 Bukti Digital

Forensika digital dan bukti digital memiliki keterkaitan, namun keduanya memiliki definisi yang berbeda. 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 (Morioka & Sharbaf, 2016). Dalam prosedur forensika digital, terdapat prosedur dasar yang sering digunakan, yaitu: pengumpulan barang bukti (*collection*), perawatan barang bukti (*preservation*), *verification, analysis, interpretation, documentation* dan presentasi hasil di pengadilan (*presentation*).

Pendapat lain tentang prosedur forensika digital, bahwa secara umum terdapat 4 proses utama dalam forensika digital, yaitu: *collection, examination, analysis* dan *reporting* (Dogan & Akbal, 2017), berikut adalah proses dari forensika digital:



Gambar 2.1 Proses Utama Forensika Digital

Berikut adalah penjelasan proses utama dalam forensika digital pada gambar 2.1.

1. *Collection,* bukti digital dikumpulkan dan dilakukan proses *imaging.*
2. *Examination,* memilih dan menentukan metode pendekatan yang tepat.
3. *Analysis,* langkah untuk menganalisis data forensik untuk mengumpulkan bukti-bukti yang ada.
4. *Reporting,* mendokumentasikan kasus yang sedang dihadapi.

Sedangkan definisi bukti digital menurut (Harbawi & Varol, 2017) adalah jejak yang dinginkan maupun tidak diinginkan yang berasal dari perubahan data

digital pada perangkat elektronik. Berdasarkan sumbernya, bukti digital terbagi menjadi 2 kategori (Marshall, 2008), yaitu *closed sistem* dan *open sistem. Closed sistem* merupakan sistem yang pernah terkoneksi internet. Artinya, sistem tersebut sangat terisolasi dan hanya terhubung dengan sistem pada komputer yang lain. Berbeda dengan *closed sistem, open sistem* merupakan sistem yang terhubung dengan internet meskipun sistem tersebut tidak terhubung dengan sistem pada komputer lain, contohnya ketika seseorang menghubungkan laptop pada WiFi.

Menurut ACPO (*Association of Chief Police Officer*) terdapat 4 prinsip dalam penanganan bukti digital. Berikut adalah 4 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.

Barang bukti kasus cybercrime terbagi menjadi 2, yaitu barang bukti digital dan barang bukti elektronik. Barang bukti elektronik merupakan barang bukti yang berupa bentuk fisik dari perangkat elektronik dan juga dapat berupa media penyimpanan, sedangkan barang bukti digital merupakan barang bukti berupa file dokumen, file history, atau file log yang berisi tentang data-data terkait

dengan suatu kasus cybercrime dan dapat dijadikan sebagai informasi pendukung pengambilan keputusan dalam penyelidikan suatu kasus cybercrime (Riadi, Umar, & Nasrulloh, 2018)

Tabel 2.2 Perbedaan Bukti Fisik dan Bukti Digital

No.	Perbedaan	Bukti Fisik	Bukti Digital
1.	Kontrol Terhadap Barang Bukti	Pencatatan dan kontrol terhadap barang bukti mudah dilakukan.	Kemudahan dalam hal modifikasi, *copy* hapus dan transfer dokumen digital membuat barang bukti sehingga sulit untuk di kontrol.
2.	Bentuk Barang Bukti	Berupa barang bukti yang berwujud atau dengan kata lain memiliki wujud yang nyata berupa media penyimpanan.	Berupa file dokumen, *file history* atau *file log*.
3.	Bentuk Penyimpanan	Membutuhkan ruang khusus yang dapat menampung bukti fisik.	Membutuhkan ruang penyimpanan sistem yang dapat menjaga agar data tidak berubah.

2.3 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 (Prayudi et al.,

2014) 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.

2.4 Sistem Informasi

Sistem informasi dapat diartikan sebagai kerangka kerja yang mengkoordinasikan sumber daya manusia atau komputer untuk mengubah masukan menjadi informasi, guna mencapai sasaran. Sistem manajemen inventory secara online dapat melakukan pengawasan menjadi lebih baik. Lemahnya pengawasan menjadi dampak buruk bagi manajemen sehingga pelaporan penerimaan atau pengeluaran barang dan pengawasan terhadap penggunaan barang menjadi terhambat. Tujuan penelitian ini adalah membuat sistem informasi manajemen inventory menggunakan Framework EasyUI yang dapat diakses dan diawasi secara online. Perancangan sistem menggunakan Unified ModellingLanguage, bahasa pemrograman PHP dan database SQLite. Penelitian ini menghasilkan sistem informasi manajemen inventory yang memberikan informasi stok secara real-time dan laporan semester penerimaan dan pengeluaran barang, sehingga proses pelaporan dan pengontrolan informasi stok dapat dilakukan dengan baik.

2.5 SQLite

SQLite adalah sebuah pustaka dalam proses yang mengimplementasikan mesin database SQL yang bersifat mandiri, tidak ada konfigurasi, tanpa server, dan transaksional. Kode sumber untuk SQLite ada di domain publik dan gratis untuk tujuan pribadi dan komersial. SQLite memiliki pengikatan ke beberapa bahasa pemrograman seperti C, C++, BASIC, C#, Python, Java dan Delphi. SQLite saat ini ditemukan di lebih banyak aplikasi, termasuk beberapa proyek profil tinggi.

SQLite adalah mesin database SQL tertanam dan tidak memiliki proses server terpisah seperti kebanyakan database SQL lainnya. SQLite membaca dan menulis langsung ke file disk biasa. SQLite adalah perpustakaan yang kompak, ukuran Perpustakaan bisa kurang dari 500KB, tergantung pada platform target dan pengaturan optimasi compiler. SQLite juga dapat dibuat untuk berjalan dalam ruang memori minimal (4KiB). SQLite pilihan mesin database populer pada gadget dibatasi memori seperti ponsel, PDA, dan MP3 player. SQLite umumnya berjalan lebih cepat.

Keuntungan dari SQLite dibandingkan dengan SQL dan MySQL yaitu:

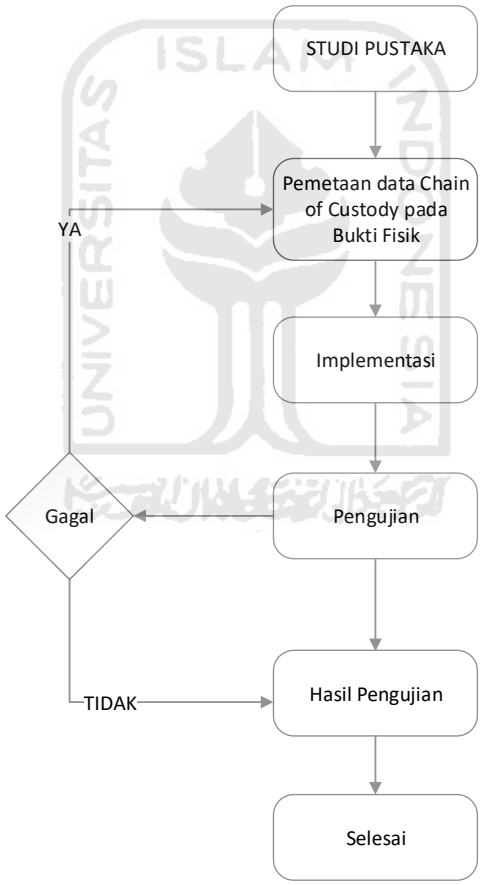
1. SQL Server dan MySQL adalah berbasis server tetapi SQLITE adalah berbasis file,
2. SQLite adalah sistem manajemen database relasional yang tertanam sedangkan SQL adalah bahasa query, MySQL adalah client sistem manajemen database relasional.
3. Karena SQLite adalah basis data yang ringan, sistem berkas langsung yang menggunakan sintaks SQL. SQLite juga tidak memerlukan server basisdata khusus atau apapun.
4. Penting untuk dicatat bahwa SQL Server dan MySQL mendukung prosedur yang tersimpan tetapi SQLite tidak.

2.6 Deep Learning

Deep Learning adalah algoritma pembelajaran jaringan saraf multilayer yang muncul dalam beberapa tahun terakhir. Ini telah membawa gelombang baru ke pembelajaran mesin, dan membuat kecerdasan buatan dan interaksi manusia-komputer maju dengan langkah besar. Hasil percobaan menunjukkan bahwa pembelajaran yang mendalam memang memiliki kemampuan belajar fitur yang sangat baik. Tidak perlu mengekstrak fitur secara manual. Pembelajaran mendalam dapat mempelajari lebih banyak fitur-fitur alami dari data (Wu & Chen, 2016). Algoritma deep learning akan menggunakan API Clarifai untuk mendukung proses pengenalan gambar atau image recognition yang dibutuhkan pada identifikasi bukti.

BAB 3
Metodologi Penelitian

Bab ini berisi tentang penjabaran skema penelitian dengan menjelaskan setiap alur proses penelitian secara struktur dan sistmatis. 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. Alur penelitian pada bab ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Alur Penelitian

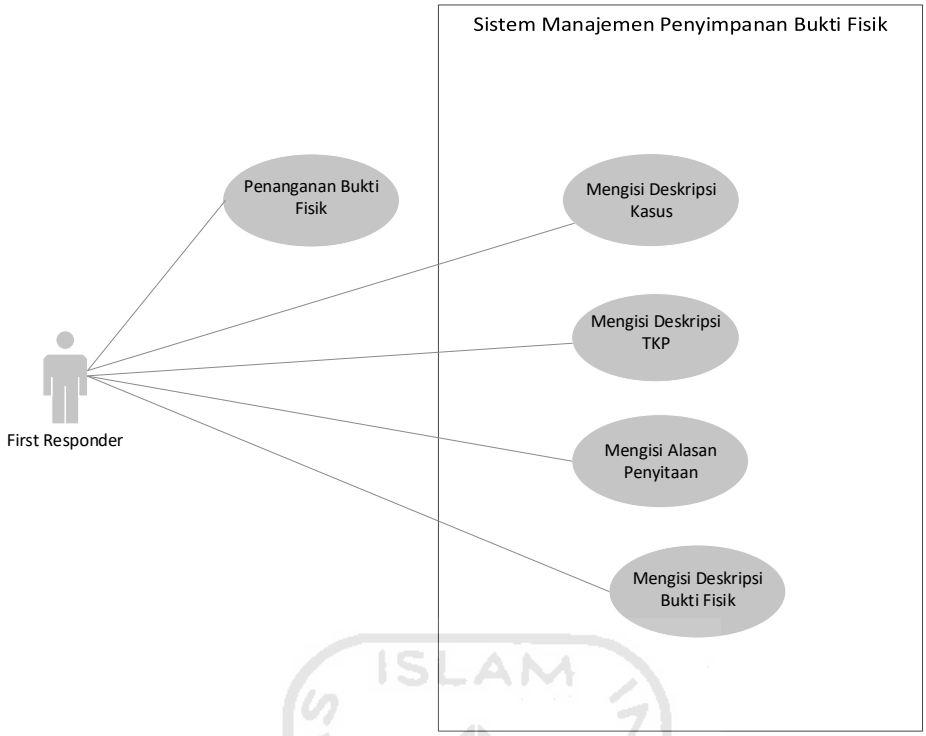
3.1 Studi Pustaka

Studi pustaka dilakukan saat langkah awal penelitian. Studi pustaka merupakan langkah awal dimana informasi dari berbagai sumber yang sesuai dengan permasalahan yang akan diteliti dikumpulkan. Jurnal ilmiah merupakan salah satu sumber yang dapat digunakan untuk acuan dalam penelitian, sumber-sumber yang lain juga bisa didapatkan lewat internet. Sumber-sumber informasi tersebut harus memiliki keterkaitan dengan penelitian ini. Sumber-sumber studi pustaka juga dapat diperoleh melalui lisan yaitu dengan menghadiri seminar-seminar ilmiah yang diadakan oleh universitas maupun instansi yang bergerak dibidang akademik atau penelitian.

Pada penelitian ini informasi yang dibutuhkun adalah informasi tentang konsep dasar penyimpanan pada CoC. Informasi yang seharusnya tersimpan pada sistem penyimpanan barang bukti fisik. Selain daripada itu, juga tentang pembagian tugas terhadap penanganan dan pengamanan kasus kejahatan komputer yang marak terjadi pada era ini.

3.2 Pembagian Hak Akses terhadap Sistem

Setelah studi pustaka dilakukan dan informasi-informasi dari berbagai sumber yang terkait dengan penelitian ini didapatkan, tahapan selanjutnya ialah 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 penenlitian tersebut dengan baik. Pembagian hak otorisasi *first responder* terhadap sistem manajemen terkait dengan penanganan bukti dijelaskan melalui *use case* pada gambar 3.2 berikut.



Gambar 3.2 *Use Case* Pembagian Hak Otorisasi pada *First Responder*

Gambar 3.2 menjelaskan bahwa *First responder* berperan sebagai orang yang menangani dan mengamankan barang bukti fisik. *First responder* tidak hanya berperan dalam penanganan dan pengamanan barang bukti fisik, tapi juga memiliki aktivitas lain terkait dengan sistem manajemen yang akan dibuat. Tabel 3.1 berikut menjelaskan tentang aktivitas first responder yang terkait dengan sistem.

Tabel 3.1 Aktivitas First Responder pada sistem

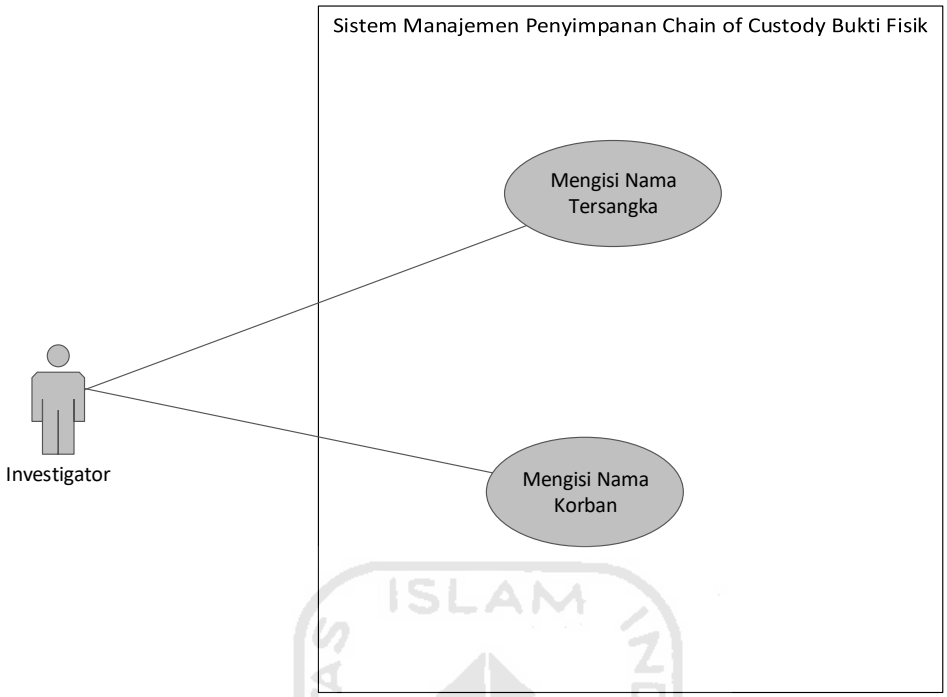
No.	**Jenis Aktivitas**	**Rincian Aktivitas**
1.	Mengisi Deskripsi Kasus	Mengisi nomor kasus
		Mengisi nama kasus
		Memilih investigator
2.	Mengisi Deskripsi TKP	Mengisi nama alat untuk akuisisi bukti digital dari bukti fisik

Tabel 3.2 Aktivitas First Responder pada system (Tabel Lanjutan)

No.	Jenis Aktivitas	Rincian Aktivitas
		Mengisi deskripsi alat untuk akuisisi bukti digital dari bukti fisik
		Mengisi waktu olah TKP
		Mengisi lokasi olah TKP
3.	Mengisi alasan penyitaan bukti fisik	Mengisi alasan penyitaan barang bukti fisik
		Mengisi bukti yang ingin didapat dari bukti fisik
4.	Mengisi deskripsi bukti fisik	Mengisi nomor registrasi bukti fisik
		Mengisi model bukti fisik
		Mengisi nomor seri bukti fisik
		Mengisi tipe bukti fisik
		Mengisi nama vendor pembuat bukti fisik
		Mengisi kapasitas penyimpanan bukti fisik

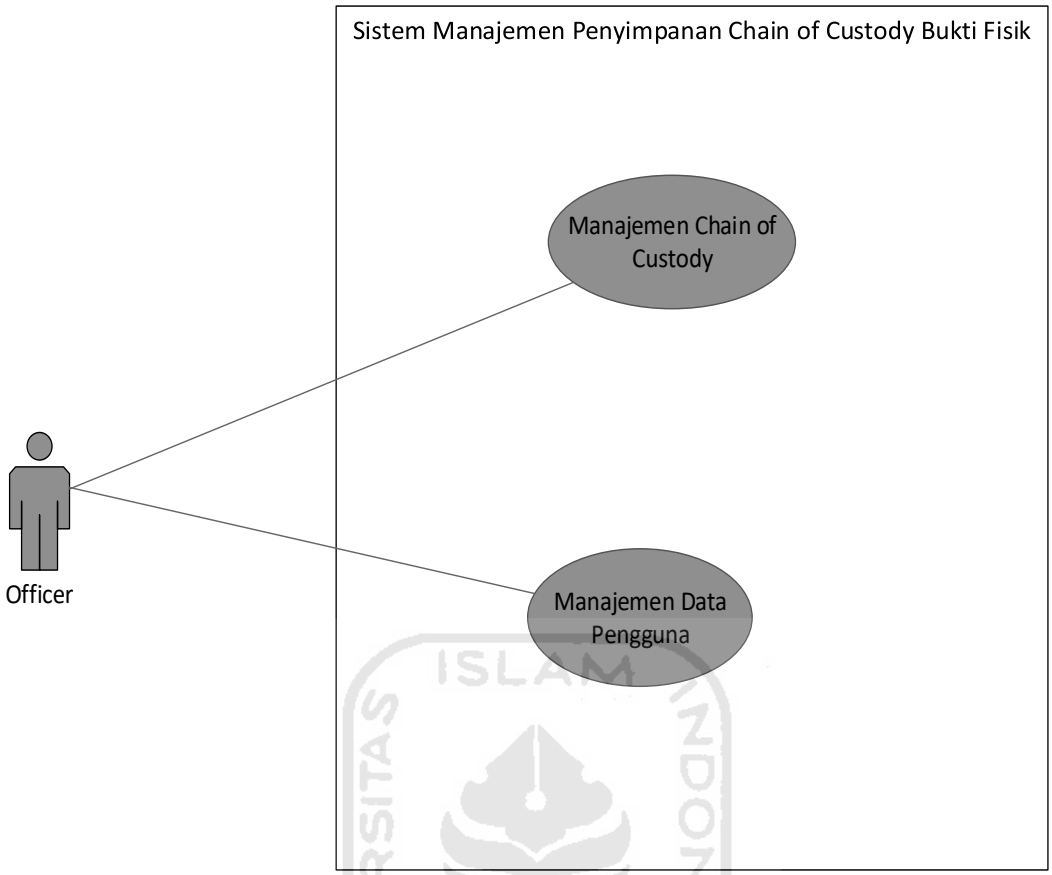
Selain aktivitas yang telah dijabarkan pada tabel 3.1, first responder juga dapat mengganti akun dengan akun lain yang sudah terdaftar pada sistem. Akun tersebut digunakan untuk masuk kedalam sistem. Akun tersebut berupa informasi tentang instansi tempatnya bekerja, username dan password.

Investigator adalah orang yang melakukan proses investigasi terhadap bukti bukti digital (hasil dari akuisisi terhadap bukti fisik) pada kasus kejahatan komputer. 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 3.3 berikut menunjukkan pembagian hak otorisasi antara investigator dengan sistem manajemen.



Gambar 3.3 *Use Case* Pembagian Hak Otorisasi pada *Investigator*

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 3.4 *Use Case* Pembagian Hak Otorisasi pada *Officer*

Gambar 3.4 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*. Tabel 3.2 berikut berisi tentang detil aktivitas yang dapat dilakukan officer terhadap sistem.

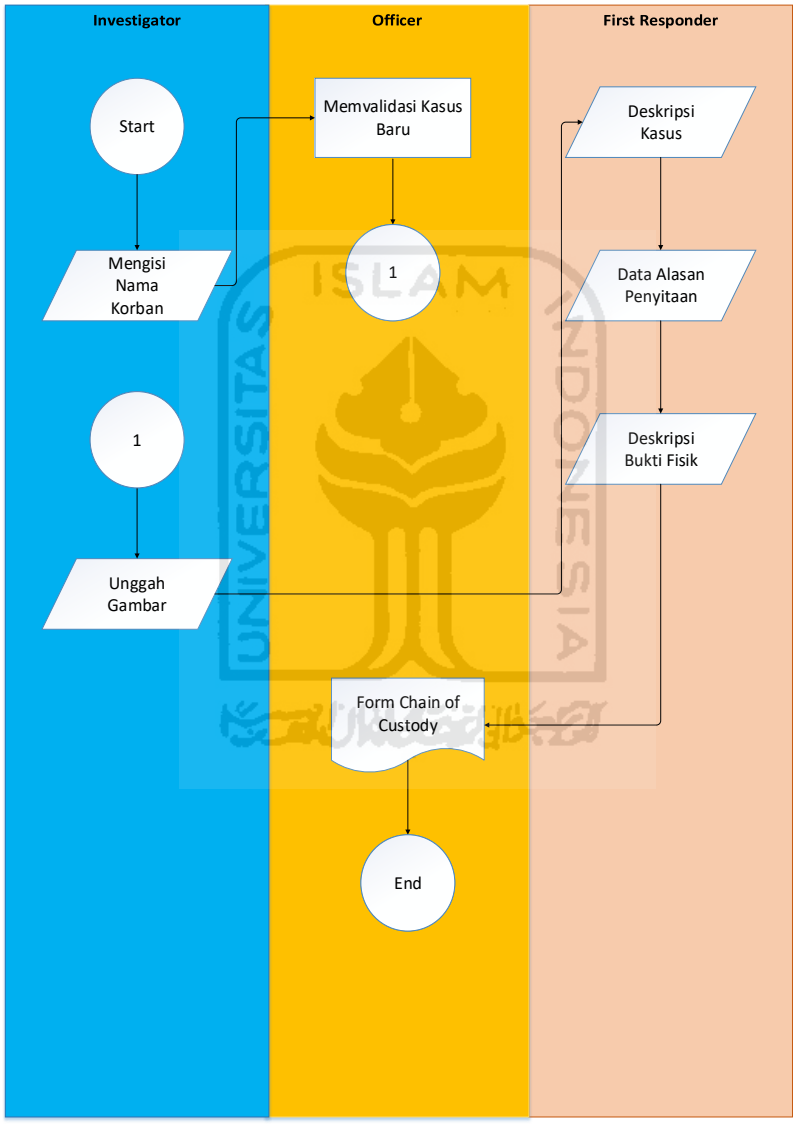
Tabel 3.3 Detil Aktivitas Officer Terhadap Sistem

No.	Jenis Aktivitas	Rincian Aktivitas
1.	Manajemen data Chain of Custody	Melakukan validasi data kasus yang masuk
		Melakukan validasi terhadap data kasus yang telah diubah
		Menghapus data kasus
		Mencetak form Chain of Custody
2.	Manajemen data pengguna	Menambahkan data investigator dan first responder
		Merubah username dan password dari investigator dan first responder
		Mengisi waktu olah TKP
		Mengisi lokasi olah TKP

3.3 Alur Penanganan Kasus Kejahatan Komputer

Terdapat beberapa tahapan yang harus dilakukan oleh *officer, first responder* dan *investigator* saat akan menyimpan data CoC dengan menggunakan sistem. Tahapan tersebut dilakukan secara urut dan terstruktur, hal ini bertujuan agar *form chain of custody* yang dibuat dapat dipertanggungjawabkan di pengadilan. Alur penanganan bukti fisik dimulai saat *investigator* melakukan pengisian data nama *korban* ke dalam sistem. Setelahnya *officer* akan melakukan pemeriksaan terhadap data kasus baru yang dimasukkan. Setelah dinyatakan benar dan sah, maka officer akan melakukan validasi terhadap isian data tersebut. Selanjutnya, investigator akan mengunduh hasil validasi dari *officer* untuk dianalisis, lalu data kembali di unggah. Data-data tersebut diunduh dan diisi oleh first responder karena ia yang mengamankan kondisi TKP termasuk barang bukti fisik yang diperoleh. Data-data TKP tersebut berupa: nama alat, deskripsi alat, waktu olah TKP dan lokasi TKP. Setelahnya, sistem akan melakukan penyimpanan sementara data tersebut, namun tidak menampilkannya. Berikutnya first responder akan mengisi data alasan penyitaan bukti fisik tersebut. Data alasan

penyitaan tersebut berupa: alasan penyitaan dan bukti. Data terakhir yang dimasukkan oleh first responder adalah data deskripsi bukti fisik. Data ini berupa deskripsi yang bersifat unik atau data yang hanya dimiliki oleh *satu* buah barang bukti saja meskipun jenisnya sama, contohnya nomor seri bukti fisik. Data deskripsi tersebut berupa: nomor registrasi, model, nomor seri, tipe, nama vendor pembuat dan kapasitas penyimpanan. Gambar 3.5 menunjukkan alur penanganan sebuah kasus kejahatan komputer.



Gambar 3.5 Alur Penanganan Kasus Kejahatan Komputer

3.4 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. Gambar 3.6 menunjukkan konsep desain *form chain of custody*.

CHAIN OF CUSTODY OF PHYSICAL EVIDENCE

To be completed by First responder and Investigator

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**
Tolls (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**
Foreciosure Reasons	**Alasan Penyitaan Bukti Elektronik**

Gambar 3.6 Konsep Desain *Form Chain of Custody*

Berbeda dengan halaman pertama yang jumlah datanya tidak akan bertambah, halaman kedua dapat dimungkinkan untuk bertambah jumlah datanya (dapat memiliki lebih dari 1 halaman). Hal ini karena halaman ini merupakan halaman yang mencatat segala aktivitas yang dilakukan pengguna saat berinteraksi dengan sistem. Interaksi tersebut berupa: validasi yang dilakukan oleh officer, isian data yang telah dimasukkan oleh first responder dan investigator. Halaman ini disebut sebagai *Digital Evidence Interactions* karena halaman ini berfungsi sebagai halaman untuk mencatat segala aktivitas pengisian informasi *chain of custody*. Gambar 3.7 menunjukkan konsep desain *form chain of custody*.

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 3.7 Konsep Desain *Form Chain of Custody*

Aktivitas ketika terjadi aktivitas unduh bukti fisik atau *form chain of custody* nama elemen dari struktur *history* akan dimunculkan beserta nilai dari setiap elemen tersebut. Hal ini dilakukan untuk mempermudah pengguna melihat elemen XML apa saja yang sudah diubah atau ditambah. Simbol "---" artinya *field* tersebut kosong (tidak ada data yang dimunculkan). Halaman ini juga memuat informasi tentang nama institusi tempat *investigator* dan *first responder* bekerja.

Halaman terakhir adalah halaman yang 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 fisik pada sistem telah melalui validasi dari *officer*. Gambar 3.8 menunjukkan desain *form chain of custody* halaman pengesahan.

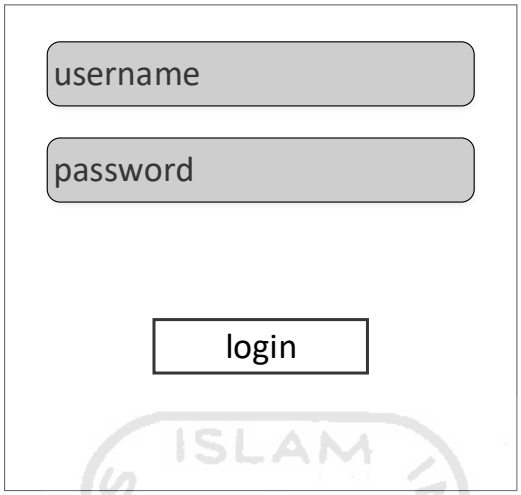
This Form Chain of Custody has been validated by officer
Nama officer
Kode hashing MD5

Gambar 3.8 Konsep Desain *Form Chain of Custody* Halaman Pengesahan

3.5 Perancangan Desain Halaman Antarmuka

Perancangan halaman antarmuka dilakukan untuk membuat tampilan yang

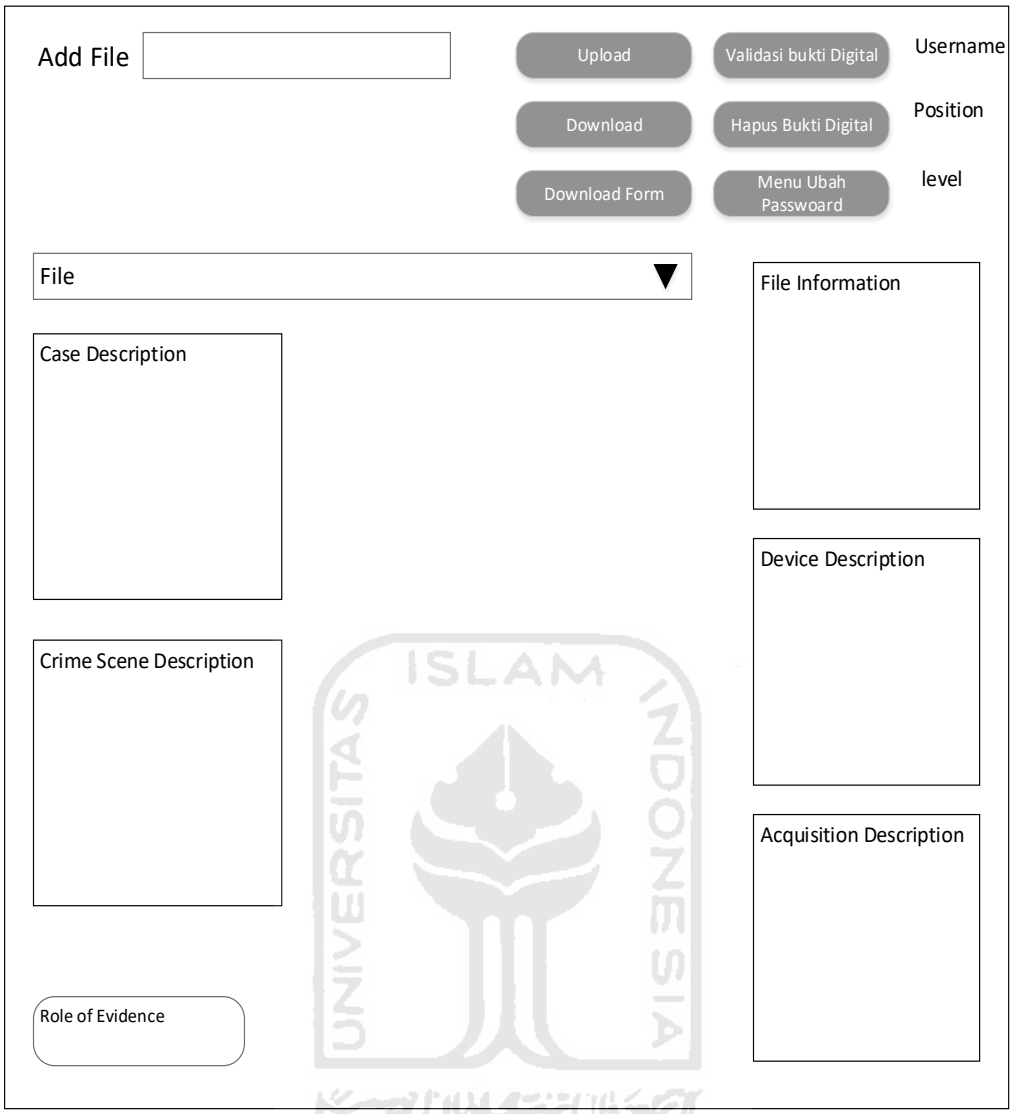
sederhana sehingga dapat dengan mudah digunakan. Perancangan halaman antarmuka dilakukan dengan menggambar secara sederhana tampilan yang akan dibuat. Gambar 3.9 menunjukkan konsep desain halaman *login*.



Gambar 3.9 Konsep Desain Halaman *Login*

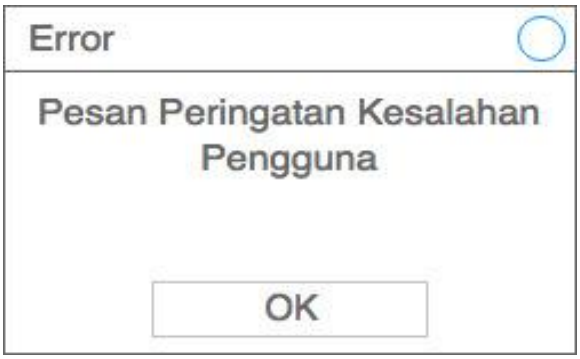
Ketika proses otorisasi selesai dan pengguna mendapat hak akses untuk masuk ke sistem, maka sistem akan menampilkan halaman utama. Namun, jika otorisasi gagal, sistem akan menampilkan pesan bahwa pengguna tidak mendapat otorisasi. Hal ini dapat terjadi karena pengguna salah memasukkan *username* atau *password.*

Halaman awal menampilkan daftar yang telah dibuat. Pengguna dapat memilih *file* untuk menampilkan daftar bukti digital yang telah diunggah. *First responder* dan *investigator* dapat mengisi *chain of custody* pada halaman utama setelah memilih bukti fisik. Halaman ini menampilkan *username, position* (*investigator, first responder* atau *officer*) dan *level (high, normal* atau *low).* Pengisian data *chain of custody* pada halaman utama dibagi menjadi 5 kelompok seperti yang telah dijelaskan pada tabel 3.1. *Officer* dapat memvalidasi data *chain of custody* dan bukti fisik yang akan diunggah pada menu *ubah password.* Gambar 3.10 menunjukkan rancangan pada halaman utama.



Gambar 3.10 Konsep Desain Halaman Utama

Ketika pengguna melanggar hak otorisasi, contohnya: *officer* memilih tombol *upload,* maka sistem akan menampilkan jendela peringatan bahwa *officer* tidak memiliki hak otoritas untuk mengunggah bukti fisik. Jendela peringatan ini juga akan muncul jika terjadi kesalahan dalam penggunaan sistem tersebut. Gambar 3.11 menunjukkan rancangan desain jendela peringatan kesalahan penggunaan sistem.



Gambar 3.11 Rancangan Desain Jendela Peringatan Kesalahan

3.6 Perancangan Deep Learning

Perancangan halaman antarmuka dilakukan untuk membuat gambar yang sudah diunggah akan menggunakan API Clarifai untuk mendukung proses pengenalan gambar atau image recognition yang dibutuhkan pada identifikasi bukti fisik yang berupa gambar yang diunggah ke sistem.

3.7 Simulasi Kasus

Simulasi kasus adalah tahapan untuk membuat skenario palsu berdasarkan kasus-kasus yang telah diselesaikan. Simulasi kasus dilakukan dengan tujuan untuk mengetahui apakah output yang akan dihasilkan sistem sudah memenuhi rancangan. Penggunaan kasus tersebut karena hasil penyelidikan bukti fisiknya sudah diketahui sehingga dapat dijadikan sebagai acuan untuk output sistem dalam tahap pengijian. Output dari sistem akan dianalisa kesesuaiannya dengan kasus yang telah disimulasikan, kemudian menghasilkan kesimpulan yang berisi keberhasilan sistem.

3.8 Pengujian

Tahapan pengujian merupakan salah satu tahapan paling penting yang akan menentukan pengembangan sistem ke depannya. Pengujian dilakukan untuk mengetahui sejauh mana sistem yang baru berjalan dan keberhasilannya memberikan output sesuai rancangan. Tahap pengujian menggunakan simulasi kasus untuk bahan ujinya agar hasil yang keluar dapat dianalisa dengan mudah.

Sistem akan memberikan hasil uji berupa form chain of custody. Form tersebut nantinya akan dibandingkan dan dianalisa dengan output dari sistem penanganan bukti fisik yang lain.

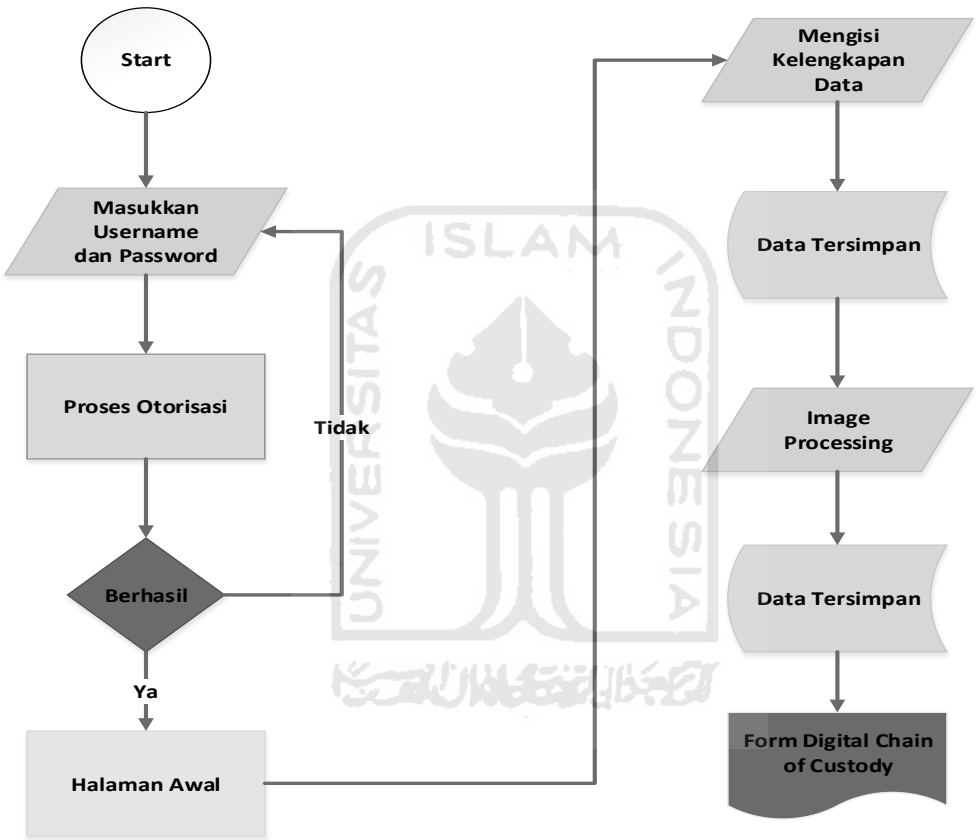
3.9 Hasil dan Kesimpulan

Pada tahap ini, *output* dari sistem akan dianalisa untuk mengetahui apakah *output* sesuai dengan rancangan. *Output* yang diinginkan adalah *form chain of custody*. *Form tersebut* dinyatakan lulus uji apabila sistem mampu menyimpan data bukti fisik dan menghasilkan *chain of custody*.

Analisa *form chain of custody* akan membantu penarikan kesimpulan. Kesimpulan tersebut akan menjadi dasar dari keberhasilan sistem. Kesimpulan memuat pencapaian sistem yang didapat dari hasil uji dan analisa. Kesimpulan menunjukan terpenuhinya tujuan pembuatan sistem baru serta hasil yang sesuai keinginkan.

BAB 4
Pembahasan

Bab ini menjelaskan tentang pengujian sistem hingga ke tahap analisis terhadap hasil dari sistem. Pengujian sistem dilakukan dengan menggunakan 3 simulasi kasus yang pernah terjadi di Indonesia maupun yang terjadi di luar Indonesia, namun nama dan barang bukti yang diperoleh adalah fiktif. Gambar 4.1 menunjukkan alur pengujian sistem.



Gambar 4.1 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.*

4.1 Form Chain of Custody (*CoC*)

Form Chain *of Custody* merupakan hasil akhir dari sistem ini yang merupakan data-data yang sudah diinputkan oleh *Investigator* dan *First Responder*. Tidak hanya data yang diinputkan saja tetapi juga hasil dari *Image Processing* yang berupa data tersembunyi dari gambar yang dijadikan barang bukti. Data-data yang ditampilkan pada halaman pertama merupakan data yang sudah di validasi oleh officer.

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/ktisnawidatama/Documents/IMG_0074 - Copy.jpg
Cabinet Structure	images/IMG_0074 - Copy
Potential Information	SMS, Telepon
Status	ACTIVE
Validator	officer

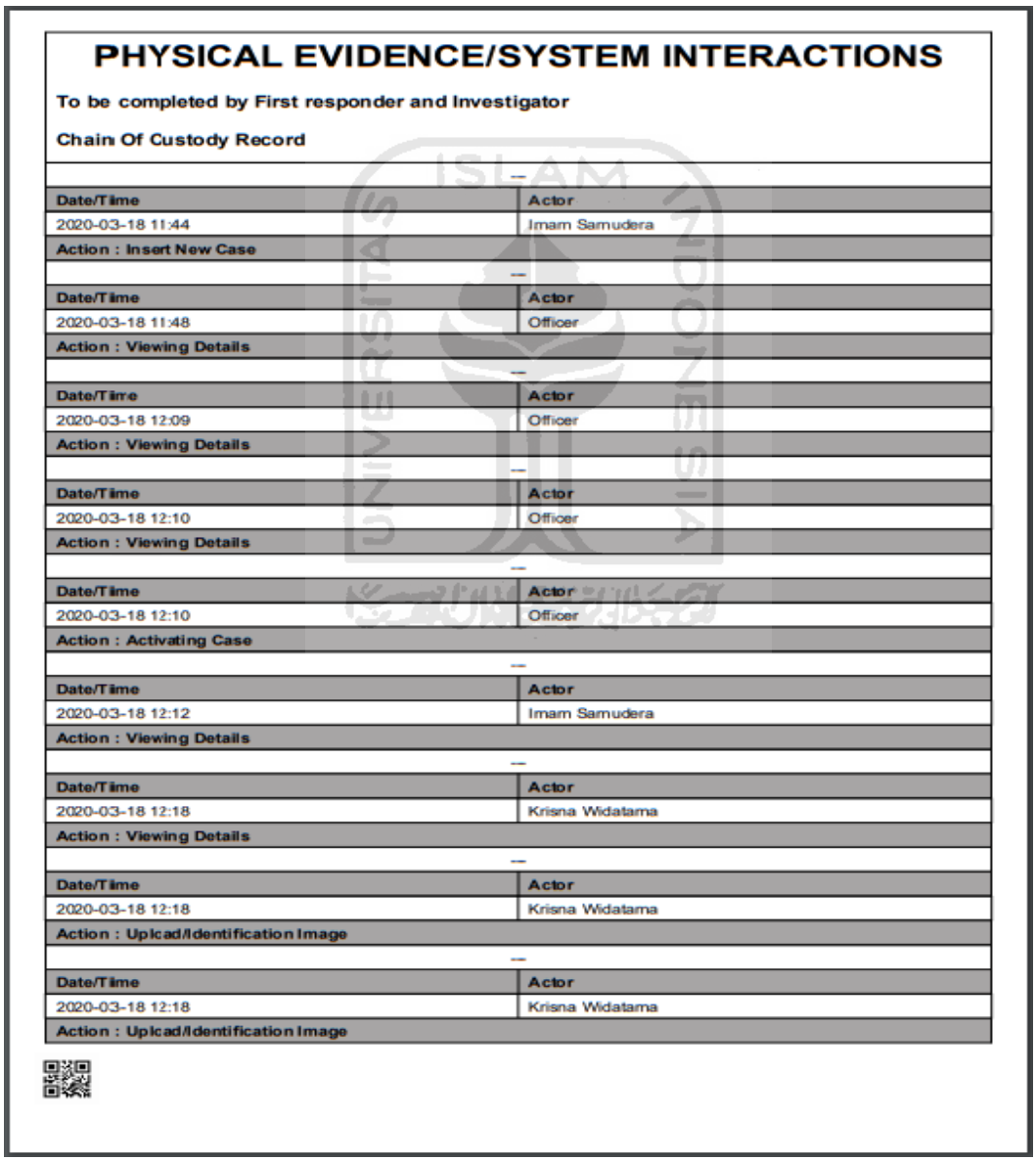
Gambar 4.2 *Form Chain of Custody* Halaman Pertama

Pada tabel 4.2 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. *First reasponder* disini merupakan nama aktor yang bertugas memasukkan dan mengupload data ke dalam sistem. Baris *institution* merupakan catatan tentang institusi yang melakukan penyelidikan kasus kejahatan.

Electronic Evidence merupakan catatan dari barang bukti yang didapatkan saat melakukan penyelidikan. *Register Number* berisi tentang catatan nomor registrasi yang digunakan untuk mendaftarkan barang bukti saat pertama dikeluarkan dari pabrik. *Type* catatan dari tipe barang bukti yang digunakan saat melakukan tindak kejahatan. *Model* merupakan catatan tentang bentuk dari barang bukti yang sudah diinptkan oleh *First Responder*. *Manufactur* berisi nama perusahaan pembuat barang bukti tersebut. *Serial number* merupakan nomor seri dari barang bukti dan setiap tipe yang sama tidak mungkin nomor serinya sama. *Ferodosure reasons* berisi tentang alasan barang dijadikan sebagai bukti terhadap kasus kejahatan.

Selanjutnya yaitu kolom *Metadata of Image Processed*, pada kolom ini merupakan catatan tentang hasil dari gambar yang telah di upload menjadi data digital. *Evidence Number* akan berisi tentang nomor bukti yang menjelaskan tentang kapan kejahatan terjadi dengan tanggal dan nomor berapa gambar diupload pada sistem. *Case number* berisikan nomor kasus kejahatan yang sudah diselidiki dan telah di inputkan ke sistem ini. *File name* merupakan nama dari gambar yang telah diupload ke sistem. *Size* adalah ukuran dari file gambar yang

dijadikan barang bukti dengan satuan *byte*. Lalu disini juga terdapat hasil enkripsi dari gambar dengan dua metode, yang pertama pada baris hashing(SHA1) dan hashing(MD5). Pada baris *source* berisi tentang sumber dari gambar yang diupload melalui PC yang digunakan. Baris selanjutnya berisikan tentang struktur kabinet dari gambar yang diupload. *Potential information* pada tabel diatas berisi SMS dan telepon, yang dimaksudkan adalah potensi barang tersebut dijadikan barang bukti. Status akan berisikian tulisan *active* yang menandakan bahwa kasus yang diselidiki sedang dalam proses penanganan. *Validator* berisi nama dari officer yang memvalidasi semua inputan dari *first responder* dan *investigator*.



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	

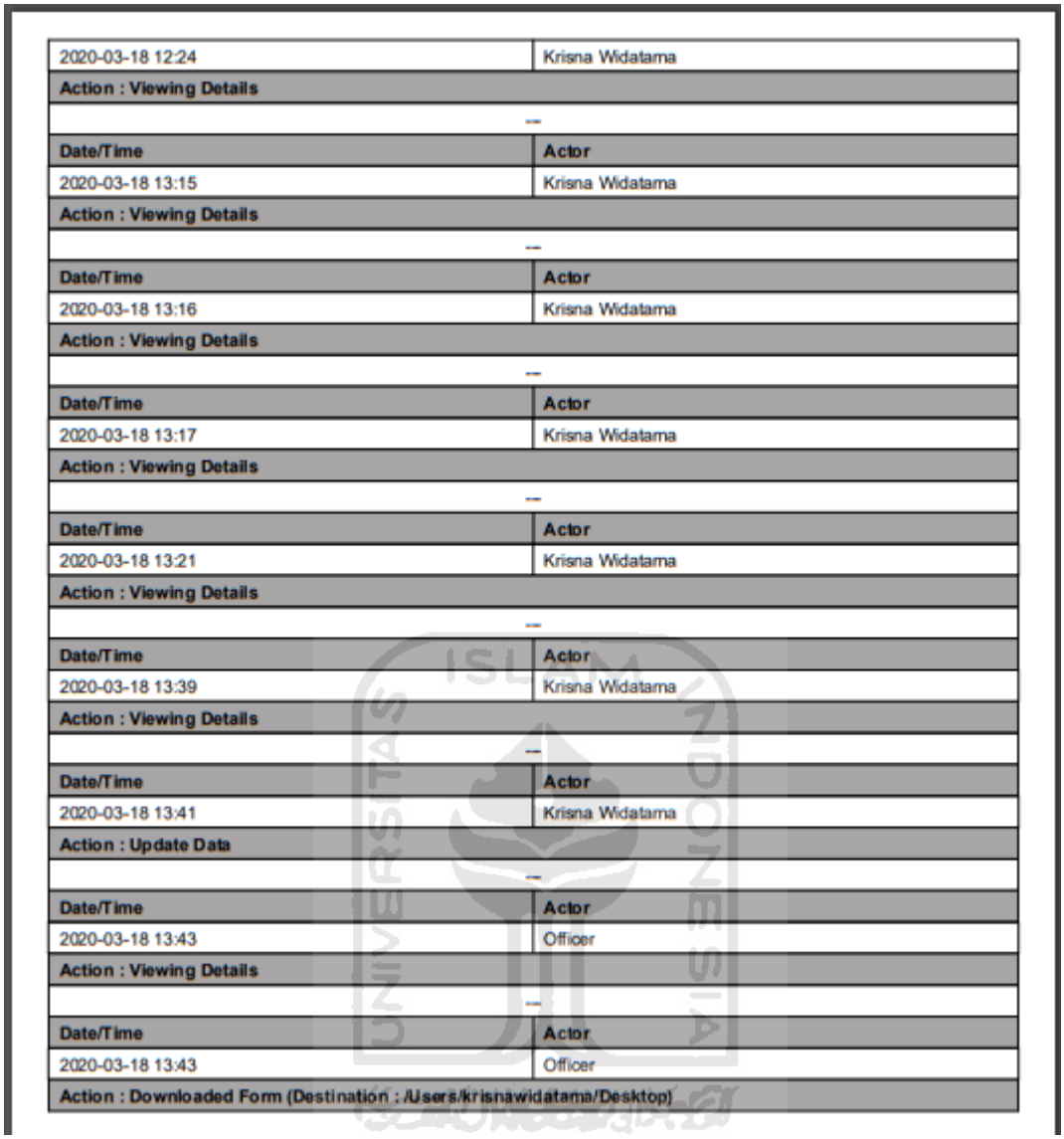
` Gambar 4.3 *Form Chain of Custody* Halaman Kedua

—	
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	
—	
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	
—	
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	
—	
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	
—	
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 4.4 *Form Chain of Custody* Halaman Kedua (Lanjutan)

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	
—	
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	
—	
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	
—	
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	
—	
Date/Time	Actor
2020-03-18 12:20	Imam Samudera
Action : Analyzed	
—	
Date/Time	Actor
2020-03-18 12:23	Imam Samudera
Action : Returned	
—	
Date/Time	Actor

Gambar 4.5 *Form Chain of Custody* Halaman Kedua (Lanjutan)



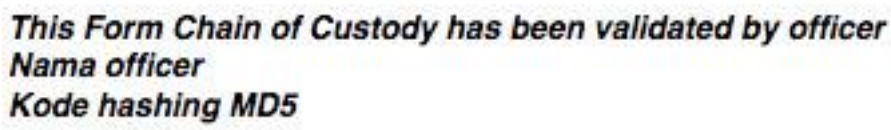
2020-03-18 12:24	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:15	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:16	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:17	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:21	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:39	Krisna Widatama
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:41	Krisna Widatama
Action : Update Data	
--	
Date/Time	**Actor**
2020-03-18 13:43	Officer
Action : Viewing Details	
--	
Date/Time	**Actor**
2020-03-18 13:43	Officer
Action : Downloaded Form (Destination : /Users/krisnawidatama/Desktop)	

Gambar 4.6 *Form Chain of Custody* Halaman Kedua (Lanjutan)

Berbeda dengan halaman pertama yang jumlah datanya tidak bisa 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.

Pada *form chain of custody* halaman kedua diatas memiliki jumlah data yang cukup banyak sehingga form tersebut menjadi lebih dari satu halaman. Lalu pada halaman terakhir terdapat catatan tentang tujuan penyimpanan *form chain of custody* pada PC pengguna. Pada halaman kedua juga tercatat nama-nama user yang berinteraksi dengan sistem dan terdapat barcode pada setiap halaman.



Gambar 4.7 *Form Chain of Custody* halaman terkahir

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*.

4.2 Spesifikasi Komputer

Pembuatan dan pengujian sistem menggunakan Laptop dengan merek Asus, berikut adalah spesifikasi laptop yang digunakan.

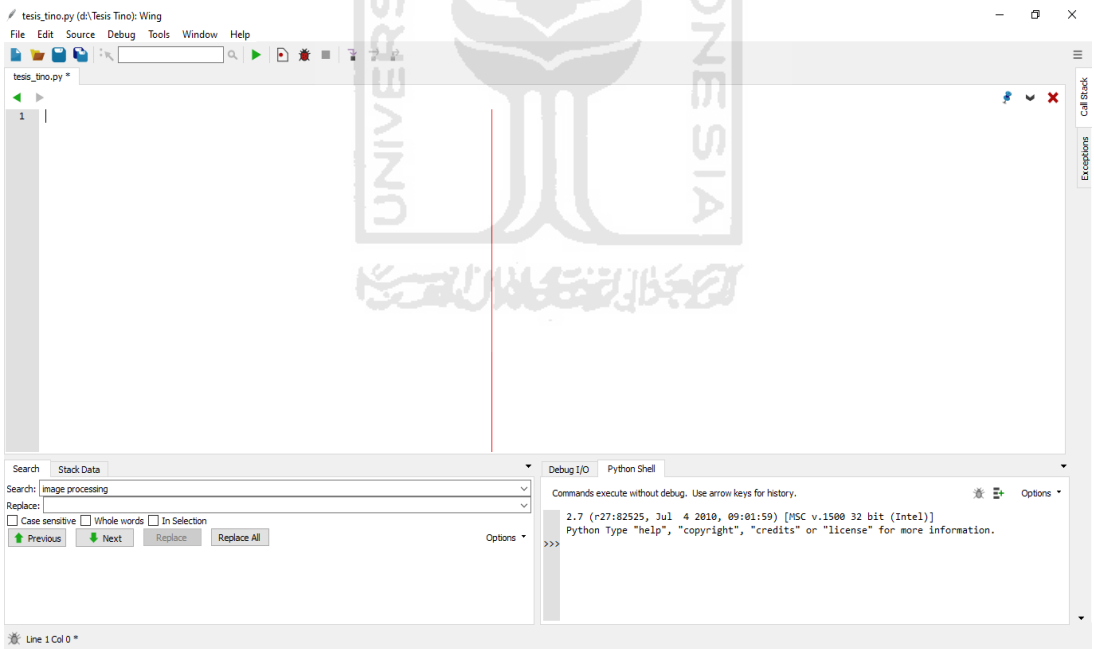
Tabel 4.1 Spesifikasi Laptop yang Digunakan

No.	Komponen	Deskripsi
1.	Nomor Serial Laptop	F6N0CX158223245
2.	Ukuran Layar	14 inch
3	Grafis	Intel IGP
4.	Resolusi	1366 x 768
5.	Prosesor	Intel Celeron N2830 Speed 2.16GHz Turbo Boost 2.41GHz
6.	Kapasitas RAM	DDR3 2GB
7.	Harddisk	500GB
8.	Port USB	2 Port USB 2.0, SD Card Slot, Infrared
9.	Koneksi	IEEE 802.11 b/g/n dan Bluetooth V4.0
10.	Optical Drive	DVDRW
11.	Berat	2 Kg

Sistem operasi yang digunakan untuk membuat sistem ini adalah Microsoft Windows 8.1. Sistem operasi ini adalah paket layanan untuk sistem operasi Windows 8 dan Windows RT dan dirilis sebagai beta publik pada bulan Juni 2013, Windows 8.1 dirilis untuk manufaktur pada tanggal 27 Agustus 2013. Windows merupakan sebuah sistem operasi yang diciptakan oleh Microsoft, dimana sistem operasi ini menyediakan antarmuka grafis (GUI/*Graphical User Interface*) agar lebih mudah dioperasikan.

4.3 Spesifikasi Compiler

Compiler merupakan aplikasi yang digunakan untuk menerjemahkan bahasa pemrograman (*Source Code*) kedalam bahasa objek (*object code*). *Compiler* yang digunakan untuk membuat adalah Wing 101 Versi 7.1.0.2. Aplikasi ini dikhususkan untuk membuat aplikasi dengan menggunakan bahasa pemrograman Python. Gambar 4.5 menunjukkan halaman awal Wing 101.



Gambar 4.8 Halaman Awal Wing 101

4.4 Implementasi Sistem

Subbab ini menjelaskan tentang implementasi sistem yang sedang di kerjakan. Sistem ini dibuat dengan menggunakan bahasa pemrograman Python versi 2.7 dan compiler yang digunakan untuk menulis program ini adalah Wing 101. Untuk spesifikasi PC agar bisa menjalankan sistem ini akan dijelaskan pada subbab berikutnya. Penggunaan bahasa python dikarenakan bahasa pemrogaraman ini dapat digunakan pada sistem operasi yang populer saat ini, seperti: Microsoft, MacOS dan Linux. Alasan penggunaan bahasa pemrograman python, penulisan bahasa pemrograman ini lebih sederhana dan ringkas sehingga tidak memakai lebih banyak syntax daripada bahasa pemrograman lain, karena tidak diperlukan penulisan tipe data.

4.4.1 Pseudo Code Image Processing

Pada baris 1 digunakan untuk membuka file yang sudah dimasukkan oleh pengguna mengenai korban, pelaku kejahatan dan kasus kejahatan. Selanjutnya pada baris 6 terdapat kode API yang akan didapatkan apabila membeli lisensi sestem ini secara resmi, jika tidak membeli lisensi maka program hanya dapat digunakan secara trial dan hanya dapat digunakan sesuai tenggang waktu yang diberikan pengembang terhadap sistem ini. pada baris 8 sistem akan menganalisa file yang akan dimasukkan pada variable concepts. Baris 9-10 digunakan untuk memasukkan file hasil analisa yang terdapat pada variable concepts ke dalam variable apii. Pada baris 12, variable apii di dalamnya terdapat array name yang berfungsi untuk mengetahui apa probabilitas dari file yang sudah dianalisis lalu dipisahkan juga variable value. Variabel value berfungsi untuk mencari berapa nilai probabilitas dari file yang sudah dianalisis. Baris 13, file yang probabilitasnya sudah dipisahkan dalam variable app akan dideskripsi dan dimasukkan dalam listbox yang akan ditampilkan pada halaman sistem.

Tabel 4.2 *Source Code Image Processing*

Baris	***Source Code***
1	dlg = fdialog.Open()
2	fl = dlg.show()
3	self.listbox.delete(0, END)
4	base = basename(fl)
5	fileDir = fl
6	app = ClarifaiApp(api_key='071e4544f98d4ac69b9462fee94bc033')
7	model = app.public_models.general_model
8	response = model.predict_by_filename(fileDir)
9	concepts = response['outputs'][0]['data']['concepts']
10	apii = ""
11	for concept in concepts:
12	apii = concept['name']+" - "+str(concept['value'])
13	self.listbox.insert(END, apii)

4.4.2 Pseudo *Code Login*

Sebuah sistem yang aman akan membutuhkan verifikasi agar bisa masuk dalam sistem dan dapat menginput maupun menghapus file dari sistem. Pada tabel 4.3 menjelaskan *Pseudo code* alur dari menu login agar dapat masuk pada sistem.

Tabel 4.3 *Pseudo Code Login*

Baris	***Pseudo Code***
1	def checklogin(self):
2	username = self.userName.get()
3	passwordx = self.passwordName.get()
4	passx = hashlib.sha1(passwordx).hexdigest()
5	try:
6	conn = sqlite3.connect("lpbd.db")
7	conn.text_factory = str
8	cur = conn.cursor()
9	cur.execute("SELECT * FROM user WHERE user_name = '"+username+"' AND
10	password_user = '"+passx+"'").rowcount
11	rows = len(cur.fetchall())
12	if(rows >= 1):
13	name = [name[3] for name in cur.execute("SELECT * FROM user WHERE user_name =
14	'"+username+"' AND password_user = '"+passx+"')]

Tabel 4.4 *Pseudo Code Login* (Lanjutan)

Baris	***Pseudo Code***
15	iduser = [iduser[0] for iduser in cur.execute("SELECT * FROM user WHERE user_name
16	= '"+username+"' AND password_user = '"+passx+"')]
17	now = datetime.datetime.now()
18	dateTime = now.strftime("%d-%m-%Y %H:%M")
19	sql = """ INSERT INTO session (iduser,date_session)
20	VALUES("""+str(iduser[0])+""","""+dateTime+""") """
21	count = cur.execute(sql)
22	conn.commit()
23	tkMessageBox.showinfo("Success", "Welcome, "+name[0]+"")
24	self.parent.destroy()
25	root = Tk()
26	menubar = Menu(root)
27	aplikasi = Cabinet(root, "Digital Evidence Cabinet")
28	root.config(menu=menubar)
29	root.mainloop()
30	else:
31	tkMessageBox.showinfo("Error", "Wrong Username or Password !")
32	except Exception as e:

Baris 1 berfungsi untuk login pengguna ke dalam sistem. Baris 2 digunakan untuk memasukkan username pengguna sedangkan baris ke 3 digunakan untuk memasukkan password pengguna pada menu login, maka selanjutnya username dan password akan diverifikasi oleh sistem. Baris 4, variabel hex akan mengenkripsi password yang dimasukkan pengguna terhadap kode primary yang terdapat pada database sistem,

Baris 6 akan menyambungkan sistem terhadap database lpbd.db untuk memverifikasi password terenkripsi. Baris 9 terdapat query cur.execute yang digunakan untuk membandingkan antara database dengan input username dan password dari pengguna yang sudah terenkripsi, jika data file yang sudah dienkripsi sama dengan data yang ada pada database (baris 12) maka sistem akan menampilkan pesan pada kotak dialog bahwa pengguna dapat masuk ke dalam sistem (baris 23). Apabila data inputan pengguna tidak sama saat proses pencocokan maka sistem akan menampilkan pesan eror (baris 31) dan pengguna diperintahkan untuk memasukkan username dan password kembali.

4.4.3 *Pseudo Code* Simpan Data

Query di bawah ini akan digunakan *investigator* dalam mengedit kasus yang telah di masukkan oleh first *responder* . pengeditan yang dilakukan *investigator* terhadap sistem ini yaitu mengenani nama tersangka dan nama korban.

Tabel 4. 5 *Pseudo Code Simpan Data*

Baris	*Pseudo Code*
1	case_name = self.caseName.get()
2	suspect_name = self.suspectName.get()
3	victim_name = self.victimName.get()
4	try:
5	conn = sqlite3.connect("lpbd.db")
6	conn.text_factory = str
7	cur = conn.cursor()
8	now = datetime.datetime.now()
9	dateTime = now.strftime("%d-%m-%Y %H:%M")
10	sql = """ INSERT INTO record (id_case, desc_record, user_detail, date_record)
11	VALUES ("""+str(self.dropMenu3xy.get())+""","Updating
12	Case","""+str(self.id_user)+""","""+dateTime+""") """
13	cur.execute(sql)
14	sql2 = """ UPDATE case_data SET case_number = """+str(case_num)+""",
15	case_name = """+str(case_name)+""", suspect_name =
16	"""+str(suspect_name)+""", victim_name = """+str(victim_name)+""" WHERE
17	id_case = """+str(self.dropMenu3xy.get())+""" """
18	cur.execute(sql2)
19	conn.commit()
20	tkMessageBox.showinfo("Success", "Your Case Has Been Updated!")
	except Exception as e:

Baris 1 digunakan untuk menampung data yang dimasukkan ke sistem oleh pengguna terhadap nama kasus. Baris 2 digunakan untuk menampung data yang berupa nama tersangka. Lalu baris 3 digunakan untuk menampung data berupa nama korban yang telah diinputkan oleh pengguna.

Baris 5 akan menyambungkan sistem terhadap database lpbd.db. setelah database tersambung dengan sistem, baris 9 akan mencatat tanggal masuk investigator dalam mengedit data yang telah dimasukkan oleh pengguna. Baris 10-12 digunakan untuk memasukkan data tanggal yang telah dicatatat pada baris 9 dan mengeksekusinya agar data tersebut tersimpan pada database lpbd.db.

4.4.4 *Pseudo Code* Pembacaan Data

Tabel 4.4 *Pseudo* Code Pembacaan Data menunjukkan potongan *Pseudo Code* untuk membaca data pada database *lpbd.db* dengan input dari user saat masuk maupun dari investigator saat mengedit kasus. Lalu menampilkannya dalam *listbox* sistem.

Tabel 4.6 *Pseudo Code* Pembaca Data

Baris	*Pseudo Code*
1	def checklogin(self):
2	username = self.userName.get()
3	passwordx = self.passwordName.get()
4	passx = hashlib.sha1(passwordx).hexdigest()
5	try:
6	conn = sqlite3.connect("lpbd.db")
7	conn.text_factory = str
8	cur = conn.cursor()
9	cur.execute("SELECT * FROM user WHERE user_name = '"+username+"'
10	AND password_user = '"+passx+"'").rowcount
11	rows = len(cur.fetchall())
12	if(rows >= 1):
13	name = [name[3] for name in cur.execute("SELECT * FROM user WHERE
14	user_name = '"+username+"' AND password_user = '"+passx+"')]
15	iduser = [iduser[0] for iduser in cur.execute("SELECT * FROM user
16	WHERE user_name = '"+username+"' AND password_user = '"+passx+"')]
17	now = datetime.datetime.now()
18	dateTime = now.strftime("%d-%m-%Y %H:%M")
19	sql = """ INSERT INTO session (iduser,date_session)
20	VALUES("""+str(iduser[0])+""","""+dateTime+""") """
21	count = cur.execute(sql)
22	conn.commit()
23	tkMessageBox.showinfo("Success", "Welcome, "+name[0]+"")
24	
25	self.parent.destroy()
26	root = Tk()
27	menubar = Menu(root)
28	aplikasi = Cabinet(root, "Digital Evidence Cabinet")
29	root.config(menu=menubar)
30	root.mainloop()
31	else:
32	tkMessageBox.showinfo("Error", "Wrong Username or Password !")
33	
34	except Exception as e:

Baris 5 digunakan untuk mencoba menyambungkan database dengan sistem, agar dapat membaca file hasil dekripsi dengan database. Setelah tersambung dengaan database maka baris 9 akan melakuka proses pencocokan terhadap file yang telah didekripsi. Setelah menemukan elemen yang dicari, baris 12 akan mencari nilai dari elemen tersebut.

Pada percabangan di baris 12 berfungsi untuk memeriksa eksistensi dari nilai setiap elemen. Jika terdapat nilai yang kosong dari elemen tertentu, maka variabel tersebut tidak diberi nilai. Dengan kata lain *field* yang ditampilkan pada halaman awal kosong, dan akan menampilkan peringatan yang akan ditampilkan pada kotak dialog sistem (baris 32). Jika elemen terisi semua maka akan ditampilkan pesan (baris 23) dan pengguna akan masuk ke dalam sistem.

4.5 Simulasi Kasus

Bagian ini adalah subbab yang berisi setting cerita mengenai beberapa kasus yang ditangani sistem. Simulasi kasus ini juga dibuat sebagai bentuk pratinjau dari kasus yang akan digunakan. Subbab ini akan menunjukan bagaimana alur kerja sistem serta pihak-pihak yang terlibat dalam kerja sistem. Pada simulasi kasus ini akan menggunakan 3 contoh kasus, yaitu kasus pornografi, kasus transaksi narkotika, dan kasus pelanggaran hak cipta.

Kasus pornografi yang digunakan sebagai simulasi kasus adalah sebuah kasus tentang jual beli video porno melalui aplikasi smartphone, bukti elektronik yang ditemukan adalah 2 buah smartphone, 2 buah kamera dan 3 buah *memory card* dengan kapasitas masing-masing 2 GB, 4 GB, dan 16 GB. Bukti digital yang ditemukan adalah ss_whatsapp.pdf yang berisi screenshot percakapan antara tersangka dengan tersangka lainnya juga beberapa gambar yang menunjukan bukti transaksi dan beberapa video yang akan dijual pelaku yang tersimpan dalam *memory card* dalam kamera.

Bukti digital yang didapat kemudian diakusisi oleh Tino Feri Efendi sekaligus sebagai first responder, yang menjadi investigator adalah Moh. Fadley Pananende dan Krisna Widatama sebagai officer.

Kasus selanjutnya adalah transaksi narkoba, bukti elektronik yang ditemukan adalah satu sebuah smartphone dan satu unit komputer. Bukti digital yang didapat adalah ss_whatsapp.pdf yang berasal dari aplikasi smartphone. Bukti digitla tersebut berisi *screenshot* percakapan antar pelaku mengenai transaksi. First responder dipegang oleh Tino Feri Efendy, Moh Fadley Pananede sebagai investigator dan Krisna Widatama sebagai officer.

Kasus ketiga adalah pelanggan hak cipta. Kasus ini mengenai pelanggaran hak cipta lagu dari sebuah rumah prosuksi yang dilakukan seorang youtuber. Youtuber tersebut melakukan pengubahan lirik lagu dan mempublikasikan lagu tersebut sebagai lagu baru dari youtuber tersebut tanpa adanya pemberitahuan untuk rumah produksi lagu tersebut. Bukti elektronik yang didapat adalah satu unit komputer. Bukti digital yang didapat adalah video yang ada dalam komputer. Video tersebut berisi lagu baru yang telah dipublikasikan oleh youtuber tersebut.

First responder pada kasus ketiga adalah Krisna Widatama, investigator adalah Tino Feri Efendi dan officer Moh. Fadly Panende. Tabel 4.7 menunjukkan deskripsi simulasi kasus untuk pengujian sistem.

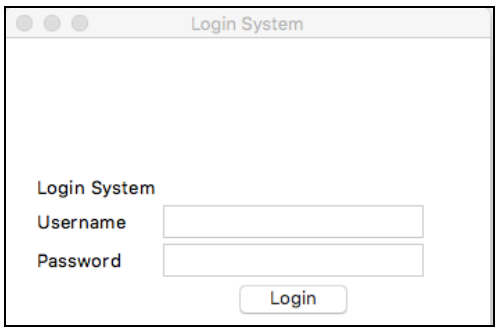
Tabel 4.7 Deskripsi Simulasi Kasus

No.	**Kasus**	**Jumlah Barang Bukti**		**Nama Petugas**		
		Jenis Elektronik	**Nama Bukti Digital**	***First Responder***	***Investigator***	***Officer***
1.	Video Porno (sex scandal)	Smartphone, kamera, *memory card*	ss_whatsapp.pdf Sex_scandal.mp4	Tino Feri Efendi	Moh. Fadly Panende	Krisna Widatama
2.	Transaksi narkoba	Komputer Smartphone	ss_whatsapp.pdf			
3.	Pelanggaran Hak Cipta	Komputer	mv_youtube.pm4	Krisna Widatama	Tino Feri Efendi	Moh. Fadly Panende

4.6 Hasil

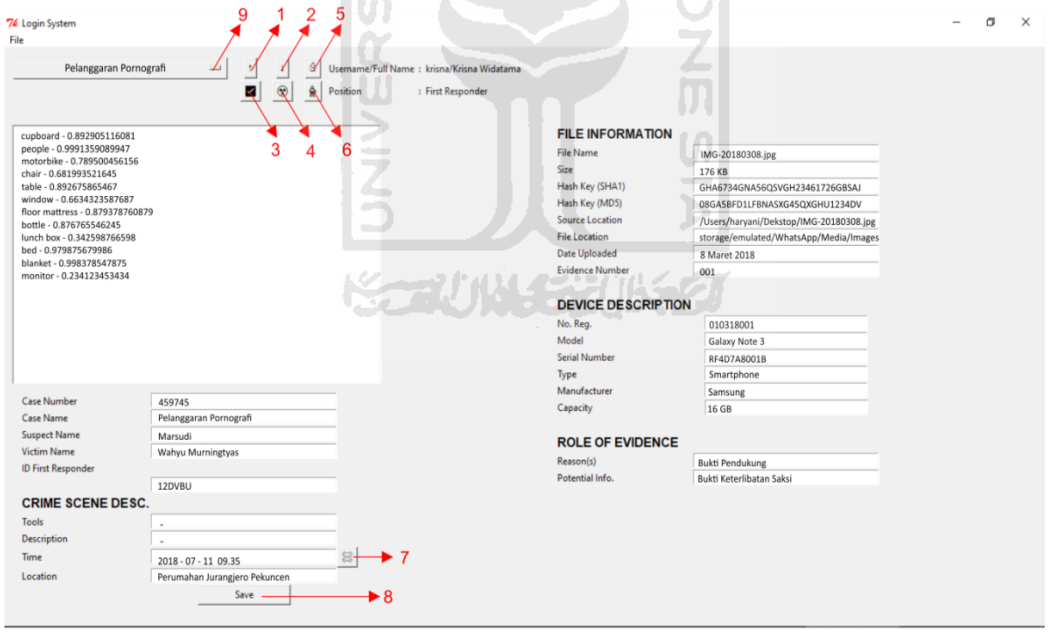
Tampilan awal sistem diawali dengan menampilkan *form login Sistem* berisi *username* dan *password. Form* tersebut digunakan *investigator, officer dan first responder* sebagai proses awal untuk memasuki sistem. Setelah memasukkan

username dan *password*, selanjutnya sistem akan melakukan proses otentikasi. Jika salah memasukkan data *username* dan *password* pada halaman awal, maka sistem akan menampilkan pesan kesalahan. Pengguna dapat memasukkan kembali data *username* dan *password* pada halaman awal tersebut. Gambar 4.6 menunjukkan menu *login* pada sistem tersebut.



Gambar 4.9 Menu *Login*

Setelah *investigator* berhasil *Login*, *investigator* akan masuk pada halaman utama. Gambar 4.6 menunjukkan tampilan halaman utama sistem.



Gambar 4.10 Halaman Utama

Gambar 4.7 menunjukkan halaman awal setelah *investigator* masuk sistem. Terdapat beberapa tombol yang memiliki fungsi yang berbeda-beda. Tabel 4.8 menunjukkan fungsi tombol pada halaman awal sistem.

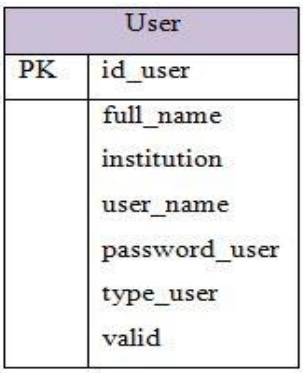
Tabel 4.8 Fungsi Tombol pada Halaman Awal

No.	Fungsi	Pengguna
1.	Upload Bukti Digital	*First Responder*
2.	Cetak Bukti Digital	*Officer*
3.	Mengaktivasi Bukti Digital	*Officer*
4.	Menghapus Bukti Digital	*First Responder*
5.	Mencetak Form *Chain of Custody*	*Officer*
6.	Mengembalikan Bukti Digital	*Officer*
7.	Menampilkan tanggal dan waktu untuk dimasukkan ke dalam form *Chain of Custody*	*First Responder*
8.	Menyimpan isian *Chain of Custody*	*First Responder*
9.	Memilih nomor kasus	*Officer*

Diasumsikan bahwa *Investigator* sudah masuk kedalam sistem dan *Officer* melakukan aktivasi. Setelah itu, *First responder* mengupload bukti digital. Penyimpanan bukti digital pada sistem ini menggunakan susunan: nama kasus, nama korban/instansi, lokasi tempat olah TKP. *Officer* melakukan peminjaman data keluar dan memasukkan kembali data bukti digital. Selanjutnya, *First Responder* memasukkan data *Chain of Custody* dan menyimpannya untuk kemudian *Form Chain of Custody* akan dicetak oleh *Officer.*

4.6.1 Tabel User

Tabel ini adalah tabel user yang bertugas untuk menyimpan data pengguna yang melakukan login. Tabel ini menjadi tempat menampung data *user* yang berisi detail informasi yang berkaitan dengan aktivitas *user*.



Gambar 4.11 Tabel *User*

Gambar 4.8 menunjukkan tabel user dengan kolom-kolom yang ada di dalamnya. Kolom-kolom ini bersal dari atribut-atribut yang dimiliki entitas user. Penamaan kolom tersebut berdasarkan dari data apa yang akan tersimpan dalam database. Tabel 4.8 menunjukkan kolom-kolom yang ada di dalam tabel *user.*

Tabel 4.9 Pembagian kolom Tabel *User*

No	Nama Kolom	Jenis Data	Length	Key
1.	id_user	Integer	30	Primary Key
2.	full_name	Text	-	-
3.	Institution	Text	-	-
4.	user_name	Text	-	-
5.	password_user	Text	-	-
6.	type_user	Text	-	-
7.	Valid	Text	-	-

Tabel 4.9 menunjukan pembagian kolom dalam tabel user berdasarkan kriteria data yang akan disimpan dalam tabel user. Kolom pada Tabel User terdiri dari 7 kolom, yaitu id_user, full_name, institution, user_name, password_user, type_user dan valid.

Kolom pertama berisi id_user, ini adalah kolom yang istimewa dalam Tabel User karena statusnya sebagai primary key. Id_user menjadi primary key karena data yang akan tersimpan di dalamnya adalah data unik. Data yang unik tersebut yang berisi data kode user dimana kode tersebut hanya memiliki satu penomeran untuk setiap datanya. Setiap data yang disimpan dalam kolom id_user tidak boleh ada yang sama karena id_user yang akan menjadi kunci utama yang membedakan setiap user yang tersimpan dalam database, sehingga setiap satu user tidak akan tercampur datanya dengan user yang lain.

Type data yang dipakai idrecord adalah integer, type data khusus angka. Integer digunakan karena type data angka sangat Cocok untuk status primary key. Type data angka memberikan ketelitian yang paling baik, perbedaan satu angka akan menjadi kode yang berbeda juga, sehingga type data ini sangat Cocok untuk kolom id_user dengan statusnya sebagai primary key yang membutuhkan perbedaan dari setiap datanya. Panjang karakter yang tersedia untuk kolom id_user adalah 30 karakter.

Kolom kedua berisi full_name, kolom ini dibuat untuk menyimpan data nama panjang user. Kolom ketiga adalah institution, kolom ini dibuat untuk menyimpan data mengenai institusi mana user berasal. Kolom keempat adalah user_name, kolom ini dibuat untuk menyimpan data user. Kolom kelima adalah password_user, kolom ini akan menyimpan data berupa kata sandi pengguna. Kolom keenam adalah type_user, kolom ini dibuat untuk menyimpan data type user. Kolom ketujuh adalah valid, kolom ini dibuat untuk menyimpan kebenaran data user yang telah dimasukkan. Type data yang digunakan id_user, full_name, institution, user_name, password_user, type_user dan valid adalah text karena type data ini mampu menampung semua jenis karakter dan tidak dibatasi dengan panjang karakternya sehingga Cocok untuk kolom yang membutuhkan banyak karakter yang berbeda jenisnya.

4.6.2 Tabel Session

Tabel ini adalah tabel session yang bertugas untuk menyimpan dan mencatat data pengguna yang masuk.

Session	
PK	idsession
	full_name
	iduser
	date_session

Gambar 4. 12 Tabel *Session*

Gambar 4.9 menunjukkan tabel session dengan kolom-kolom yang ada di dalamnya. Kolom-kolom ini bersal dari atribut-atribut yang dimiliki entitas session. Penamaan kolom tersebut berdasarkan dari data apa yang akan tersimpan dalam database. Tabel 4.9 menunjukkan kolom-kolom yang ada di dalam tabel *session.*

Tabel 4.10 Pembagian kolom Tabel *Session*

No	Nama Kolom	Jenis Data	Length	Key
1.	Idsession	Integer	30	Primary Key
2.	full_name	Text	-	-
3.	Iduser	Integer	30	-
4.	date_session	Text	-	-

Tabel 4.9 menunjukan pembagian kolom dalam tabel session berdasarkan kriteria data yang akan disimpan dalam tabel session. Kolom pada Tabel Session terdiri dari 3 kolom, yaitu idsession, iduser dan data_session.

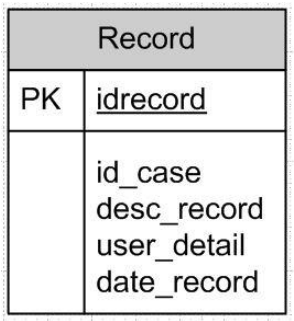
Kolom pertama berisi idsession, ini adalah kolom yang istimewa dalam Tabel Session karena statusnya sebagai primary key. Idsession menjadi primary key karena data yang akan tersimpan di dalamnya adalah data unik. Data yang unik tersebut yang berisi data kode pengguna dimana kode tersebut hanya memiliki satu penomeran untuk setiap datanya. Setiap data yang disimpan dalam kolom idsession tidak boleh ada yang sama karena idsession yang akan menjadi kunci utama yang membedakan setiap user yang tersimpan dalam database, sehingga setiap satu user tidak akan tercampur datanya dengan user yang lain.

Type data yang dipakai idsession adalah integer, type data khusus angka. Integer digunakan karena type data angka sangat Cocok untuk status primary key. Type data angka memberikan ketelitian yang paling baik, perbedaan satu angka akan menjadi kode yang berbeda juga, sehingga type data ini sangat Cocok untuk kolom idsession dengan statusnya sebagai primary key yang membutuhkan perbedaan dari setiap datanya. Panjang karakter yang tersedia untuk kolom idsession adalah 30 karakter.

Kolom kedua berisi iduser, kolom ini dibuat untuk menyimpan data user. Type data yang digunakan adalah integer dan panjang karakter 30. Kolom ketiga adalah date_session, kolom ini dibuat untuk menyimpan data berupa tanggal saat pengguna masuk ke sistem. Type data yang digunakan adalah text karena type data ini mampu menampung semua jenis karakter dan tidak dibatasi dengan panjang karakternya sehingga Cocok untuk kolom yang membutuhkan banyak karakter yang berbeda jenisnya.

4.6.3 Tabel Record

Tabel ini adalah tabel dalam database yang bertugas untuk menyimpan data mengenai perekaman penyelidikan. Tabel ini menjadi tempat menampung data *record* yang berisi detail informasi yang berkaitan dengan aktivitas *record* barang bukti.



Gambar 4.13 Tabel *Record*

Gambar 4.10 menunjukkan tabel record dengan kolom-kolom yang ada di dalamnya. Kolom-kolom ini bersal dari atribut-atribut yang dimiliki entitas record. Penamaan kolom tersebut berdasarkan dari data apa yang akan tersimpan dalam. Tabel 4.11 menunjukkan kolom-kolom yang ada di dalam tabel *record.*

Tabel 4.11 Pembagian kolom Tabel Record

No	Nama Kolom	Type Data	Length	Key
1.	Idrecord	Integer	30	Primary Key
2.	id_case	Integer	30	Foreign Key
3.	desc_record	Text	-	-
4.	user_detail	Text	-	-
5.	date_record	Text	-	-

Tabel 4.10 menunjukan pembagian kolom dalam tabel record berdasarkan kriteria data yang akan disimpan dalam tabel record. Kolom pada Tabel Record terdiri dari 5 kolom, yaitu idrecord, id_case, desc_record, user_detail dan date_record.

Kolom pertama berisi idrecord, ini adalah kolom yang istimewa dalam Tabel Record karena statusnya sebagai primary key. Idrecord menjadi primary key karena data yang akan tersimpan di dalamnya adalah data unik. Data yang unik tersebut yang bersisi data kode record dimana kode tersebut hanya memiliki satu

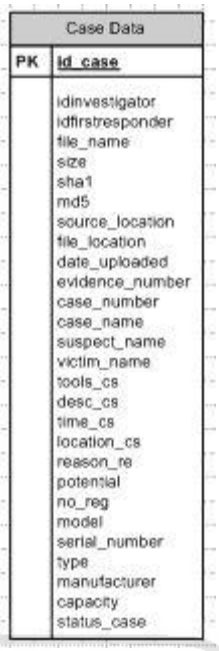
penomeran untuk setiap datanya. Setiap data yang disimpan dalam kolom idrecord tidak boleh ada yang sama karena idrecord yang akan menjadi kunci utama yang membedakan setiap record yang tersimpan dalam database, sehingga setiap satu record tidak akan tercampur datanya dengan record yang lain.

Type data yang dipakai idrecord adalah integer, type data khusus angka. Integer digunakan karena type data angka sangat Cocok untuk status primary key. Type data angka memberikan ketelitian yang paling baik, perbedaan satu angka akan menjadi kode yang berbeda juga, sehingga type data ini sangat Cocok untuk kolom idrecord dengan statusnya sebagai primary key yang membutuhkan perbedaan dari setiap datanya. Panjang karakter yang tersedia untuk kolom idrecord adalah 30 karakter.

Kolom kedua berisi idcase dengan status foreign key karena kolom tersebut digunakan untuk menghubungkan tabel record dengan tabel case data. Type data yang digunakan adalah integer dan panjang karakter 30. Kolom ketiga adalah desc_record, kolom ini dibuat untuk menyimapan data mengenai deskripsi perekaman barang bukti. Kolom keempat adalah user_detail, kolom ini dibuat untuk menyimpanan detail record oleh user. Kolom kelima adalah date_record, kolom ini akan menyimpan data berupa tanggal perekaman barang bukti. Type data yang digunakan desc_record, user_daetail, date_record adalah text karena type data ini mampu menampung semua jenis karakter dan tidak dibatasi dengan panjang karakternya sehingga Cocok untuk kolom yang membutuhkan banyak karakter yang berbeda jenisnya.

4.6.4 Tabel Case Data

Tabel ini adalah tabel yang ada dalam database dengan tugas untuk menampung data mengenai kasus yang berkaitan dengan bukti yang sedang diselidiki. Data kasus berguna untuk kelengkapan berkas barang bukti. Tabel Case Data terdiri dari kolom-kolom yang akan menampung data sesuai dengan pembagian kolomnya.



Gambar 4.14 Tabel Case data dalam relasi antar tabel

Gambar 4.11 adalah gambar tabel case data yang ada dalam relasi antar tabel. Kolom yang ada dalam tabel case data adalah kolom-kolom yang dibuat berdasarkan atribut case data.

Tabel 4.12 Pembagian kolom Tabel Case data

No	Nama Kolom	Type Data	Length	Key
1.	id_case	Integer	30	Primary key
2.	Idinvestigator	Integer	30	-
3.	Idfirstresponder	Integer	30	-
4.	file_name	Text	-	-
5.	Size	Text	-	-
6.	sha1	Text	-	-
7.	md5	Text	-	-
8.	source_location	Text	-	-
9.	file_location	Text	-	-
10.	date_uploaded	Text	-	-
11.	evidence_number	Integer	30	-
12.	case_number	Integer	30	-
13.	case_name	Text	-	-
14.	suspect_name	Text	-	-
15.	victim_name	Text	-	-
16.	Tools_cs	Text	-	-
17.	desc_cs	Text	-	-

Tabel 4.13 Pembagian kolom Tabel Case data (Lanjutan)

No	Nama Kolom	Type Data	Length	Key
18.	time_cs	Text	-	-
19.	location_cs	Text	-	-
20.	reason_re	Text	-	-
21.	Potential	Text	-	-
22.	no_reg	Text	-	-
23.	Model	Text	-	-
24.	serial_number	Text	-	-
25.	Type	Text	-	-
26.	Manufacturer	Text	-	-
27.	Capacity	Text	-	-
28.	status_case	Text	-	-

Pada tabel Tabel 4.12 menunjukan pembagian kolom yang ada dalam tabel Case data. Kolom pertama adalah id_case, kolom ini berfungsi menyimpan data mengenai kode nomor kasus. Kolom id_case berstatus primary key karena id case membedakan setiap kasus dengan kasus lainyya dalam Tabel Case Data, panjang karakternya 30 dan type datanya integer. Kolom kedua adalah idinvestigator, kolom ini akan menyimpan data id dari investigator dalam tabel case data, type data yang digunakan adalah integer dan panjang karakternya adalah 30. Kolom ketiga adalah idfirstresponder, kolom ini menyimpan data berupa kode fisrt responder, type data yang digunakan adalah integer dan panjang karakternya adalah 30. Kolom keempat adalah file_name, kolom ini akan meyimpan data tentang nama file barang bukti, type data yang digunakan adalah text karena mampu menyimpan karakter kombinasi dari angka dann huruf.

Kolom kelima adalah size, kolom ini digunakan untuk menyimpan data ukuran file barang bukti. Type data yang digunakan adalah text karena dapat menampung angka dan huruf. Kolom keenma dan ketujuh adalah sha1 dan md5, type data yang digunakan adalah text. Kolom kedelapan adalah source_location, kolom ini digunakan untuk menampung data tentang sumber file barang bukti, type data yang digunakan adalah text. Kolom kesembilan adalah file location, kolo, ini digunakan untuk menyimpan data tentang lokasi file barang bukti. Type data yang digunakan adalah text.

Kolom kesepuluh adalah date_uploaded, kolom ini digunakan untuk menyimpan data tentang tanggal pengunggahan bukti ke sistem. Kolom berikutnya adalah evidence_number, kolom ini digunakan untuk menyimpan data nomor bukti dalam tabel case data, type data yang digunakan adalah integer dan panjang karakternya dalah 30. Selanjutnya kolom case_number, kolom ini digunakan untuk menyimpan nomor kasus dalam tabel case data. Type datanya adalah integer dan panjang karakternya 30. Kolom selanjutnya adalah cse_name, kolom ini digunakan untuk menyimpan data tentang nama kasus yang masuk ke dalam sistem. Type datanya adalah text.

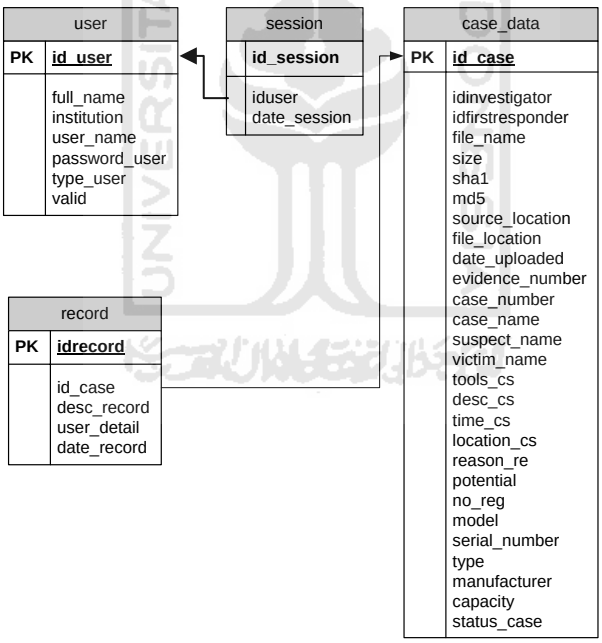
Kolom keempat belas adalah suspect_name, kolom ini digunakan untuk menyimpan data tentang nama tersangka kasus dalam tabel case data. Type datanya adalah text. Kolom kelima belas adalah victim_name, kolom ini digunakan untuk menyimpan data tentang nama korban. Type datanya adalah text. Kolom ke enam belas adalah tools_cs, kolom ini akan menyimpan data tentang peralatan yang digunakan dalam penyelidikan bukti. Type datanya adalah text karena mampu menampung banyak karakter. Kolom ketujuh belas adalah desc_cs, kolom ini digunakan untuk menyimpan data tentang deskripsi kasus. Type datanya adalah text. Kolom kedelapan belas adalah time_cs, kolom ini digunakan untuk menyimpan catatan waktu kasus. Type datanya adalah text. Kolom kesembilan belas adalah location_cs, kolom ini digunakan untuk menyimpan data tentang lokasi kasus, type datanya adalah text. Kolom kedua puluh adalah reason_re, kolom ini digunakan untuk menyimpan data tentang asal mula penyelidakan kasus. Kolom kedua puluh satu adalah potential, kolom inin berisi bagaimana status bukti tersebut ke depannya di pengadilan. Type datanya adalah text.

Kolom kedua puluh dua adalah no_reg, kolom ini digunakan untuk menyimpan data tentang nomor registrasi bukti. Type datanya adalah text karena bisa menampung banyak karakter berbeda. Kolom kedua puluh tiga adalah model, kolom ini digunakan untuk menyimpan data tentang model barang bukti, type datanya adalah text. Kolom kedua puluh empat adalah serial_number, kolom ini digunakan untuk menyimpan data serial number dari bukti fisik. Type datanya

adalah text karena serial number terdiri dari banyak karakter berbeda. Kolom kedua puluh lima adalah type, kolom ini digunakan untuk menyimpan nama type bukti fisik. Type datanya adalah text karena nama type bukti fisik terdiri dari banyak karakter berbeda. Kolom kedua puluh enam adalah manufacturer, kolom ini akan menyimpan data tentang nama produsen atau nama dagang dari bukti fisik dalam sistem, type datanya adalah text.

Kolom selanjutnya adalah capacity, kolom ini digunakan untuk menyimpan data tentang capasitas penyimpana dari bukti fisik yang ditemukan, type datanya adalah text. Kolom terakhir adalah status_case, kolom ini digunakan untuk menyimpan data tentang status kasus yang bukti fisiknya ada dalam sistem, type datanya adalah text.

4.6.5 Relasi Antar Tabel



Gambar 4.15 Relasi Antar Tabel

Tabel-tabel dalam *database* akan menampung data berdasarkan kolom yang dibuat. Dalam *database* ini memuat empat tabel, satu tabel mempunyai hubungan dengan tabel lainnya dalam satu *database*. Hal ini terjadi karena untuk memfungsikan database dengan maksimal harus menghubungkan tabel-tabel

didalamnya. Hubungan ini yang disebut relasi antar tabel. Prinsip yang digunakan dalam menentukan hubungan antar tabel adalah relasi antar tabel, dengan menentukan jenis hubungan satu tabel dengan tabel lainnya.

Terdapat 3 jenis relasi berdasarkan hubungan entitasnya, one to one, one to manydan many to many. Setelah penentuan jenis relasi dilakukuan, maka tabel dapat dihubungkan. Menghubungkan tabel-tabel dilakukan dengan menghubungkan primary key satu tabel dengan foreign keynya pada tabel lain.

4.7 Pembahasan

Pembahasan adalah suatu proses yang dilakukan setelah tahapan implementasi selesai dilakukan. Pembahasan pada subbab ini adalah menjelaskan tentang solusi-solusi yang didapat dari setiap rumusan masalah yang ada. Terdapat 3 permasalahan yang akan dianalisis, yaitu: *form* Bukti Fisik *chain of custody,* Sistem Manajemen Pengelolaan, Algoritma deep learning menggunakan API Clarifai untuk mendukung proses pengenalan gambar atau image recognition yang dibutuhkan pada identifikasi bukti.

4.7.1 Pembahasan Form Phisycal *Chain of Custody*

Berdasarkan pada permasalahan yang sebelumnya, terdapat permasalahan tentang informasi apa saja yang perlu dicantumkan pada *form* digital *chain of custody* untuk bukti fisik ini. Berdasarkan atas data yang telah diperoleh mulai dari perancangan, hingga pada tahap implementasi, maka didapatkan sebuah solusi bahwa informasi yang tercantum pada *form* digital *chain of custody* terbagi menjadi 3 lembar utama. Lembar pertama berisikan informasi tentang: hasil olah TKP, informasi bukti fisik dan informasi mengenai hasil dari proses *image* processing yang dilakukan oleh sistem. Lembar kedua memuat informasi berupa interaksi yang dilakukan oleh pengguna terhadap sistem. Tabel 4.13 menunjukkan informasi yang tercantum pada *form* digital *chain of custody.*

Tabel 4.14 Informasi pada *Form* Digital *Chain of Custody*

No.	**Kelompok Informasi**	***Field* Informasi**	**Keterangan**
1.	Olah TKP	Nama kasus	Nama kasus yang sedang ditangani
2.		Nama tersangka	Nama tersangka pada kasus yang ditangani
3.		Nama korban	Nama korban pada kasus yang ditangani
4.		Lokasi	Lokasi olah TKP (Where)
5.		Tanggal dan waktu	Tanggal dan waktu terjadinya olah TKP (When)
6.		Nama *tools*	Perangkat yang digunakan saat *live forensics*
7.		Deskripsi *tools*	Deskripsi *tools* yang digunakan saat *live forensics*
8.		Nama *first responder*	Nama *first responder*
9.		Nama institusi	Nama institusi *first responder*
10.	Bukti Elektronik	Nomor register	Nomor registrasi penyimpanan bukti fisik di lab. Forensic
11.		Tipe	Jenis bukti fisik, contoh: Flashdisk, Harddisk.
12.		Model	Nama seri bukti fisik
13.		Nama manufaktur	Nama perusahaan pembuat bukti fisik
14.		Nomor serial	Nomor seri pada bukti fisik
15.		Alasan penyitaan	Alasan penyitaan bukti elektronik
16.	Hasil *Image Processing*	Nomor barang bukti	Nomor *file image* unik yang diberikan otomatis saat *file* diunggah
17.		Nomor Kasus	Nomor kasus yang diberikan secara manual oleh *investigator*
18.		Nama *file*	Nama *file image* asli yang diunggah
19.		Ukuran *file*	Ukuran *file image* dalam satuan *byte*
20.		Nilai *Hash* SHA1	Nilai *hash* SHA 1 dari *file image*
21.		Nilai *Hash* MD5	Nilai *hash* MD5 1 dari *file image*
22.		*Source*	Alamat/*path* penyimpanan secara visual *file image* setelah selesai dianalisis
23.		Struktur *cabinet*	Struktur penyimpanan *file image* pada sistem
24.		Potensi informasi	Informasi yang akan dicari pada bukti fisik
25.		Status	Status kasus yang ditangani aktif (*active*) atau telah selesai (*closed*)

Tabel 4.15 Informasi pada *Form* Digital *Chain of Custody* (Lanjutan)

No.	**Kelompok Informasi**	***Field* Informasi**	**Keterangan**
26.	Interaksi Pengguna dengan sistem	Validator	Nama *officer*
27.		Tanggal dan waktu interaksi	*Requested*
28.		Tanggal dan waktu disetujui	*Approved*
29		Tanggal dan waktu penerimaan (bukti digital atau *form* digital *chain of custody*)	*Received*
30.		Interaksi yang dilakukan	*Action*

4.7.2 Pembahasan Sistem Manajemen Pengelolaan

Data tersimpan pada satu DBMS bernama SQLite. Cara kerja dan *query* yang digunakan sama dengan yang digunakan pada MySQL. Data-data tersebut akan tersimpan pada tabel-tabel tertentu pada sebuah *database*. Informasi yang tersimpan merupakan informasi bukti fisik dan *file image*, identitas pengguna sistem serta interaksi yang terjadi antara pengguna sistem. Tabel 4.14 menunjukkan informasi tabel tempat penyimpanan aktivitas pengguna pada sistem.

Tabel 4.16 Struktur Penyimpanan Informasi Aktivitas Penggunaan Sistem

No.	**Nama Elemen**	**Informasi yang Tersimpan**
1.	idrecord	Nomor identifikasi unik pada setiap aktivitas yang tersimpan (PK)
2.	id_case	Nomor/ID kasus dimana pengguna melakukan interaksi (FK)
3.	desc_record	Detil aktivitas yang dilakukan pengguna saat mengakses sistem
4.	user_detail	Nama pengakses sistem
5.	date_record	Tanggal dan waktu aktvitas tersebut dilakukan

Selain digunakan untuk penyimpanan informasi aktivitas penggunaan sistem, data yang terkait bukti fisik juga tersimpan. Tabel yang digunakan berbeda dengan yang digunakan pada table penyimpanan aktivitas informasi. Tabel 4.15 menunjukkan struktur tabel penyimpanan informasi bukti fisik.

Tabel 4.17 Struktur Penyimpanan Informasi Bukti Fisik

No.	Nama Elemen	Informasi yang Tersimpan
1.	id_case	Nomor ID dari kasus baru yang masuk (PK)
2.	Idinvestigator	ID dari Investigator
3.	Idfirstresponder	ID dari First Responder
4.	file_name	Nama *file image* yang dianalisis
5.	Size	Ukuran *file image* (dalam satuan Byte)
6.	Sha1	Enkripsi pada *file image* dengan tipe SHA1
7.	Md5	Enkripsi pada *file image* dengan tipe MD5
8.	Source_location	Lokasi asal tempat *file image* tersebut diunggah
9.	File_location	Lokasi penyimpanan *file image* saat dianalisis
10.	Date_uploaded	Tanggal unggah dan analisis *file image*
11.	Evidence_number	Nomor ID yang diberikan pada *file image*
12.	Case_number	Nomor kasus yang sedang ditangani
13.	Case_name	Nama kasus yang sedang ditangani
14.	suspect_name	Nama tersangka
15.	victim_name	Nama korban
16.	Tools_cs	Nama *tools* yang digunakan saat olah TKP
17.	desc_cs	Deskripsi *tools* yang digunakan saat olah TKP
18.	time_cs	Waktu olah TKP
19.	location_cs	Lokasi olah TKP
20.	reason_re	Alasan penyitaan bukti fisik
21.	Potential	Informasi yang ingin didapat dari bukti fisik
22.	no_reg	Nomor registrasi yang digunakan untuk penyimpanan bukti fisik di Laboratorium Forensik
23.	Model	Model dari bukti fisik
24.	serial_number	Nomor seri bukti fisik
25.	Type	Tipe/nama seri bukti fisik
26.	Manufacturer	Nama perusahaan pembuat bukti fisik
27.	Capacity	Kapasitas penyimpanan bukti fisik
28.	status_case	Status kasus yang dihadapi

Informasi yang juga penting untuk disimpan adalah data pengguna sistem. Pengguna sistem terbagi menjadi 3 yaitu: *first responder, investigator* dan *officer.* Nama-nama pengguna ini akan tercantum pada *form* digital *chain of custody* terutama pada halaman interaksi sistem. Tabel 4.16 menunjukkan struktur penyimpanan informasi data pengguna sistem.

Tabel 4.18 Struktur Penyimpanan Informasi Pengguna Sistem

No.	Nama Elemen	Informasi yang Tersimpan
1.	id_user	ID unik untuk pengguna sistem
2.	full_name	Nama lengkap pengguna
3.	institution	Nama institusi dari tiap pengguna
4.	user_name	*Username* dari tiap pengguna
5.	password_user	*Password* dari tiap pengguna
6.	type_user	Tipe pengguna: First Responder, Investigator atau Officer
7.	valid	Tandatangan dalam bentuk nilai *hash* MD5 milik *officer* untuk memvalidasi *form* digital *chain of custody*

Secara umum sistem ini mengandalkan DBMS Sqlite sebagai penyimpanan data bukti fisik. Penyimpanan data-data ini disimpan dalam beberapa tabel yang beberapa diantaranya saling berelasi. Penggunaan sistem ini yang disertai dengan manajemen penyimpanan menggunakan DBMS Sqlite lebih baik setidaknya untuk saat ini dibandingkan dengan menggunakan cara-cara 'tradisional' yang menggunakan catatan manual.

4.7.3 Pembahasan Kelebihan dan Kekurangan Sistem

Setelah proses implementasi selesai dilakukan, maka akan diperoleh beberapa informasi tentang kelebihan dan kekurangan sistem yang dibangun. Analisis kelebihan dan kekurangan pada sistem ini didasarkan atas penyimpanan informasi penting terhadap bukti fisik dan interaksi antar sistem dan pengguna serta proses analisis file image yang dilakukan. Berikut adalah kelebihan dari sistem.

Penyimpanan data pada bukti fisik, detil kasus dan interaksi antara pengguna dan sistem menggunakan DBMS SQLite. DBMS jenis ini tidak membutuhkan web server seperti MySQL. Hal ini tentunya membuat alokasi memori yang digunakan di RAM menjadi lebih kecil karena tidak perlu menggunakan web server. Selain itu, file yang dihasilkan untuk menyimpan data sangat kecil ukurannya. Dari sisi keamanan, data yang tersimpan pada DBMS jenis ini, memiliki enkripsi khusus yang hanya bisa terbuka jika program untuk membuka SQLite tersebut diaktifkan. Hal ini tentu membuatnya tidak mudah terbaca jika tanpa aplikasi SQLite.

Sistem ini mempunyai kemampuan untuk membaca dan menganalisis suatu file gambar yang diunggah. Hasil dari analisis ini akan ditampilkan saat proses analisis telah selesai dilakukan. Hasil analisis berupa deteksi terhadap objek-objek yang ada pada gambar tersebut dan probabilitasnya. Hal ini akan membantu investigator dalam menganalisis file gambar yang diperoleh dari hasil akuisisi bukti fisik.

Salah satu aspek penting dalam hal penanganan barang bukti adalah apa yang disebut sebagai chain of custody, yaitu sebuah prosedur untuk secara kronologis melakukan pendokumentasian terhadap barang bukti serta pencatatan interaksi terhadapnya. Dokumentasi, pencatatan dan kontrol terhadap barang bukti sangatlah mudah dilakukan pada barang bukti fisik, namun tidak demikian halnya dengan bukti digital. Karakteristik khusus dari bukti digital seperti kemudahan dalam hal modifikasi, copy, hapus, transfer dokumen digital telah menjadi tantangan sendiri dalam proses dokumentasi bukti digital. Untuk itu, chain of custody untuk bukti digital lebih sulit dibandingkan dengan barang bukti fisik pada umumnya serta merupakan sebuah permasalahan yang sangat luas dan kompleks.

Sistem ini dilengkapi dengan satu fitur login. Fitur ini memiliki kemampuan untuk mengenali jenis pengguna yang akan masuk ke dalam sistem. Selain itu, sistem ini juga memiliki tabel khusus yang berfungsi untuk mencatat setiap pengguna yang masuk. Hal ini bertujuan untuk mengetahui pengguna yang terakhir melakukan interaksi dengan sistem.

Selain memiliki kelebihan, tentu saja sistem ini memiliki beberapa kelemahan. Kelemahan ini menjadi bagian dari kekurangan sistem yang dapat digunakan sebagai bahan acuan untuk penelitian selanjutnya yang bertujuan sebagai peningkatan kinerja sistem dalam penanganan bukti fisik. berikut adalah kekurangan yang ada pada sistem ini.

Penyimpanan data yang ada digunakan pada sistem ini akan menghasilkan sebuah file berekstensi .db dimana di dalam file ini tersimpan segala macam informasi penting yang telah disimpan dalam file. Hal ini tentu saja menjadi kelemahan, dimana file ini dapat dipindahkan secara illegal dan juga dapat

dihapus oleh orang yang tidak bertanggung jawab. Data yang tersimpan dalam file ini memang telah terenkripsi dengan jenis enkripsi tertentu, namun enkripsi file ini bisa dibuka hanya dengan menggunakan aplikasi editor SQLite yang telah tersedia di internet secara gratis. Kekurangan ini berdampak pada keamanan data yang tersimpan menjadi sedikit berkurang, karena hasil enkripsi yang dihasilkan masih dapat dibuka.

Penyimpanan data pada sistem ini masih terpusat dalam satu komputer saja. Padahal pada praktiknya untuk melakukan penanganan suatu tindak kejahatan komputer, pengguna sistem lebih dari satu orang dan harus memiliki mekanisme pertukaran data yang baik. Sistem pertukaran data antar komputer ini dibutuhkan agar metadata yang terdapat pada file tidak berubah.

Bab 5
Kesimpulan dan Saran

5.1 Kesimpulan

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

1. Berdasarkan atas data yang telah diperoleh mulai dari perancangan, hingga pada tahap implementasi, maka didapatkan sebuah solusi bahwa informasi yang tercantum pada form digital chain of custody terbagi menjadi 3 lembar utama. Lembar pertama berisikan informasi tentang: hasil olah TKP, informasi bukti fisik dan informasi mengenai hasil dari proses image processing yang dilakukan oleh sistem.
2. Data yang telah diperoleh mulai dari perancangan, hingga pada tahap implementasi, sistem terbagi menjadi 3 Aktor yaitu First Responder, Investigator dan Officer. Dengan Tahapan dilakukan secara urut dan terstruktur, hal ini bertujuan agar *form chain of custody* yang dibuat dapat dipertanggungjawabkan di pengadilan.

5.2 Saran

Adapun saran-saran yang perlu diberikan dalam hasil penitian ini adalah:

1. Penyimpanan bukti fisik 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.
2. Penyimpanan data bukti fisik pada sistem ini menggunakan DBMS SQLite. Jenis DBMS ini meskipun unggul dari segi portabilitas karena dapat dipindahkan dengan cepat dan mudah, namun hal ini dapat menjadi satu kekurangan yang fatal karena dapat digandakan bahkan diubah secara ilegal. Diperlukan satu metode untuk mencegah SQLite ditransmisikan maupun diubah secara ilegal.

Daftar Pustaka

Agusta, S. A., & A, T. A. F. (2016). Implementasi Algorithma Stream Cipher RC4 dalam Aplikasi Pendataan Alumni STMIK Amik Riau. *Jurnal Inovtek Polbeng - Seri Informatika*, *1*(1), 1–8.

Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. *Jurnal Teknik ITS*, *6*(1), 116–121.

Casey, E. (2011). *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition.*

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. In *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*. https://doi.org/10.1109/ARES.2013.72

Ćosić, J., Ćosić, Z., & Bača, M. (2011). An ontological approach to study and manage digital chain of custody of digital evidence. *Journal of Information and Organizational Sciences*, *35*(1), 1–13.

Das, S., Dey, H., & Ghosh, R. (2015). An Approach to Assess the Optimality of Refining RC4. *Third International Conference on Computer, Communication, Control and Information Technology (C3IT)*.

Dogan, S., & Akbal, E. (2017). Analysis of Mobile Phones in Digital Forensics. *2017 40th Convention on Information and Communication Technology, Electronoics and Microelectronics*, 1241–1244.

Gayed, T. F., Lounis, H., & Bari, M. (2012). Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web. *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 19–23.

Giova, G. (2011). Improving Chain of Custody in Forensic Investigation of Electronic Digital Sistems. *International Journal of Computer Science and Network Security*, *11*(1), 1–9.

Harbawi, M., & Varol, A. (2017). An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I : *2017 5Tth International Symposium on Digital Forensic and Security*, 6.

Marshall, A. M. (2008). *Digital Forensics : Digital Evidence in Criminal Investigation*.

Morioka, E., & Sharbaf, M. S. (2016). Digital Forensics Research on Cloud Computing : An investigation of Cloud Forensics Solutions. *IEEE Symposium on Technologies for Homeland Security (HST)*, 1–6.

Pehlivanoğlu, M., & Duru, N. (2015). Email Encryption using RC4 Algorithm. *International Journal of Computer Applications*, *130*(14), 25–29.

Prayudi, Y. (2014). Problema dan Solusi Digital Chain Of Custody. *Seminar Nasional Aplikasi Teknologi Informasi (Senasti), 2011*, 197–204.

Prayudi, Y., Ashari, A., & Priyambodo, T. (2019). The pseudo metadata concept for the chain of custody of digital evidence. *International Journal of Electronic Security and Digital Forensics*, *11*, 395. https://doi.org/10.1504/IJESDF.2019.102554

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets : A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*, *107*(9), 30–36.

Prayudi, Y., & SN, A. (2015). *Digital Chain of Custody : State of the Art*. *114*(5), 1–9.

Widjaja, A., & Kalabadzi, A. (2017). CRYPTOGRAPHIC ALGORITHM WITH APPLICATIONS RC4 AND RSA WEB BASED ON PT PACKET SISTEMS INDONESIA. *International Journal of Pure and Applied Mathematics*, *117*(15), 805–816.

Wu, M., & Chen, L. (2016). Image recognition based on deep learning. *Proceedings - 2015 Chinese Automation Congress, CAC 2015*, 542–546. https://doi.org/10.1109/CAC.2015.7382560