



**MANAJEMEN PENGELOLAAN BUKTI DIGITAL UNTUK
MENINGKATKAN AKSESIBILITAS LABORATORIUM
FORENSIKA DIGITAL**

Moch Bagoes Pakarti
15917217

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2020

Lembar Pengesahan Pembimbing

MANAJEMEN PENGELOLAAN BUKTI DIGITAL UNTUK MENINGKATKAN AKSESIBILITAS LABORATORIUM FORENSIKA DIGITAL

Moch Bagoes Pakarti

15917217

Yogyakarta, 9 Juli 2020



Pembimbing I

Dhomas Hatta Fudholi, ST., M.Eng., Ph.D

Pembimbing II

Dr. Yudi Prayudi, S.Si., M.Kom

Lembar Pengesahan Penguji

Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Laboratorium Forensika Digital

Moch Bagoes Pakarti
15917217

Yogyakarta, 25 Juli 2020

Tim Penguji,

Dhomas Hatta Fudholi, ST., M.Eng., Ph.D

Ketua

Dr. Yudi Prayudi, S.Si., M.Kom

Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia



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

Abstrak

MANAJEMEN PENGELOLAAN BUKTI DIGITAL UNTUK MENINGKATKAN AKSESIBILITAS LABORATORIUM FORENSIKA DIGITAL

Pengelolaan bukti digital membutuhkan penanganan khusus yang dapat menyimpan dan menjaga integritas bukti digital. Permasalahan yang ada saat ini adalah tidak adanya konsep penyimpanan bukti digital yang dapat diakses secara online yang memiliki aksesibilitas yang lebih luas. Manajemen pengelolaan bukti digital daring diusulkan sebagai solusi untuk memecahkan masalah tersebut. Konsep ini berupa sebuah sistem manajemen bukti digital *online* yang dapat diakses dimana saja dan kapan saja serta menyajikan data bukti digital yang ada secara aktual dengan tetap menjaga sifat-sifat bukti digital agar dapat diterima secara hukum. Permasalahan pada manajemen bukti digital tersebut membutuhkan Sistem Manajemen untuk Bukti Digital yang sesuai untuk diterapkan dilingkungan Laboratorium Forensika Digital UII. Penelitian ini telah berhasil mengimplementasikan konsep Data Inventory. Diharapkan dengan adanya konsep Manajemen Barang Bukti Digital ini kontrol barang bukti digital dan segala aktivitas yang berkaitan dengannya dapat terjaga serta terdokumentasi dengan baik dan menjangkau area yang lebih luas dapat diakses dimana saja dan kapan saja.

Kata kunci

bukti digital, *chain of custody*, aksesibilitas

Abstract

DIGITAL EVIDENCE MANAGEMENT TO IMPROVE DIGITAL FORENSICS LABORATORY ACCESSIBILITY

Management of digital evidence requires special handling that can store and maintain the integrity of digital evidence. The current problem is that there is no concept of storing digital evidence that can be accessed online that has wider accessibility. Online digital evidence management is proposed as a solution to solve this problem. This concept is in the form of an online digital evidence management system that can be accessed anywhere and anytime and presents the actual digital evidence data while maintaining the characteristics of digital evidence so that it can be legally accepted. The problems with digital evidence management require a Management System for Digital Evidence that is suitable for use in the UII Digital Forensics Laboratory. This research has successfully implemented the concept of Data Inventory. It is expected that with this Digital Evidence Management concept digital control of evidence and all activities related to it can be maintained and well documented and reach a wider area can be accessed anywhere and anytime.

Keywords

Chain of custody, digital evidence, accessibility

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, 25 Juli 2020



Moch Bagoes Pakarti

Daftar Publikasi

Pakarti, M.B., Fudholi, D.H., & Prayudi, Y. (2021). Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Laboratorium Forensika Digital. *Jurnal Ilmiah Sinus*, Vol. 19 No. 1 Januari 2021

Saputro, F. H., & Pakarti, M. B. (2018). Evaluasi Penerapan E-Learning sebagai Media Pembelajaran Perkuliahan Online bagi Mahasiswa Universitas Sahid Surakarta. *Tekinfo: Jurnal Ilmiah Teknik Industri Dan Informasi*, 5(2), 106–112. <https://doi.org/10.31001/tekinfo.v5i2.235>

Publikasi yang menjadi bagian dari tesis

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Moch Bagoes Pakarti	Mendesain eksperimen (60%) Menulis <i>paper</i> (100%)
Dr. Yudi Prayudi, S.Si., M.Kom	Mendesain eksperimen (40%)
Dhomas Hatta Fudholi, ST., M.Eng., Ph.D	Melakukan Evaluasi dan Analisis

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

“Dengan rahmat Allah yang Maha Pengasih lagi Maha Penyayang,”

Karya ini penulis persembahkan kepada :

Bapak **Masngudi** dan Ibu **Kustinah** yang tidak pernah berhenti memberikan dukungan dan doa

Istriku **Khamsatul Faizati** dan kedua putri kesayanganku **Shafiyyah Az Zahra** dan **Karizma Arawinda** yang senantiasa menemani dan memberikan semangat hingga karya ini selesai

Kata Pengantar

Syukur Alhamdulillah penulis ucapkan kepada kehadiran 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. Terima kasih penulis ucapkan kepada berbagai pihak :

1. Rektor Universitas Islam Indonesia, Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D yang memberikan kesempatan kepada penulis untuk menimba ilmu di Universitas Islam Indonesia
2. Dekan Fakultas Teknologi Industri Universitas Islam Indonesia, Bapak Prof. Dr. Ir. Hari Purnomo, M.T yang memberikan fasilitas pembelajaran.
3. Ketua Program Studi Informatika Program Magister Universitas Islam Indonesia, Ibu Izzati Muhimmah, ST, M.Sc., Ph.D.
4. Dhomas Hatta Fudholi, ST., M.Eng., Ph.D, Dr. Yudi Prayudi, S.Si., M.Kom, dan Dr. Ir. Bambang Sugiantoro, S.Si., M.T.selaku dosen pembimbing dan penguji yang telah memberikan pengarahan, bimbingan, masukan, serta semangat selama pelaksanaan penulisan Tesis.
5. Rekan-rekan Mahasiswa MI UII XII yang telah berjuang bersama
6. Ketua STP Sahid Surakarta Bapak Dr. Budi Purnomo M.Hum yang telah memberikan kesempatan untuk menjalankan study S2 di UII Yogyakarta.

Kritik dan saran dari semua pihak yang bersifat membangun selalu penulis harapkan. Semoga Tesis ini dapat memberikan manfaat kepada kita semua. Akhir kata, penulis sampaikan terima kasih kepada semua pihak yang telah berperan serta dalam penyusunan Tesis ini dari awal sampai akhir.

Yogyakarta, 25 Juli 2020

Moch Bagoes Pakarti

Daftar Isi

Lembar Pengesahan Pembimbing.....	i
Lembar Pengesahan Penguji	ii
Abstrak	iii
Abstract	iv
Pernyataan Keaslian tulisan	v
Daftar Publikasi.....	vi
Halaman Kontribusi	vii
Halaman Persembahan	viii
Kata Pengantar	ix
Daftar Isi.....	x
Daftar Tabel	xii
Daftar Gambar.....	xiii
BAB 1 Pendahuluan.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Manfaat Penelitian	4
1) Studi Pustaka.....	4
2) Pembuatan Kategori bukti digital.....	5
3) Pembagian Aktivitas Terhadap Sistem	5
4) Pembuatan Konsep Penyimpanan Bukti Digital	5
5) Perancangan Desain Halaman Antarmuka.....	5
6) Implementasi	5
7) Simulasi Kasus.....	6
1.7 Struktur Penelitian.....	6
BAB 2 Tinjauan Pustaka.....	8
2.1 Pendahuluan	8
2.2 Bukti Digital.....	15
2.3 Chain of Custody	18
2.4 Metadata.....	19
2.5 Konsep Lemari Penyimpanan Bukti Digital	20
2.6 Standar Pencatatan Bukti Digital	21
BAB 3 Metodologi Penelitian.....	23
3.1 Studi Pustaka.....	23

3.2	Pemetaan Data Chain of Custody Bukti Digital	24
3.3	Pembuatan Kategori Bukti Digital	25
3.4	Pembagian Aktivitas Terhadap Sistem	27
3.5	Konsep Desain Formulir Chain of Custody	31
3.6	Pembuatan Konsep Penyimpanan Bukti Digital	33
3.7	Perancangan Desain Halaman Antarmuka	35
3.8	Implementasi	39
3.9	Simulasi Kasus	39
3.10	Pengujian	39
3.11	Hasil dan Kesimpulan	39
BAB 4 Implementasi dan Pembahasan		40
4.1	Implementasi Sistem	40
4.1.1	Alur Sistem	40
4.1.3	Implementasi Antar muka	44
4.1.4	Implementasi Database	47
4.2	Perangkat Pendukung Penelitian	52
4.2.1	Perangkat Keras	53
4.2.2	Perangkat Lunak	53
4.2.3	Arsitektur Jaringan	54
4.3	Simulasi Kasus	55
4.4	Pengujian Sistem	56
4.4.1	Pengujian Dengan Metode <i>Black Box</i>	57
4.4.2	Pengujian Nilai Hash	64
4.4.4	Analisis Kelebihan dan Kekurangan Sistem	67
Bab 5 Kesimpulan dan Saran		71
5.1	Kesimpulan	71
5.2	Saran	71
Daftar Pustaka		72

Daftar Tabel

Tabel 2. 1 Perbandingan Penelitian Terdahulu	9
Tabel 2. 2 Standar Laporan Bukti Digital	21
Tabel 3. 1 Komponen Chain of Custody	24
Tabel 4. 1 Komponen Tabel Kejahatan	47
Tabel 4. 2 Komponen Tabel jenis_kejahatan	48
Tabel 4. 3 Komponen Tabel User	49
Tabel 4. 4 Komponen tabel record	49
Tabel 4. 5 komponen tabel kasus	51
Tabel 4. 6 Spesifikasi Laptop yang Digunakan	53
Tabel 4. 7 Spesifikasi PC Server yang Digunakan	53
Tabel 4. 8 Deskripsi Simulasi Kasus.....	56
Tabel 4. 9 Rencana Pengujian.....	57
Tabel 4. 10 Pengujian Sign In	58
Tabel 4. 11 Pengujian Tambah Data Pengguna	59
Tabel 4. 12 Pengujian Ubah Data Pengguna.....	59
Tabel 4. 13 Unggah Bukti Digital	60
Tabel 4. 14 Input Kelengkapan Data Bukti Digital	61
Tabel 4. 15 Aktivasi Status Kasus.....	61
Tabel 4. 16 Unduh Form Chain of Custody	62
Tabel 4. 17 Unduh Bukti Digital.....	62
Tabel 4. 18 Melengkapi Data Kasus	63
Tabel 4. 19 Perubahan Data Statistik Dashboard.....	63
Tabel 4. 20 Perubahan Data Interaksi Bukti Digital	64
Tabel 4. 21 Perbandingan Hasil Nilai hash pada File BB hp.E01.	64
Tabel 4. 22 Perbandingan Hasil Nilai hash pada File 19111200113UQ0F.mp4..	65
Tabel 4. 23 Perbandingan Hasil Nilai hash pada File file Picture 001.jpg.	65
Tabel 4. 24 Perbandingan <i>Chain of Custody</i> dengan Peneltian Sebelumnya	66
Tabel 4. 25 Perbandingan Aksesibilitas Bukti Digital	68
Tabel 4. 26 Tabel Penilaian <i>expert</i>	69

Daftar Gambar

Gambar 2. 1 Proses Utama Forensika Digital.....	16
Gambar 3. 1 Alur Penelitian.....	23
Gambar 3. 2 Use Case Pembagian Hak Otorisasi pada <i>First Responder</i>	28
Gambar 3. 3 Use Case Pembagian Hak Otorisasi pada <i>Investigator</i>	29
Gambar 3. 4 Use Case Pembagian Hak Otorisasi pada <i>Officer</i>	30
Gambar 3. 5 Use Case Pembagian Hak Otorisasi pada Officer	31
Gambar 3. 6 Konsep Desain Form Chain of Custody bagian pertama	32
Gambar 3. 7 Konsep Desain Form Chain of Custody bagian kedua	33
Gambar 3. 8 Konsep Desain Form Chain of Custody.....	33
Gambar 3. 9 Alur Penanganan Bukti Digital pada Sistem Penyimpanan Bukti Digital.....	34
Gambar 3. 10 Konsep Desain Halaman login.....	35
Gambar 3. 11 Konsep Desain Halaman Input Kasus Baru	36
Gambar 3. 12 Konsep Desain Halaman Detail Kasus.....	37
Gambar 3. 13 Konsep Desain Halaman Investigator	38
Gambar 3. 14 Konsep Desain Halaman Investigator	38
Gambar 4. 1 Alur Kerja Sistem.....	41
Gambar 4. 2 Form Chain of Custody Halaman Pertama	42
Gambar 4. 3 Form Chain of Custody halaman kedua.....	44
Gambar 4. 4 Menu Login	44
Gambar 4. 5 Halaman Beranda <i>first responder</i>	45
Gambar 4. 6 Halaman input data <i>first responder</i>	45
Gambar 4. 7 Halaman <i>officer</i>	46
Gambar 4. 8 Grafik Kejahatan	46
Gambar 4. 9 Management Pengguna	47
Gambar 4. 10 Tabel Kejahatan	47
Gambar 4. 11 Tabel jenis_kejahatan.....	48
Gambar 4. 12 Tabel User	48
Gambar 4. 13 Tabel record.....	49

Gambar 4. 14 Tabel Kasus	50
Gambar 4. 15 Relasi Antar Tabel.....	52
Gambar 4. 16 Halaman NetBeans IDE 8.2	54
Gambar 4. 17 Arsitektur Jaringan	54
Gambar 4. 18 Konfigurasi IP	55
Gambar 4. 19 Konsep aksesibilitas sistem.....	67

Glosarium

APJII	- Asosiasi Penyedia Jasa Internet Indonesia
CoC	- Chain of Custody
DEMC	- Digital Evidence Management Framework
PPBB	- Pejabat Pengelola Barang Bukti
XML	- eXtensible Markup Language

BAB 1

Pendahuluan

1.1 Latar Belakang

Pertumbuhan pengguna internet di Indonesia terus berkembang dengan pesat. Berdasarkan data dari Statista menunjukkan bahwa Indonesia menempati peringkat ke 5 dari negara di seluruh dunia dengan jumlah pengguna internet sebanyak 143 juta pengguna. Hal ini berbanding lurus dengan meningkatnya jumlah kasus *cybercrime* (kejahatan dunia maya) di Indonesia yang menurut Polri jumlah kasus *cybercrime* di Indonesia menempati peringkat kedua di dunia, dimana menjadi tantangan untuk mengelola barang bukti yang terkait dengan kasus *cybercrime*.

Dalam penanganan kasus *cyber crime* terdapat dua jenis barang bukti, yaitu bukti elektronik dan bukti digital. Bukti elektronik memiliki wujud fisik yang dapat dilihat dan diraba wujudnya, seperti: komputer, handphone, flashdisk, laptop serta perangkat penyimpanan lainnya.

Pada buku “Digital Evidence and Computer Crime Forensic Science, Computer and the Internet 3 rd Edition” (Casey, 2000) Bukti digital didefinisikan sebagai data yang dapat memberikan pernyataan dari sebuah tindak kejahatan yang telah terjadi, atau data yang dapat menghubungkan antara kejahatan dengan korban atau antara kejahatan dan pelakunya. Ada pendapat lain yang menyebutkan bahwa bukti digital adalah sebuah abstraksi dari beberapa objek digital atau kejadian (Venema & Farmer, 2000).

Barang bukti elektronik dan digital yang telah diperoleh harus didokumentasikan atau disebut sebagai CoC (Chain of Custody). *Chain of custody* memuat informasi dasar barang bukti yang diamankan. Pada bukti digital informasi dasar yang dicatat adalah: nama, ukuran dan fungsi hash. Informasi tersebut dikenal dengan istilah metadata. Dalam hal ini, selain metadata yang bersifat statis terdapat juga informasi yang bersifat dinamis yang akan diisi oleh

penyidik, misalnya: nama investigator, nomor kasus, tanggal barang bukti digital tersebut masuk atau diunduh dari komputer. Penanganan bukti digital baik fisik maupun digital seharusnya memiliki prosedur yang sama. Salah satu bentuk kesamaan penanganan tersebut adalah dalam bentuk penanganan yang standar untuk dokumentasi dan pencatatan pada form *chain of custody* (Jeff, 2016).

Pengelolaan bukti digital tidak kalah penting dengan pengelolaan bukti elektronik. Bukti elektronik yang berbentuk fisik dapat dikelola dan disimpan dalam ruangan khusus dengan rak atau lemari penyimpanan.

Bukti digital disimpan dan dikelola oleh sebuah laboratorium forensika digital. Dimana terjadi proses Akuisisi, *imaging*, eksplorasi dan analisa untuk menyelesaikan kasus *cyber crime*. Untuk kebutuhan penyelidikan data hasil pengelolaan dapat dimanfaatkan oleh laboratorium yang lain.

Terdapat beberapa penelitian yang dilakukan berkaitan dengan pengelolaan bukti digital. Penelitian pertama dilakukan oleh (Tamer, Hakim, & Moncef, 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 kedua dilakukan oleh (Jasmin, Zoran, & Miroslav, 2011) mengangkat isu tentang pengelolaan CoC pada dengan pendekatan ontologis pada bukti digital.

Penelitian ketiga 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 keempat dilakukan oleh (Prayudi, Ashari, & Priyambodo, 2014) yang mengangkat isu tentang pembuatan digital evidence cabinet sebagai pendekatan baru dalam penanganan barang bukti digital. Penelitian kelima dilakukan oleh (Widatama & Prayudi, 2018) mengangkat isu penggunaan XML untuk mendukung form CoC pada lemari penyimpanan bukti digital.

Pada ilmu forensika digital terdapat sebuah prinsip dasar yang disebut Locard's Exchange yang menyatakan bahwa setiap kontak yang terjadi antara benda-benda pasti akan meninggalkan jejak (Prayudi & Priyambodo, 2015). Hal

ini juga berlaku pada bukti digital sehingga perlu diperhatikan dalam proses pengelolaan bukti digital itu sendiri, supaya bukti digital yang sudah dikelola memiliki kredibilitas dan dapat dipertanggung jawabkan.

Saat ini belum ada sistem pengelolaan bukti digital daring yang dapat memberikan akses yang lebih luas. Sistem yang ada saat ini hanya dapat diakses ketika berada di lingkungan laboratorium forensika digital saja. Kendala yang dihadapi dengan adanya keterbatasan sistem ini yaitu lambannya proses penyimpanan bukti digital. Hal ini disebabkan oleh pengaruh jarak dan waktu ketika petugas harus datang ke laboratorium forensika digital secara langsung untuk mengantar bukti digital yang telah diakusisi.

Dengan memanfaatkan konsep lemari penyimpanan bukti digital yang diimplementasikan secara daring pada laboratorium forensika digital maka akan lebih mudah dalam menghimpun data yang tersebar. Data yang dikelola dapat dipantau secara daring, kemudian data ini dapat dikelola menjadi informasi yang dapat digunakan untuk membantu dalam proses pengambilan keputusan dan kebijakan.

Maka perlu dibuat sebuah sistem yang dapat menangani bukti digital pada laboratorium forensika digital. Sistem ini dapat diakses secara daring dengan pembagian hak akses pengguna yang berbeda-beda namun tetap menjaga integritas bukti digital dengan hasil keluaran berupa formulir *chain of custody* dan log pengguna. Dari data bukti digital yang sudah dikelola dapat disajikan informasi melalui dashboard sesuai dengan kebutuhan.

1.2 Rumusan Masalah

Dari penjabaran permasalahan pada latar belakang, dapat diambil beberapa rumusan masalah yaitu:

1. Bagaimana mekanisme pengelolaan bukti digital yang dapat diakses dari mana saja dan kapan saja?
2. Bagaimana konsep formulir pencatatan data bukti digital untuk mendukung *Chain of Custody*?
3. Apa saja kebutuhan informasi yang perlu disajikan secara aktual?

1.3 Batasan Masalah

Agar permasalahan tidak terlalu luas, maka penelitian ini dibatasi pada beberapa topik permasalahan diantaranya:

1. Data bukti digital yang digunakan adalah data yang disimpan pada lemari penyimpanan bukti digital.
2. Aplikasi yang dibuat sebagai media implementasi dan pengujian terbatas pada pengambilan data dan penyajian informasi dari bukti digital yang dikelola.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Memodelkan mekanisme dalam pencatatan data bukti digital.
2. Menyediakan akses yang luas dalam mengelola bukti digital.
3. Menyajikan informasi terkait bukti digital yang dikelola untuk keperluan persidangan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Mampu memberikan akses yang lebih mudah dan luas pada pengelolaan bukti digital
2. Mampu mengumpulkan data bukti digital beserta data kasus yang melekat pada bukti digital.
3. Mampu memberikan informasi yang lengkap dan akurat agar dapat diterima oleh hukum.

1.6 Metode Penelitian

Dalam perancangan sistem ini, metodologi penelitian yang penulis pakai adalah sebagai berikut :

1) Studi Pustaka

Dilakukan pada langkah awal untuk menghimpun informasi yang relevan dengan topik atau masalah yang akan diteliti. Sumber-sumber informasi

pada studi pustaka dapat diperoleh melalui buku-buku yang memiliki keterkaitan dengan masalah yang akan diteliti, jurnal ilmiah serta sumber-sumber informasi lainnya yang dapat diperoleh melalui internet.

2) Pembuatan Kategori bukti digital

Melakukan pengelompokan jenis-jenis bukti digital berdasarkan dari media yang digunakan dan jenis kasus *cyber crime*-nya, hal ini dilakukan untuk menentukan keterkaitan antara keduanya sehingga dapat ditarik kesimpulan dan memberikan informasi.

3) Pembagian Aktivitas Terhadap Sistem

Tahapan setelah terkumpulnya informasi melalui tahapan studi pustaka adalah tahapan pembuatan konsep penyimpanan bukti digital. Perancangan konsep ini dimulai dengan memisahkan pembagian hak otorisasi orang-orang yang berinteraksi dengan bukti digital tersebut terhadap sistem manajemen barang bukti digital dan *chain of custody* (coc) pada penyimpanan laboratorium forensika digital.

4) Pembuatan Konsep Penyimpanan Bukti Digital

Alur penyimpanan bukti digital pada konsep ini adalah ketika melakukan akuisisi bukti digital, ia akan menyimpan bukti digital tersebut ke dalam sebuah sistem manajemen bukti digital.

5) Perancangan Desain Halaman Antarmuka

Perancangan antarmuka dilakukan untuk membuat tampilan yang sederhana sehingga dapat dengan mudah digunakan. Perancangan antarmuka dilakukan dengan menggambar secara sederhana tampilan yang akan dibuat.

6) Implementasi

Tahapan ini merupakan aktivitas untuk pembuatan sistem penyimpanan bukti digital berdasarkan perancangan yang telah dibuat sebelumnya. Hal ini untuk memastikan bahwa sistem dapat dijalankan sebagaimana mestinya. Pada tahap ini, pembuatan sistem penyimpanan bukti digital daring.

7) Simulasi Kasus

Tahapan simulasi kasus merupakan tahapan untuk membuat skenario tertentu yang bertujuan untuk membuat kesesuaian antara kebutuhan dengan sistem yang dibuat. Simulasi kasus ini dibuat dengan menggunakan bukti digital dari kasus-kasus tertentu.

1.7 Struktur Penelitian

Tahapan yang menjelaskan secara umum terkait sistematika penulisan yang berisi penjelasan secara ringkas terhadap kerangka penulisan yang digunakan.

BAB I : PENDAHULUAN

Tahap awal dari penelitian berisi penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode serta struktur penulisan yang digunakan. Dalam bagian ini juga dijelaskan mengenai temuan paling relevan dengan penelitian sebelumnya dan kontribusi ilmiah yang diharapkan.

BAB II : KAJIAN PUSTAKA

Tahap ini menjelaskan tentang kajian atas pustaka yang relevan dengan penelitian dan rumusan masalah berupa manajemen dokumentasi bukti digital, *chain of custody* bukti digital, model metadata untuk menentukan rancangan metadata bukti digital serta bahasa pemrograman Java dan XML untuk mendukung penerapan konsep metadata sebagai *chain of custody* bukti digital.

BAB III : METODOLOGI PENELITIAN

Menguraikan metode penelitian yang digunakan untuk memperoleh data dan informasi sesuai dengan topik penelitian. Pada penelitian ini, metodologi yang digunakan adalah berbasis penelitian desain (*design research*).

BAB IV : ANALISIS DAN PERANCANGAN

Menjelaskan kebutuhan informasi metadata, analisis dan perancangan model informasi metadata yang digunakan serta aplikasi/sistem yang dibangun sebagai wujud implementasi model metadata.

BAB V : IMPLEMENTASI DAN PEMBAHASAN

Menjelaskan penerapan atau implementasi dari rancangan model metadata dan aplikasi yang telah dibuat. Memaparkan hasil analisis dan

pembahasan terkait model informasi metadata yang digunakan dan aplikasi/sistem dokumentasi *chain of custody* terhadap proses manajemen bukti digital.

BAB VI : PENUTUP

Berisi simpulan dari hasil penelitian disertai dengan beberapa saran

DAFTAR PUSTAKA

BAB 2

Tinjauan Pustaka

2.1 Pendahuluan

Terdapat beberapa penelitian terdahulu yang dilakukan berkaitan dengan pengelolaan bukti digital. Penelitian pertama dilakukan oleh (Tamer, Hakim, & Moncef, 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 kedua dilakukan oleh (Jasmin, Zoran, & Miroslav, 2011) mengangkat isu tentang pengelolaan CoC pada dengan pendekatan ontologis pada bukti digital. Penelitian ini membandingkan berbagai model dan kerangka kerja yang ada dan dikembangkan dalam beberapa tahun terakhir dan mengusulkan kerangka kerja baru berdasarkan "rantai bukti digital". Kerangka kerja ini akan dimodelkan menggunakan diagram UML - Use Case and Activity.

Penelitian ketiga 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. Melakukan upaya untuk menjaga integritas bukti digital serta prosedur untuk melakukan dokumentasi secara kronologis terhadap bukti. Karakteristik bukti digital telah menyebabkan rantai penanganan tahanan menjadi lebih rumit dan kompleks

Penelitian keempat dilakukan oleh (Prayudi, Ashari, & Priyambodo, 2014) yang mengangkat isu tentang pembuatan digital evidence cabinet sebagai pendekatan baru dalam penanganan barang bukti digital.

Penelitian kelima dilakukan oleh (Widatama & Prayudi, 2018) mengangkat isu penggunaan XML untuk mendukung form CoC pada lemari penyimpanan bukti digital. Penyimpanan bukti digital dimana informasi metadata bukti digital dan *chain of custody* disimpan pada struktur XML. Setelah informasi bukti digital telah tersimpan dalam bentuk strukturXML, selanjutnya adalah mengenkripsinya dengan menggunakan algoritma RC4.

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: <i>digital evidence management frameworks</i> , <i>digital evidence bags</i> dan <i>secure communication</i> .	Tersimpannya bukti digital pada digital evidence cabinet dan pembatasan akses terhadap bukti digital.
2.	(Prayudi, 2014)	Penanganan <i>chain of custody</i> pada bukti digital.	Penggunaan <i>tools</i> tertentu.	<p>1. Pendekatan <i>evidence oriented design</i> yaitu <i>tools</i> yang mampu mendukung aktifitas proses investigasi.</p> <p>2. Pemodelan yang telah digunakan dalam forensika umum yaitu kantung barang bukti digital (<i>sealed digital evidence bag</i>).</p>	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.	<p>1. Penggunaan konsep DEMC (Digital Evidence Management Framework).</p> <p>2. Penerapan UML dan UMML dengan tujuan untuk menyajikan data proses perencanaan (<i>planning performing</i> dan aktivitas forensika yang terjadi.</p>	Integritas dan kredibilitas prosedur dalam penanganan <i>chain of custody</i> pada bukti digital.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
4.	(Giova, 2011)	Kualitas bukti digital untuk diajukan ke pengadilan.	Pengembangan format AFF4 (<i>Advanced Forensic Format</i>) sebagai <i>tool</i> forensika dan penggunaan RDF (<i>Resource Description Format</i>).	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 <i>chain of custody</i> dari bentuk dokumen ke bentuk digital.	Penggunaan <i>semantic web</i> untuk merepresentasikan informasi <i>chain of custody</i> .	<i>Semantic web</i> digunakan untuk mengatur format struktur XML pada RDF.	Informasi <i>Chain of custody</i> bukti digital dapat dilihat pada halaman web.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
6.	(Ćosić, Ćosić, & Bača, 2011)	Pengelolaan pada bukti digital.	Pendekatan ontologis terhadap <i>bukti digital</i> .	<p>Membuat hirarki pada bukti digital, berikut adalah penjelasannya:</p> <ol style="list-style-type: none"> 1. <i>Characteristic</i>, yaitu sumber dan tipe. Sumber berupa: <ol style="list-style-type: none"> a. <i>Personal Computer</i>, yaitu: Laptop, Netbooks, Notebooks, Server, Desktop. b. Cloud (penyimpanan virtual), yaitu: <i>magnetic, flash, optical</i>. c. LSDD (<i>Large Scale Digital Devices</i>): kamera digital, telepon, dll. <p>Sedangkan <i>type</i> berupa: <i>Original, best copy, working copy</i>.</p> 2. Dynamics (hal-hal apa saja yang berpengaruh serta jenis bukti digital), dibagi menjadi 3 yaitu: <i>equipment (hardware and software)</i> dan <i>human</i> dan <i>natural dynamics</i>. <i>Human dynamics</i> (orang terlibat secara langsung maupun tidak 	<p>Pemahaman terhadap pengelolaan bukti digital yang melibatkan 2 domain, yaitu: <i>forensic investigator</i> terhadap bukti digital dan <i>forensic investigator</i> terhadap <i>tools</i> yang digunakan untuk memperoleh bukti digital.</p>

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
				<p>3. langsung terhadap kasus yang sedang dihadapi) yaitu:</p> <ul style="list-style-type: none"> a. <i>First responder</i>. b. Investigator. c. <i>Prosecution</i> (pihak penuntut). d. <i>Court</i> (pihak pengadilan). e. <i>Victim</i> (korban). f. <i>Suspect</i> (Tersangka). <p><i>Natural dynamics</i> (hal-hal yang dapat merusak bukti digital):</p> <ul style="list-style-type: none"> a. <i>Earthquake</i> (gempa bumi). b. <i>Fire</i> (kebakaran). c. <i>Weather</i> (Cuaca). <p>4. <i>Factors</i> (jawaban atas pertanyaan <i>what, where, who, why, when</i> dan <i>how</i> terhadap bukti digital).</p> <ul style="list-style-type: none"> a. <i>What</i>, jenis bukti digital yang diperoleh. b. <i>Where</i>, dimana lokasi bukti digital. c. <i>Who</i>, siapa saja yang terlibat pada bukti digital tersebut. 	

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
				<ul style="list-style-type: none"> d. <i>When</i>, kapan bukti digital tersebut diperoleh. e. <i>How</i>, bagaimana bukti tersebut diperoleh. 5. <i>Institutions</i>, tempat diperolehnya bukti digital. 6. <i>Integrity</i>, penjelasan mengenai <i>tools</i> dan metode yang digunakan untuk memperoleh bukti digital. 	
7.	(Widjaja & Kalabadzi, 2017)	Penerapan metode enkripsi untuk pengamanan pengiriman informasi pada Perusahaan Packet Systems 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 <i>file</i> harus melalui enkripsi terlebih dahulu, setelah terenkripsi, <i>file</i> maupun teks dapat dikirim melalui email.	<i>File</i> hasil enkripsi dalam bentuk ekstensi .psi. Terdapat 9 jenis <i>file</i> yang berhasil dienkripsi, yaitu: .rar, .docx, .mp3, .pdf, .png, .jpg, .xlsx, .vsd, .mp4.

Tabel 2.1 Perbandingan Penelitian Terdahulu (lanjutan)

No.	Paper	Isu	Solusi	Metode	Hasil
8.	(Widatama & Prayudi, 2018)	Pengembangan konsep lemari penyimpanan bukti digital untuk mendukung implementasi digital <i>chain of custody</i> form serta penggunaan mekanisme tertentu untuk pengamanan informasi bukti digital.	akses bukti digital berdasarkan peran petugas dalam penanganan kasus. Metode enkripsi digunakan sebagai pengamanan informasi bukti digital yang telah tersimpan.	Penyimpanan bukti digital dimana informasi metadata bukti digital dan <i>chain of custody</i> disimpan pada struktur XML. Setelah informasi bukti digital telah tersimpan dalam bentuk struktur XML, selanjutnya adalah mengenkripsinya dengan menggunakan algoritma RC4.	Lemari penyimpanan bukti digital yang dapat menghasilkan informasi bukti digital yang telah terenkripsi yang sulit terbaca.
	Penyimpanan bukti digital secara daring yang mampu menghasilkan formulir <i>chain of custody</i> serta informasi yang disajikan dalam bentuk <i>dashboard</i> . Sistem yang dirancang memberikan kemudahan akses bukti digital yang lebih luas dengan mengabaikan keterbatasan waktu dan lokasi.				

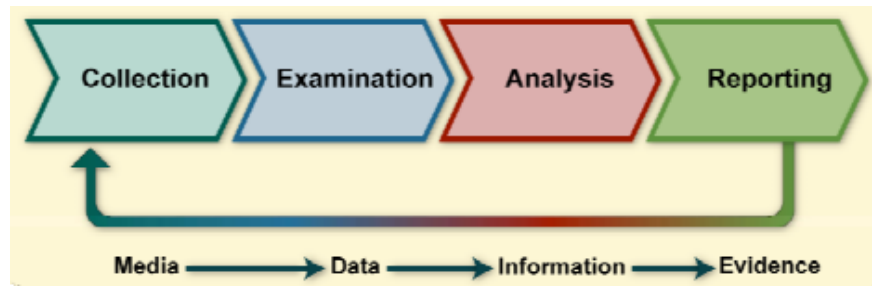
2.2 Bukti Digital

Bukti Digital merupakan barang bukti yang umumnya ditemukan pada kejahatan siber (cyber crime) dan kejahatan yang melibatkan perangkat elektronik. Bukti digital adalah obyek digital yang mengandung informasi handal dalam mendukung atau menolak terkait kasus kejahatan dalam proses investigasi (Carrier, 2005). Di Indonesia, pedoman hukum cyber yaitu Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) tidak mencantumkan istilah bukti digital. Akan tetapi di dalam UU ITE tersebut dikenal dua istilah alat bukti elektronik yaitu Informasi Elektronik dan dokumen Elektronik. Alat bukti elektronik ialah Informasi Elektronik dan Dokumen Elektronik yang memenuhi persyaratan formil dan materiil yang diatur di dalam Undang-Undang ITE. Sesuai Pasal 5 ayat (1) UU ITE menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetakannya merupakan alat bukti (Digital Evidence) hukum yang sah.

Sedangkan yang dimaksud dengan Informasi Elektronik dalam Pasal 1 ayat (1) UU ITE bahwa Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto elektronik data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Yang dimaksud dengan Dokumen Elektronik dalam Pasal 1 ayat (2) UU ITE adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. 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:

Dalam prosedur forensika digital, terdapat prosedur dasar yang sering digunakan, yaitu: *collection*, *examination*, *analysis* dan *reporting* (Dogan & Akbal, 2017), berikut adalah proses dari forensika digital:



Gambar 2. 1 Proses Utama Forensika Digital

Tahap *Collection* (Pengumpulan Data) meliputi aktivitas identifikasi sumber data yang relevan terkait kasus, pelabelan dan pencatatan. Dalam tahapan ini seluruh prosedur yang dilakukan harus sesuai dengan pedoman dan Standar Operasional Prosedur yang berlaku untuk menjaga integritas barang bukti digital. Termasuk di dalamnya melakukan verifikasi integritas data (Nilai Hash, MD5 atau SHA-1) dari data asli dan hasil akuisisi.

Tahap *Examination* (Pemeriksaan) meliputi aktivitas penggunaan *tools* atau perangkat lunak dan teknik tertentu untuk melakukan identifikasi dan ekstraksi informasi yang relevan. Tahap pemeriksaan dapat menggunakan *tools* otomatis atau melalui proses manual.

Tahap *Analysis* (Analisis) merupakan aktifitas analisis terhadap hasil pemeriksaan untuk mendapatkan informasi yang berguna sehingga diperoleh kesimpulan.

Tahap *Reporting* (Pelaporan) merupakan aktivitas yang memuat tindakan, prosedur, alat yang digunakan dan memberikan rekomendasi perbaikan kebijakan dan petunjuk dalam aspek proses forensik.

Sedangkan definisi bukti digital menurut (Harbawi & Varol, 2017) adalah jejak yang diinginkan maupun tidak diinginkan yang berasal dari perubahan data digital pada perangkat elektronik. Berdasarkan sumbernya, bukti digital terbagi menjadi 2 kategori (Marshall, 2008), yaitu *closed system* dan *open system*. *Closed system* merupakan sistem yang pernah terkoneksi internet. Artinya, sistem tersebut sangat terisolasi dan hanya terhubung dengan sistem pada komputer yang lain. Berbeda dengan *closed system*, *open system* merupakan sistem yang terhubung dengan internet meskipun sistem tersebut tidak terhubung dengan sistem pada komputer lain, contohnya ketika seseorang menghubungkan laptop pada WiFi.

Menurut 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.

Berikut beberapa contoh barang bukti digital yaitu: *Logical file, Deleted File, Lost File, File slack, Log File, Encrypted File, Steganography file, Office file, Audio File, video File, Image file, Email, User ID dan Password, Short Message Service (SMS), Multimedia Message Service (MMS), Call Logs*. Bukti digital juga adalah *file* bukti digital hasil ekstraksi (*full copy*) bit per bit dari media penyimpanan yaitu *hard drives, flash drives, floppy disk* dan *optical media* yang dikenal dengan istilah *Disk Image*.

Menurut (Kuntze, Rudolph, Richter, Kuntze, & Rudolph, 2017) untuk dapat diterima di persidangan barang bukti digital harus memenuhi karakteristik bukti digital yaitu Admissible (layak), Authentic (Asli), Complete (Lengkap), Reliable (Dapat dipercaya) dan Believable (terpercaya).

- **Admissible**

Barang bukti digital harus sesuai dengan fakta dan masalah yang terjadi dan dapat diterima serta digunakan secara hukum mulai dari proses penyidikan sampai ke pengadilan.

- **Authentic**

Bahwa barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan barang bukti bukan hasil rekayasa. Barang bukti adalah masih asli dan tidak pernah diubah-ubah.

- **Complete**

Barang bukti harus lengkap dan dapat membuktikan tindakan jahat yang dilakukan pelaku kejahatan. Barang bukti yang dikumpulkan, tidak cukup hanya berdasarkan satu perspektif dari sebuah kejadian yang berlangsung.

- **Reliable**

Barang bukti yang dikumpulkan harus dapat dipercayai. Pengumpulan barang bukti dan analisis yang dilakukan harus sesuai prosedur dan dilakukan dengan jujur. Selain itu barang bukti tidak boleh meragukan dan benar benar harus dapat dipercayai serta sesuai dengan prosedur yang SOP yang berlaku.

2.3 Chain of Custody

Chain of custody adalah prosedur pencatatan / dokumentasi kronologis barang bukti sejak barang bukti ditemukan, proses duplikasi, penyimpanan barang bukti baik itu secara fisik ataupun digital hingga sampai pada presentasi dan keputusan akhir terhadap barang bukti. *Chain of custody* digunakan untuk memastikan integritas dan orisinalitas dari barang bukti (Prayudi & SN, 2015).

Dokumentasi *chain of custody* selama ini tidak memiliki standar yang baku. Sehingga setiap penegak hukum dapat memiliki form dokumentasi *chain of custody* yang berbeda-beda. Namun untuk dapat diterima di persidangan, sebuah form *chain of custody* setidaknya mencakup informasi “5W dan 1 H” untuk mencatat setiap proses investigasi diantaranya (Cosic, 2017):

- a. Siapa yang terlibat dalam penanganan barang bukti
- b. Kapan waktu setiap proses penanganan barang bukti dilakukan
- c. Bagaimana proses penanganan yang dilakukan terhadap barang barang bukti
- d. Kemana saja alur perjalanan proses penanganan barang bukti itu dibawa dan dimana disimpan
- e. Mengapa pihak tersebut menangannya
- f. Apa saja barang bukti yang telah dikumpulkan

Dalam melakukan *chain of custody*, ada hal-hal yang harus diperhatikan diantaranya (Leintz, n.d.) :

a. *Security and Trust*

Proses *chain of custody* seharusnya mampu menjamin keamanan dan tingkat kepercayaan di persidangan. Menciptakan dan memelihara *chain of custody* artinya menjaga *log* detail terkait dimana barang bukti ditemukan dan *log* seluruh aktivitas yang terjadi pada barang bukti.

b. *Documentation*

Proses *chain of custody* dimulai di Tempat Kejadian Perkara (TKP) yaitu pada saat proses investigasi dan ketika barang bukti pertama kali diperoleh. Dokumentasi yang dilakukan di TKP umumnya dilakukan dengan menggunakan foto-foto TKP dan catatan investigasi awal sampai selesai kasus.

c. *Preventing Contamination*

Merupakan aspek pencegahan barang bukti dari adanya kontaminasi, perubahan dan kerusakan selama proses penanganan. Hal ini berkaitan dengan nilai integritas dan keaslian dari barang bukti. Pihak-pihak yang berwenang dalam mengakses barang bukti, mendokumentasikan, dan menyerahkan merupakan pihak yang bertanggung jawab. Menurut (Cosic & Baca, 2010b) dalam dunia forensika digital, nilai integritas barang bukti digital adalah memastikan bahwa informasi yang terkandung dalam bukti yang dihadirkan lengkap dan tidak mengalami perubahan oleh pihak yang tidak memiliki wewenang otorisasi mulai pada saat diciptakan, penanganan hingga selesai persidangan. Salah satu metode yang dapat digunakan untuk memastikan integritas bukti digital adalah tidak berubahnya nilai fungsi MD5/hash barang bukti digital. MD5 merupakan fungsi hash yang paling umum digunakan dan merupakan pengembangan dari MD4. Fungsi MD5 memiliki panjang 128 bit. MD5 bekerja dengan membawa setiap pesan yang ada dan menghitung total bit yang terdapat pada pesan dan melakukan *message digest* dengan langkah penambahan *padding bit*, penambahan nilai panjang semula, inisialisasi buffer, pengolahan buffer dan pengolahan pesan dalam blok 512 bit

2.4 Metadata

(NISO, 2004) Metadata sering disebut sebagai data atau informasi tentang data atau informasi. Metadata adalah informasi terstruktur yang mendeskripsikan, menjelaskan, menempatkan atau memberikan kemudahan untuk mengambil, menggunakan atau mengelola sumber informasi. Di dalam terminologi lingkungan perpustakaan, umumnya metadata digunakan untuk berbagai skema formal deskripsi sumber, diterapkan pada berbagai tipe obyek baik digital maupun non-digital. Terdapat tiga tipe metadata diantaranya:

a. *Descriptive Metadata*

menggambarkan sumber daya untuk tujuan seperti penemuan dan identifikasi. Mencakup unsur-unsur seperti judul, abstrak, penulis, dan kata kunci

b. Structural Metadata

Menunjukkan bagaimana kumpulan obyek disusun secara bersama-sama menjadi satu, semisal bagaimana halaman-halaman ditata untuk membentuk suatu bab.

c. Administrative Metadata

Menyediakan informasi untuk membantu mengelola suatu obyek, seperti kapan dan bagaimana obyek dibuat, tipe *file* dan informasi teknikal lainnya, serta siapa yang bisa mengaksesnya. Dan salah satu bagian dari *administrative metadata* adalah *preservation metadata* yang mendeskripsikan informasi yang dibutuhkan untuk keperluan arsip dan penyimpanan suatu obyek.

Secara teknis, implementasi metadata dapat menempel secara langsung pada obyek digital atau dapat disimpan secara terpisah. Metadata yang menempel umumnya disimpan dalam *fileheader* untuk memastikan bahwa metadata tidak akan hilang, *file* dan metadata terhubung serta *file* dan metadata diperbaharui secara bersamaan. Sedangkan metadata yang terpisah dengan obyek dapat menyederhanakan pengelolaan metadata dan mendukung fasilitas pencarian dan pengambilan informasi.

Skema metadata adalah set elemen metadata yang dirancang untuk tujuan tertentu, seperti mendeskripsikan jenis informasi tertentu pada sebuah obyek. Skema metadata dapat dibuat menggunakan SGML (*Standard Generalized Mark-up Language*) atau XML (*Extensible Mark-up Language*). Beberapa skema metadata yang telah dikembangkan diantaranya *DublinCore*, *The Text Encoding Initiative (TEI)*, *Metadata Encoding and Transmission Standard (METS)*, *Metadata Object Description Schema (MODS)*, *The Encoded Archival Description (EAD)*, *Learning Object Metadata* dan lain-lain.

2.5 Konsep Lemari Penyimpanan Bukti Digital

Munculnya konsep lemari penyimpanan bukti digital didasarkan atas permasalahan dalam penanganan bukti digital yang berakibat dalam beberapa hal yaitu: model bisnis dari bagian-bagian yang berhubungan langsung dengan bukti digital, penyimpanan informasi metadata bukti digital maupun kontrol akses dan keamanan 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.

2.6 Standar Pencatatan Bukti Digital

Banyaknya *tools* yang ada saat ini dalam penanganan bukti digital membuat format laporan bukti digital menjadi berbeda-beda. Ketika antar investigator menggunakan sebuah *tools* yang berbeda dalam penanganan bukti digital, maka akan terjadi kesulitan dalam pembuatan laporan yang akan dipresentasikan di pengadilan. Hal inilah yang menjadi penyebab dibutuhkan suatu standar tertentu dari setiap untuk mencatat hal-hal apa saja yang harus tercatat dalam laporan bukti digital.

Penelitian tentang standar pencatatan bukti digital ini dilakukan oleh (Bariki, Hashmi, & Baggili, 2010). Dalam penelitiannya, dilakukan beberapa tahap untuk menentukan standar pencatatan bukti digital, berikut adalah prosesnya.

1. Menganalisa fungsi pelaporan bukti digital dari beberapa *tools*, yaitu: FTK versi 1.71, ProDiscover versi 5.5 dan EnCase versi 6.
2. Menganalisa perbandingan laporan dari tiap-tiap *tool* tersebut dengan menggunakan tabel perbandingan.
3. Membuat kuisisioner yang ditujukan untuk komunitas forensika digital tentang temuan data pada tabel. Survei ini ditujukan untuk orang-orang yang memiliki jenjang pendidikan dan orang-orang yang memiliki pengalaman dibidang forensika digital.

Berdasarkan hasil survei dan diskusi tersebut, disimpulkan bahwa standar laporan bukti digital terbagi menjadi 4 bagian utama, yaitu: informasi kasus (*case information*), informasi sumber bukti digital tersebut diperoleh (*evidence source information*), informasi bukti digital (*evidence item*), *chain of custody*. Berikut adalah tabel deskripsi dari keempat bagian utama standar laporan bukti digital.

Tabel 2. 2 Standar Laporan Bukti Digital

Informasi kasus		Keterangan
1.	Nomor Kasus	Nomor urut kasus yang terdaftar
2.	Nama Kasus	Nama Kasus yang diberikan
3.	Deskripsi Kasus	Deskripsi detail kasus
4.	Tanggal pembuatan laporan	Tanggal Laporan dibuat
5.	Nama <i>tool</i> forensik dan versi yang digunakan	Nama Perangkat yang digunakan
6.	Informasi <i>forensic examiner</i> (nama, instansi, alamat, nomor telepon, fax, email, komentar)	Instansi terkait yang melakukan pemeriksaan bukti digital
Informasi Sumber Bukti Digital		Keterangan
1.	Nama bukti digital	<i>File Imaging</i>
2.	<i>Path</i> bukti digital	Lokasi bukti digital disimpan
3.	Tipe <i>file</i> bukti digital	Ekstensi

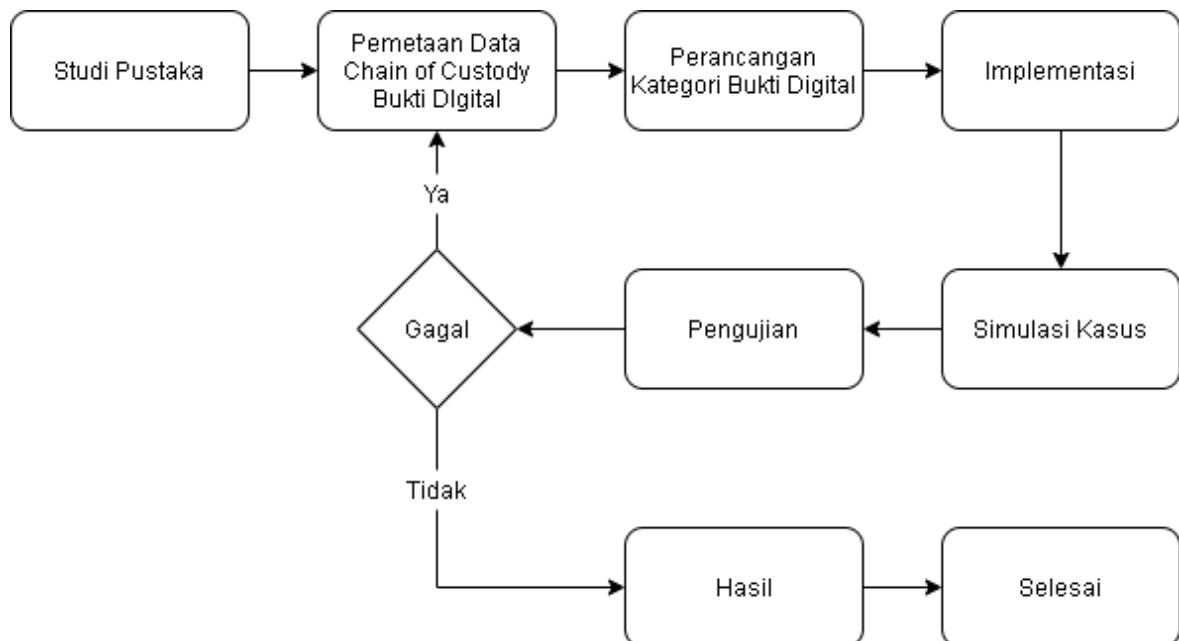
Tabel 2. 3 Standar Laporan Bukti Digital (lanjutan)

Informasi kasus		Keterangan
4.	Ukuran <i>file</i> bukti digital	Ukuran bukti digital
5.	Bukti digital <i>checksum</i>	MD5, SHA1
6.	Waktu yang tertera pada bukti digital	Metadata
7.	Metode <i>write block</i> yang digunakan saat mengambil bukti digital	Nama aplikasi
8.	Informasi pengguna	Nama
9.	Versi sistem operasi	Sistem operasi yang dipakai
10.	Sistem <i>file</i>	Struktur file sistem
11.	Informasi partisi	Jenis partisi yang digunakan
12.	Enkripsi yang digunakan	Jenis: MD5, SHA1
Informasi Bukti Digital		Keterangan
1.	Nama <i>file</i>	Nama dari bukti digital
2.	<i>File path</i>	Lokasi penyimpanan
3.	Tipe <i>file</i>	Ekstensi file
4.	Ukuran <i>logical file</i>	Ukuran file partisi
5.	Ukuran <i>physical file</i>	Ukuran keseluruhan media penyimpanan
6.	<i>Hash (checksum)</i>	Tanda tangan digital
7.	Tanggal dibuat	Tanggal bukti digital diakuisisi
8.	Tanggal diubah	Tanggal bukti digital diubah
9.	Tanggal diakses	Tanggal bukti digital diakses
10.	<i>Sector</i>	Lokasi sector bukti digital
11.	<i>Cluster</i>	Lokasi klaster bukti digital
12.	Dihapus	Apakah <i>file</i> tersebut dalam keadaan terhapus?
13.	Disembunyikan (<i>hidden</i>)	Apakah <i>file</i> tersebut dalam disembunyikan?
14.	Berada pada posisi <i>unallocated cluster</i>	Apakah <i>file</i> tersebut dalam klaster yang belum dipartisi?
15.	<i>Offset</i>	perhitungan
16.	Catatan	Catatatan tambahan mengenai informasi bukti digital
Chain of Custody		
1.	Tanggal	Tanggal pencatatan
2.	Nama pemberi	Nama petugas yang menyerahkan
3.	Nama penerima	Nama petugas yang menerima
5.	Lokasi penerimaan	Tempat serah terima
6.	Deskripsi bukti digital	deskripsi
7.	<i>Change of custody log</i> (tujuan perubahan bukti, metode transfer bukti digital, <i>released by</i> , <i>released date</i> , nama penerima, tanggal diterima, nilai <i>hash</i>)	Jika sewaktu-waktu bukti digital harus digandakan (copy)

BAB 3

Metodologi Penelitian

Pada bab ini dijabarkan skema penelitian dengan menjelaskan setiap alur proses penelitian secara struktur dan sistmatis. Dengan membuat alur penelitian yang sistematis diharapkan dapat membantu menyelesaikan masalah yang ditemui dalam proses penelitian. Permasalahan yang ditemui diselesaikan dengan menemukan solusi yang tepat sehingga penelitian yang dilakukan dapat memberikan hasil yang diharapkan. Alur penelitian pada bab ini dapat dilihat pada gambar 3.1.



Gambar 3. 1 Alur Penelitian

3.1 Studi Pustaka

Studi pustaka dilakukan pada langkah awal untuk menghimpun informasi yang relevan dengan topik atau masalah yang akan diteliti. Sumber-sumber informasi pada studi pustaka dapat diperoleh melalui jurnal ilmiah yang memiliki keterkaitan dengan masalah yang akan diteliti, serta sumber-sumber informasi lainnya yang dapat diperoleh melalui internet. Informasi-informasi yang di dapat juga dapat diperoleh dengan menghadiri seminar-seminar ilmiah yang sering diadakan oleh beberapa universitas.

3.2 Pemetaan Data Chain of Custody Bukti Digital

Di dalam formulir *chain of custody* selain terdapat informasi dokumentasi bukti digital juga terdapat informasi metadata bukti digital. Untuk menghasilkan formulir *digital chain of custody* yang memenuhi standar maka perlu diformulasikan komponen-komponen metadata yang akan disimpan dalam sistem. Metadata yang disimpan dapat dibedakan menjadi metadata statis dan dinamis. Sifat statis merupakan sifat yang dimiliki oleh setiap *field* informasi yang pengisian datanya diisi secara otomatis oleh sistem dan tidak dapat diubah melalui sistem. Sedangkan *field* informasi yang memiliki sifat dinamis, datanya dapat diubah melalui sistem oleh *first responder* atau *investigator*.

Tabel 3. 1 Komponen Chain of Custody Sumber: (Ratnasari, Prayudi, & Sugiantoro, 2018)

No.	Kelompok Informasi	Field Informasi	Sifat		Jenis Informasi
			Statis	Dinamis	
1.	Deskripsi Kasus	No. Kasus		✓	Nomor kasus.
		Kategori		✓	Kategori Kejahatan yang dilakukan
		<i>Suspect</i>		✓	Nama tersangka.
		Victim		✓	Nama korban.
2.	<i>First Responder</i>	Nama lengkap		✓	Nama <i>first responder</i>
		Instansi pekerjaan		✓	Nama institusi tempat <i>first responder</i> bekerja
3.	Olah TKP Bukti Elektronik	Alat		✓	Nama perangkat yang digunakan dalam olah TKP barang bukti (<i>live forensic</i>).
		Waktu		✓	Tanggal dan waktu proses olah TKP.
		Lokasi		✓	Tempat olah TKP dilakukan.
4.	Bukti Elektronik	Model		✓	Nama perangkat bukti elektronik
		<i>Serial Number</i>		✓	Nomor serial dari bukti elektronik.
		<i>Type</i>		✓	Tipe bukti elektronik.
		Manufaktur		✓	Perusahaan pembuat bukti elektronik.
		Spesifikasi teknis		✓	Spesifikasi teknis bukti elektronik
		No. Registrasi		✓	Nomor registrasi bukti elektronik
		Nama pemilik		✓	Nama pemilik bukti elektronik
		Deskripsi fisik		✓	Deskripsi fisik bukti elektronik
5.	Proses Akuisisi	Waktu	✓		Waktu akuisisi bukti elektronik.
		<i>Tools</i>		✓	Nama <i>tools</i> yang digunakan untuk akuisisi bukti elektronik.
		Tanggal	✓		Tanggal dilakukannya proses akuisisi.
		Petugas akuisisi		✓	Nama petugas yang melakukan akuisisi.

Tabel 3. 2 Komponen Chain of Custody(lanjutan)

No.	Kelompok Informasi	Field Informasi	Sifat		Jenis Informasi
			Statis	Dinamis	
		<i>Device</i>		✓	Nama perangkat
6.	Hasil <i>Imaging</i> Bukti Elektronik	Nama <i>file</i>	✓		Nama <i>file</i> hasil akuisisi
		Ukuran	✓		Ukuran <i>file</i>
		MD5	✓		<i>Hash file</i> MD5
		No.register bukti digital		✓	Nomor pendaftaran bukti digital
		SHA-1	✓		<i>Hash file</i> SHA-1
		SHA-256	✓		<i>Hash file</i> SHA-256
		Status BD	✓		Status bukti digital
7.	Lokasi Penyimpanan Bukti Digital	Lokasi <i>file</i>		✓	Lokasi (<i>path</i>) penyimpanan <i>file</i>
		Tanggal/waktu simpan		✓	Tanggal dan waktu unggah bukti digital
		Validator		✓	Nama petugas validator (<i>officer</i>) bukti digital
8.	<i>Role of Evidence</i>	Alasan penyitaan		✓	Alasan penyitaan bukti elektronik
		Potensi informasi		✓	Informasi yang ingin didapat dari akuisisi bukti elektronik
9.	Interaksi para Pihak	<i>Authorized by</i>		✓	Nama petugas (<i>officer</i>) yang memvalidasi aksi
		<i>Received by</i>		✓	Nama petugas (<i>officer</i>) yang menerima <i>form</i> digital <i>chain of custody</i>
		<i>Request time</i>		✓	Tanggal dan waktu aksi
		Approved Time		✓	Tanggal dan waktu validasi
		<i>Received time</i>		✓	Tanggal dan waktu <i>form</i> digital <i>chain of custody</i> diterima
		Aksi		✓	Nama aksi yang dilakukan pengguna
		Approved Time		✓	Tanggal dan waktu validasi

3.3 Pembuatan Kategori Bukti Digital

Dalam pengembangan sistem ini penulis membuat kategori bukti digital berdasarkan jenis kejahatan yang melibatkan bukti digital tersebut. Penggolongan yang dilakukan menggunakan jenis kejahatan dari KUHP (Kitab Undang-Undang Hukum Pidana) yang merupakan hukum yang berlaku di Indonesia. Sehingga secara teknis aplikasi sesuai dengan proses penegakan hukum yang berlaku di Indonesia.

Penggolongan ini bertujuan untuk memudahkan dalam pencatatan bukti digital serta memberikan informasi jumlah kejahatan yang nantinya dapat disajikan pada dashboard dan memberikan gambaran trend kejahatan yang terjadi di Indonesia.

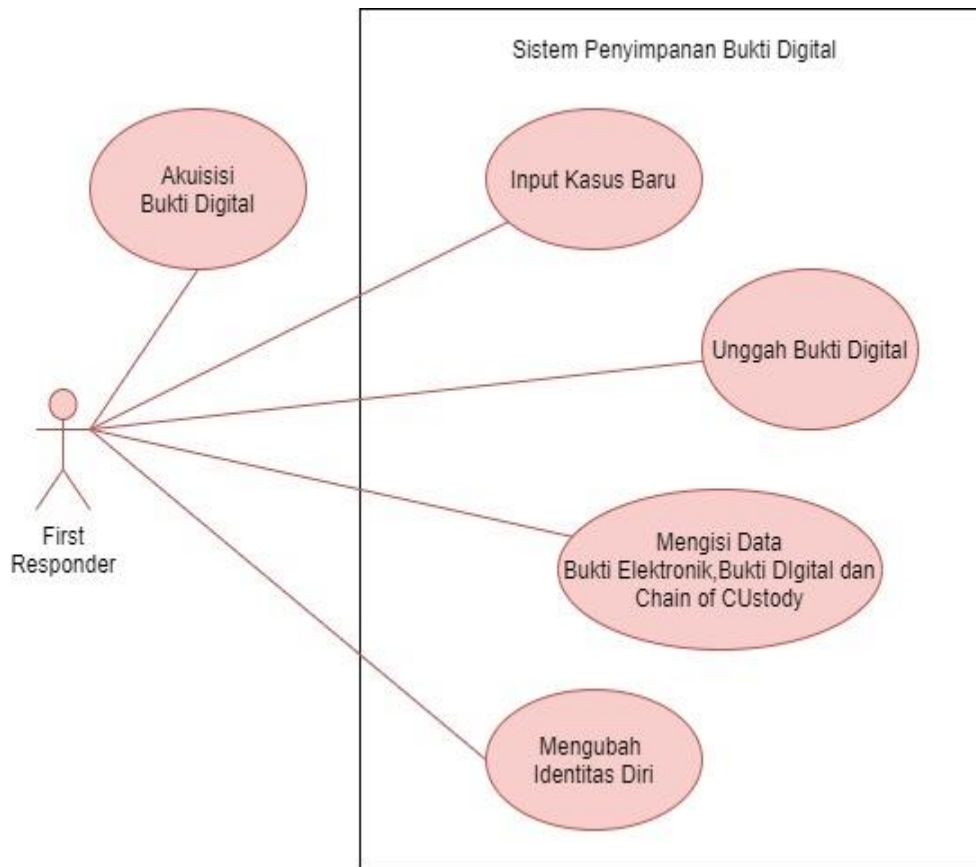
Secara umum penggolongan tindak-tindak kejahatan dapat dirumuskan dengan 7 kategori utama dan beberapa turunannya, penggolongan tersebut dapat dijabarkan sebagai berikut:

1. Kejahatan terhadap harta benda
 - a. Pencurian
 - b. Pencurian khusus
 - c. Pemerasan
 - d. Pengancaman
 - e. Penipuan
 - f. Penadahan
 - g. Kejahatan dengan alat percetakan
2. Kejahatan terhadap jiwa seseorang
 - a. Tindak pidana pembunuhan
 - b. Pembunuhan dengan pemberatan
 - c. Pembunuhan yang direncanakan
 - d. Pembunuhan terhadap anak yang baru lahir
 - e. Pembunuhan anak yang telah direncanakan dahulu
 - f. Turut serta dalam pembunuhan anak
 - g. Abortus
 - h. Euthanasia
 - i. Pembunuhan diri
3. Kejahatan terhadap badan seseorang
 - a. Penganiayaan biasa
 - b. Psl. 351 (4) dalam praktek
 - c. Penganiayaan ringan
 - d. Penganiayaan yang direncanakan biasa
 - e. Penganiayaan berat
 - f. Hukuman tambahan
 - g. Penyerangan/perkelahian
4. Kejahatan terhadap kehormatan seseorang
 - a. Pencemaran nama baik
 - b. Penghinaan tertulis
 - c. Memfitnah
 - d. Penghinaan ringan

- e. Mengadu secara memfitnah
 - f. Tuduhan secara memfitnah
5. Kejahatan mengenai pemalsuan
- a. Sumpah palsu
 - b. Pemalsuan uang
 - c. Mengedarkan uang palsu
 - d. Merusak uang
 - e. Mengedarkan uang logam yang dirusak
6. Kejahatan mengenai kesusilaan
- a. Pornografi
 - b. Tindak pidana perzinahan
 - c. Tindak pidana perkosaan
 - d. Mengadakan hubungan kelamin diluar perkawinan
7. Kejahatan terhadap negara
- a. Makar terhadap kepala negara
 - b. Makar untuk memasukkan indonesia dalam penguasaan asing

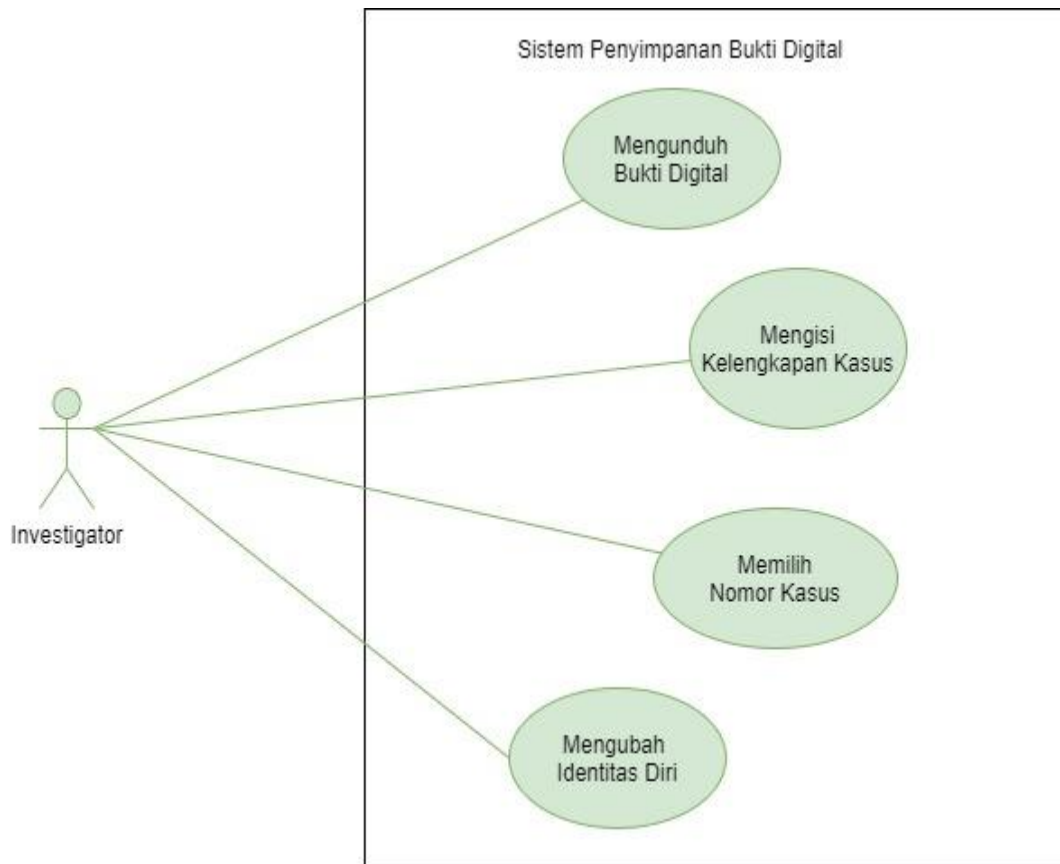
3.4 Pembagian Aktivitas Terhadap Sistem

Tahapan setelah terkumpulnya informasi melalui tahapan studi pustaka adalah tahapan pembuatan konsep penyimpanan bukti digital. Perancangan konsep ini dimulai dengan memisahkan pembagian hak otorisasi orang-orang yang berinteraksi dengan bukti digital tersebut terhadap sistem penyimpanan bukti digital. Terdapat setidaknya 4 orang yang berinteraksi dengan sistem penyimpanan bukti digital terkait dengan penanganan bukti digital. Pembagian hak otorisasi *first responder* terhadap sistem terkait dengan penanganan bukti dijelaskan melalui *use case* pada gambar 3.2 berikut.



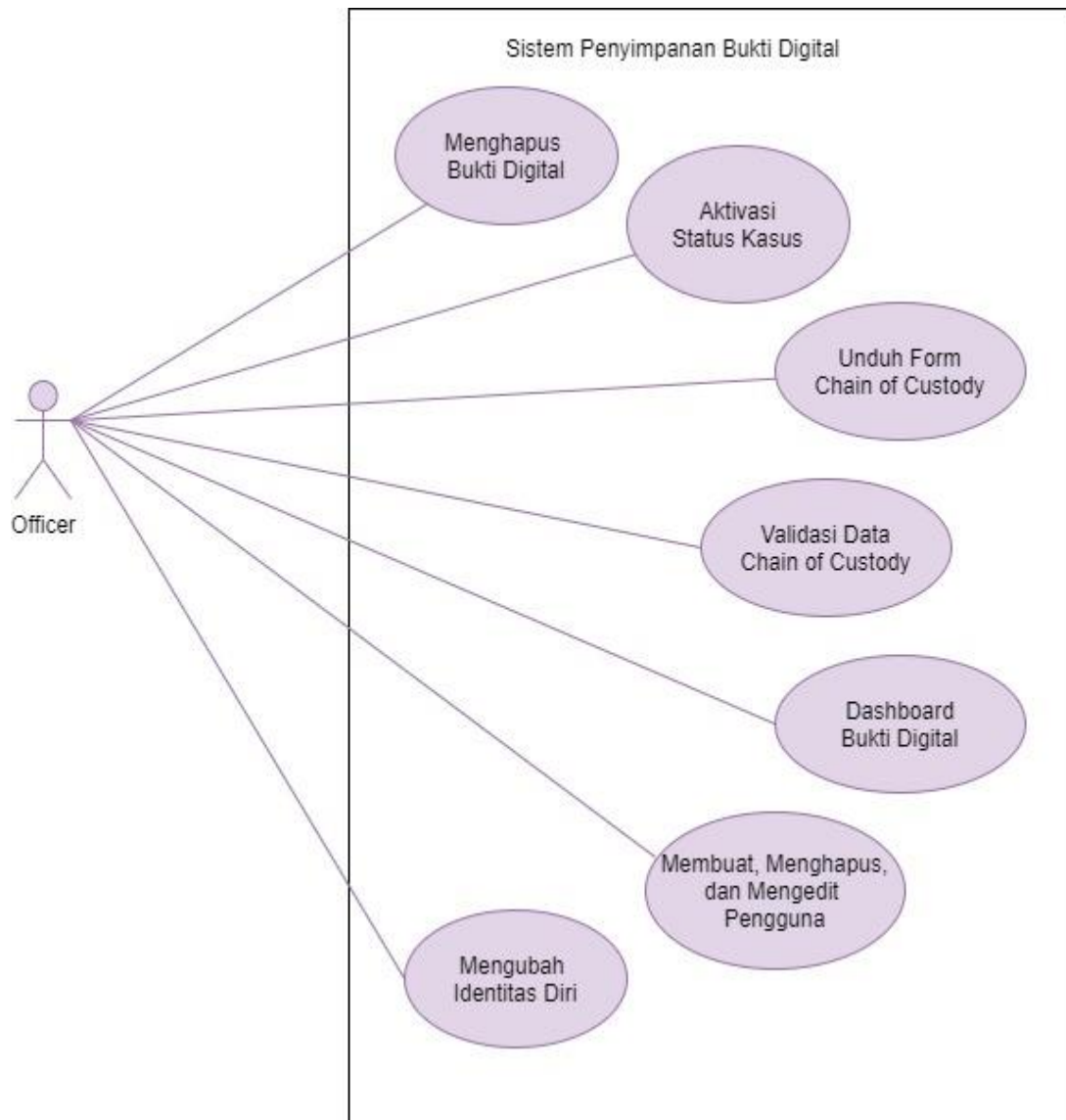
Gambar 3. 2 Use Case Pembagian Hak Otorisasi pada *First Responder*

Gambr 3.2 menjelaskan bahwa *First responder* memiliki kemampuan yang sama dengan investigator (Koch et al., 2008). *First responder* berperan sebagai orang yang pertama menunggah bukti digital dan melakukan proses akuisisi bukti digital sebelum bukti digital tersebut disimpan dalam sistem penyimpanan bukti digital. Ia juga dapat membuat *cabinet*, *rack* dan *bag* yang baru. Selain itu, *first responder* dapat mengisi data awal dari *chain of custody* berupa: informasi di TKP (*crime scene description*), informasi bukti elektronik (*device description*) dan informasi akusisi bukti digital (*acquisition description*). Selain memiliki hak akses untuk mengisi kelengkapan data *chain of custody*, *first responder* memiliki hak akses untuk memilih nomor kasus, jika terdapat kasus yang memiliki lebih dari 1 bukti digital. Namun, jika terdapat lebih dari 1 bukti digitl dalam satu kasus, maka bukti-bukti digital tersebut harus tersimpan dalam struktur *cabinet* yang sama *First responder* juga memiliki akses untuk merubah *username* dan *password* sebagai hak akses untuk masuk kedalam sistem penyimpanan bukti digital. Selain merubah *username* dan *password*, *first responder* dapat merubah data diri berupa: nama lengkap dan nama instansi.



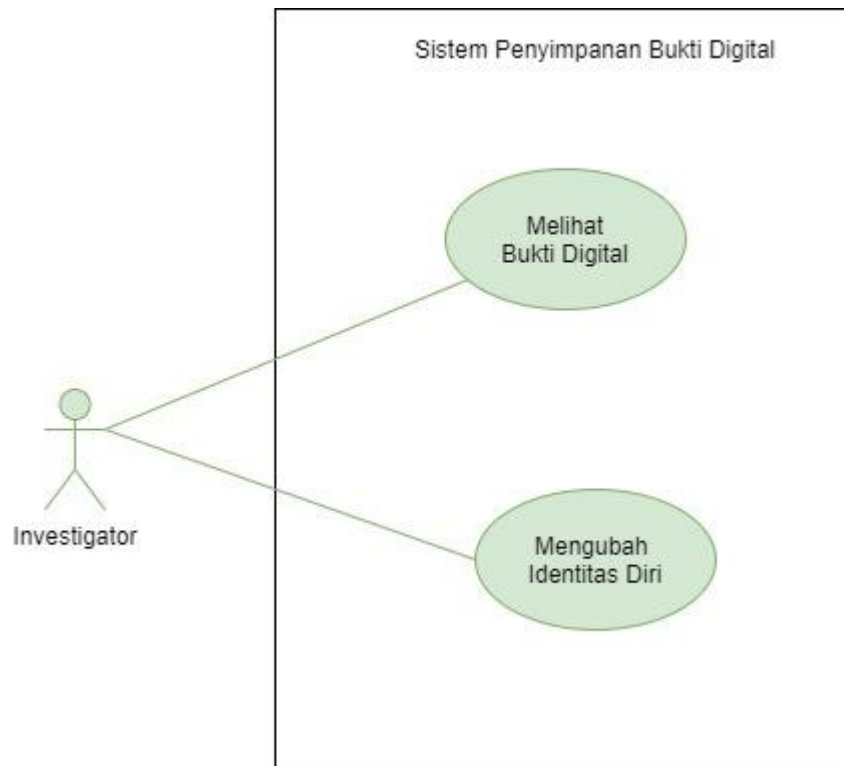
Gambar 3. 3 Use Case Pembagian Hak Otorisasi pada *Investigator*

Investigator adalah orang yang melakukan investigasi bukti digital terhadap kasus yang sedang dihadapi. Selain diberikan akses untuk mengunduh bukti digital, *investigator* juga dapat mengisi data *chain of custody* yang berkaitan dengan informasi kasus yang ditangani (*case description*) dan deskripsi peranan bukti digital dalam kasus tersebut (*role of evidence*). Seperti halnya dengan *first responder*, *investigator* juga dapat merubah *username* dan *password* yang dimiliki untuk hak akses kedalam sistem penyimpanan bukti digital. Data instansi dan nama lengkap juga dapat diubah oleh *investigator*.



Gambar 3. 4 Use Case Pembagian Hak Otorisasi pada *Officer*

Gambar 3.4 menjelaskan bahwa *Officer* memiliki peran utama sebagai validator atas apa yang dilakukan oleh *investigator* dan *first responder*. Kegiatan yang divalidasi oleh *officer* adalah: validasi kasus (selesai atau belum), validasi pengunduhan bukti digital dan validasi *chain of custody*. Selain itu, ia memiliki akses untuk mencetak form data *chain of custody*. Tidak hanya sebagai validator, *officer* juga memiliki peran dalam hal mengunduh *form chain of custody* dan mengubah kode *signature* (digunakan sebagai kode dalam *form chain of custody*). Selain memiliki kemampuan untuk merubah data *username* dan *password* yang dimilikinya, *officer* juga dapat menghapus bukti digital dan dapat merubah *password* dari *first responder* dan *investigator*. Selain itu, *officer* juga dapat merubah nama lengkapnya dan kode *signature* yang digunakan untuk memvalidasi *form digital chain of custody*.



Gambar 3. 5 Use Case Pembagian Hak Otorisasi pada Officer

Laywer merupakan penasehat hukum bagi tersangka di pengadilan. Meskipun *lawyer* tidak memiliki kepentingan untuk menganalisis bukti digital, namun dengan seizin hakim dan *officer* sebagai penanggungjawab terhadap bukti digital yang tersimpan, ia hanya hanya dapat melihat bukti digital yang telah tersimpan pada sistem penyimpanan bukti digital. Tidak semua kasus dapat dilihat oleh *lawyer*, hanya kasus yang sedang dihadapi saja yang dapat dilihatnya.

3.5 Konsep Desain Formulir Chain of Custody

Dalam aplikasi penyimpanan bukti digital ini akan men-*generate* formulir *chain of custody* yang dibagi menjadi 3 bagian. Setiap halaman pada formulir *chain of custody* memiliki id berupa angka untuk menjaga keaslian bukti digital. Hal ini bertujuan untuk mencegah terjadinya manipulasi data *form chain of custody* pada setiap halaman. Formulir dapat diunduh dengan format file pdf. Setiap formulir dibuat dengan sederhana untuk memudahkan dalam membaca informasi di dalamnya.

Bagian pertama adalah halaman yang berisi informasi detail kasus, bukti elektronik dan bukti digital. Kolom detail kasus terdiri dari; Nama kasus, nama tersangka, nama korban, lokasi kejadian, waktu, nama *first responder*, alat yang digunakan untuk olah dan institusi *first responder* berasal. Pada kolom detail bukti digital dan bukti elektronik

berisikan metadata dari barang bukti tersebut. Gambar 3.5 menunjukkan konsep desain *form chain of custody* halaman pertama.

CHAIN OF CUSTODY OF DIGITAL 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
Tools (Live Forensics)	Tools yang Digunakan saat Olah TKP
Tools Description	Spesifikasi dari Perangkat yang Digunakan
Institution	Nama Institusi Tempat First Responder Bekerja
Electronic Evidence	
Register Number	Nomor Inventaris Bukti Elektronik
Type	Tipe Bukti Elektronik
Model	Model Bukti Elektronik
Manufacture	Nama Perusahaan Pembuat Bukti Elektronik
Serial number	Nomor Serial Bukti Elektronik
Foreclosure Reasons	Alasan Penyitaan Bukti Elektronik
Digital Evidence	
Case Number	Nomor Kasus
File Name	Nama Bukti Digital
Time (Acquisition)	Tanggal dan Waktu Akuisisi Bukti Digital
Device (Acquisition)	Nama Tools yang Digunakan saat Akuisisi
Size (Byte)	Ukuran Bukti Digital
Hashing (SHA1)	Fungsi Hash Bukti Digital (SHA1)
Hashing (MD5)	Fungsi Hash Bukti Digital (MD5)
Source	Direktori Asal Bukti Digital
Cabinet Structure	Struktur Cabinet Penyimpanan Bukti Digital
Potential Information	Deskripsi Informasi yang Diharapkan Didapat
Status	Status Kasus (Active/Closed)
Validator	Nama Officer

Gambar 3. 6 Konsep Desain Form Chain of Custody bagian pertama

Pada halaman kedua terdapat perbedaan yang signifikan dengan halaman pertama. Pada halaman pertama jumlah data dan halamannya tidak akan bertambah, namun pada halaman kedua jumlah datanya bisa bertambah mengikuti banyaknya interaksi dengan bukti digital, karena halaman ini merupakan halaman yang mencatat segala aktivitas yang dilakukan pengguna dalam penanganan bukti digital. Halaman ini disebut juga sebagai *Digital Evidence Interactions* yang berfungsi mencatat aktivitas pengisian informasi *chain*

of custody, informasi bukti digital dan *form chain of custody* yang diunduh. Gambar 3.7 menunjukkan konsep desain *form chain of custody* halaman kedua.

Date/Time		Authorized by
Requested	Tanggal & Waktu Chain of Custody Ditambahkan	Nama Officer
Approved	Tanggal & Waktu Divalidasi	Submitted by
Received	---	Nama First Responder/Institusi
Action: Added Data		
Nama Elemen XML	Nilai Elemen XML	
Date/Time		Authorized by
Requested	Tanggal & Waktu Bukti Digital Diunduh	Nama Officer
Approved	Tanggal & Waktu Pengunduhan Divalidasi	Submitted by
Received	Tanggal & Waktu Bukti Digital Diterima	Nama Investigator/Institusi
Action: Downloaded File		
destination	Direktori Tujuan Bukti Digital Diunduh	
Date/Time		Authorized by
Requested	---	Nama Officer
Approved	---	Submitted by
Received	Tanggal & Waktu Form Chain of Custody Diterima	Nama Officer
Action: Downloaded Form		
destination	Direktori Tujuan Form Chain of Custody Diunduh	

Gambar 3. 7 Konsep Desain Form Chain of Custody bagian kedua

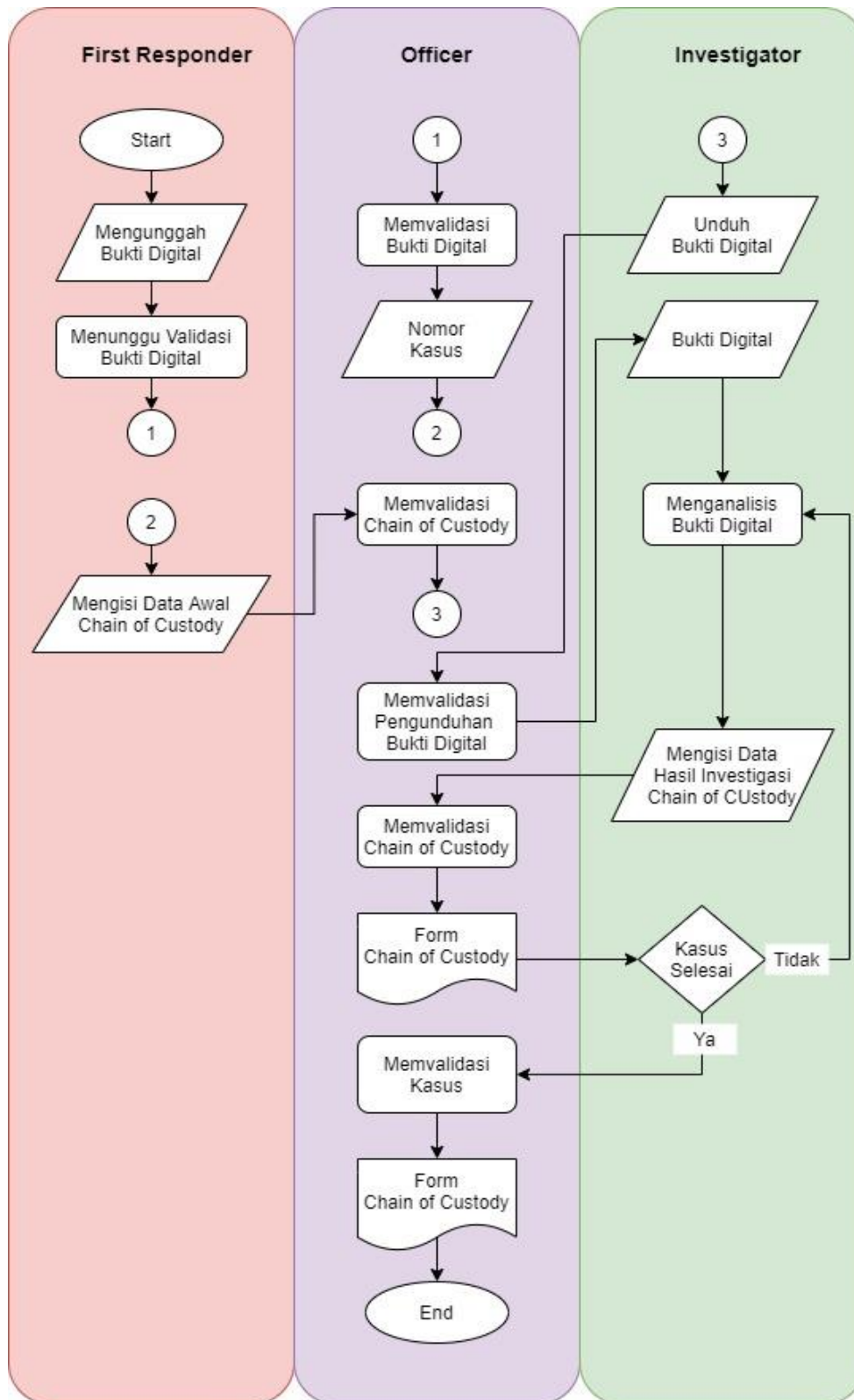
Bagian terakhir adalah halaman yang berisi tandatangan officer yang telah dienkripsi menggunakan metode enkripsi MD5. Officer dapat memasukkan tandatangan dalam bentuk string melalui sistem penyimpanan bukti digital. Halaman ketiga ini berfungsi sebagai bentuk pengesahan bahwa segala aktivitas yang terkait dengan bukti digital pada PENGELOLAAN BUKTI DIGITAL telah melalui validasi dari officer. Gambar 3.8 menunjukkan desain form chain of custody halaman ketiga.

<p><i>This Form Chain of Custody has been validated by officer</i> <i>Nama officer</i> <i>Kode hashing MD5</i></p>

Gambar 3. 8 Konsep Desain Form Chain of Custody

3.6 Pembuatan Konsep Penyimpanan Bukti Digital

Terdapat beberapa tahapan yang harus dilakukan oleh *officer*, *first responder* dan *investigator* dalam penanganan bukti digital dengan menggunakan sistem penyimpanan bukti digital. Proses tersebut dilakukan secara urut agar *form chain of custody* yang tercipta dapat dipertanggungjawabkan di pengadilan. Berikut adalah penjelasan alur penanganan bukti digital pada sistem penyimpanan bukti digital.



Gambar 3. 9 Alur Penanganan Bukti Digital pada Sistem Penyimpanan Bukti Digital

Alur penanganan bukti digital dimulai saat *first responder* melakukan unggah bukti digital yang telah diakuisisi. Setelah bukti digital berhasil diunggah, *officer* akan melakukan validasi terhadap bukti digital. Selanjutnya, sistem akan mengeluarkan nomor kasus secara

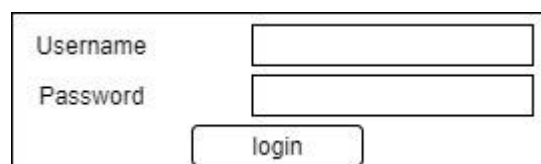
otomatis yang tidak dapat diubah pengguna. *First responder* mengisi data awal *chain of custody* berupa: informasi TKP *crime scene description*), informasi bukti elektronik (*device description*) dan informasi akusisi bukti digital (*acquisition description*). Ketika data awal *chain of custody* telah disimpan, selanjutnya *officer* melakukan validasi data awal *chain of custody* hingga data-data tersebut dapat terlihat pada sistem.

Investigator mengunduh bukti digital tersebut untuk dianalisis. Sebelum bukti digital tersebut berhasil diunggah menuju direktori tertentu, *officer* akan melakukan validasi terhadap bukti digital tersebut. Setelah bukti digital tersebut telah divalidasi, *investigator* dapat mengunduh bukti digital menuju direktori tertentu. Setelah berhasil diunduh, *investigator* dapat melakukan analisis bukti digital. Saat proses analisis telah selesai, *investigator* menulis hasil analisis kedalam *chain of custody* berupa: deskripsi kasus yang ditangani (*case description*). Saat data hasil investigasi telah disimpan, *officer* akan melakukan validasi kembali terhadap isian data *chain of custody*.

Setelah divalidasi, *officer* mengeluarkan *form chain of custody* sementara yang dapat digunakan di pengadilan jika dibutuhkan. Saat kasus selesai ditangani, maka *investigator* akan memberitahu *officer* bahwa kasus tersebut telah selesai dan siap untuk divalidasi. Validasi akhir yang dilakukan oleh *officer* ini akan membuat sistem penyimpanan bukti digital akan mengunci semua data sehingga data *chain of custody* tidak dapat berubah. Sehingga *Form chain of custody* yang dicetak setelah kasus selesai adalah *form* yang sudah tidak akan berubah data-datanya. Gambar 3.9 menunjukkan alur penanganan bukti digital pada sistem.

3.7 Perancangan Desain Halaman Antarmuka

Perancangan antarmuka dibuat berdasarkan fungsi dan hak akses penggunanya. Pada halaman awal pengguna harus memasukkan *username* dan *password* yang telah diberikan, halaman login ini berfungsi untuk membatasi akses otorisasi pengguna. Setelah berhasil login pengguna akan memasuki tampilan sesuai dengan jenis pengguna. Konsep desain halaman login dibuat sederhana agar pengguna mudah dalam mengoperasikannya. Konsep desain halaman login dapat dilihat pada gambar 3.10 berikut.



The image shows a conceptual design of a login page. It consists of a rectangular container with a thin border. Inside the container, on the left side, are the labels 'Username' and 'Password' stacked vertically. To the right of 'Username' is a horizontal rectangular input field. To the right of 'Password' is another horizontal rectangular input field. Below the 'Password' input field, centered horizontally, is a button labeled 'login'.

Gambar 3. 10 Konsep Desain Halaman login

Setelah melakukan proses otorisasi pengguna maka pengguna akan disajikan tampilan yang berbeda-beda dengan menu yang dibutuhkan oleh masing-masing petugas. Pada menu *first responder* pada tampilan awalnya berupa form input kasus. Hal pertama yang dilakukan adalah memilih Kategori kejahatan dan Detail kejahatan yang sudah digolongkan sebelumnya, setelah itu baru mengisi kolom nama investigator, nama jaksa, nama pengacara, nama penyidik dan mengunggah berkas bukti digital dan kemudian klik tombol simpan. Desain form input kasus baru dapat dilihat pada gambar 3.11.



Input Kasus Baru

Kategori Kejahatan

Detail Kejahatan

Nama Investigator

Nama Jaksa

Nama Pengacara

Nama Penyidik

Pilih Berkas

SIMPAN

Gambar 3. 11 Konsep Desain Halaman Input Kasus Baru

Setelah Kasus Baru divalidasi oleh *officer* maka *Investigator* dapat memulai mengisi detail kasus yang berkaitan dengan bukti digital tersebut yang berisi metadata meliputi deskripsi tempat kejadian perkara, deskripsi bukti elektronik, peranan bukti digital dalam kasus tersebut, serta waktu dan tempat bukti digital tersebut diakuisisi. Desain form input kasus baru dapat dilihat pada gambar 3.12.

Input Detail Kasus

Kategori Kejahatan

Detail Kejahatan

Nama Bukti Digital

Status

Deksripsi TKP

Nama Alat

Deskripsi

Waktu

Lokasi

Deksripsi Bukti Elektronik

No. Reg

Model

Serial Number / IMEI

Tipe

Merk

Kapasitas

Peranan Bukti

Alasan

Info

Akuisisi

Waktu

Tool

Gambar 3. 12 Konsep Desain Halaman Detail Kasus

Sedangkan pada menu investigator akan ditampilkan berupa form untuk mengisi detail kasus yang lebih terperinci. Untuk dapat mengisi detail tersebut sebelumnya investigator harus memilih file bukti digitalnya terlebih dahulu baru dapat mengisi data meliputi; no kasus, nama kasus, nama pelaku, nama korban, nama investigator, nama jaksa, nama pengacara dan nama penyidik, desain form investigator dapat dilihat pada gambar 3.10 Konsep Desain Halaman Investigator.

First Responder	<input type="text"/>
Kategori Kejahatan	<input type="text"/>
Detail Kejahatan	<input type="text"/>
Nama Bukti Digital	<input type="text"/>

Detail Kasus	Informasi File
No Kasus	Nama File
<input type="text"/>	<input type="text"/>
Nama Kasus	Ukuran file
<input type="text"/>	<input type="text"/>
Nama Pelaku	Kunci Hash (SHA1)
<input type="text"/>	<input type="text"/>
Nama Korban	Kunci Hash (MD5)
<input type="text"/>	<input type="text"/>
Investigator	Lokasi File
<input type="text"/>	<input type="text"/>
Jaksa	Tanggal Upload
<input type="text"/>	<input type="text"/>
Pengacara	
<input type="text"/>	
Penyidik	
<input type="text"/>	

Gambar 3. 13 Konsep Desain Halaman Investigator

Unduh Bukti Digital	
Kategori Kejahatan	<input type="text"/>
Detail Kejahatan	<input type="text"/>
Nama Bukti Digital	<input type="text"/>

Gambar 3. 14 Konsep Desain Halaman Investigator

3.8 Implementasi

Tahap implementasi merupakan tahap penerapan sistem baru kepada sistem sebelumnya. Tahap ini bertujuan untuk mengetahui sejauh mana sistem yang baru dapat berjalan sesuai rancangannya. Tahap implementasi juga memberikan informasi kelebihan dan kekurangan setelah sistem diterapkan, sehingga akan membantu untuk pengembangan penelitian.

Tahap implementasi memuat pembangunan lemari penyimpanan bukti digital sebagai bagian yang baru dari sistem. Bahasa pemrograman yang digunakan adalah bahasa pemrograman php dan netbeans 6.8 sebagai complier.

3.9 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 pengujian. Output dari sistem akan dianalisa kesesuaiannya dengan kasus yang telah disimulasikan, kemudian menghasilkan kesimpulan yang berisi keberhasilan sistem.

3.10 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.

3.11 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*.

BAB 4

Implementasi dan Pembahasan

4.1 Implementasi Sistem

Pada tahap implementasi dilakukan kegiatan perancangan sistem dan merupakan tahap usaha untuk mewujudkan sistem yang dirancang. Tahapan dari proses implementasi adalah sebuah rangkaian kegiatan dari awal sampai akhir yang harus dilalui dalam mewujudkan sistem yang telah dirancang. Hasil dari tahapan implementasi ini adalah suatu sistem pengolahan data yang sudah dapat berjalan dengan baik

4.1.1 Konsep Akses Bukti digital

Dalam pengelolaan bukti digital perlu adanya akses terhadap bukti digital baik dari *first responder* yang menyerahkannya ke *officer* dan menyediakan bukti digital untuk diberikan kepada *investigator* untuk investigasi. Akses atau penyerahan bukti digital yang dilakukan selama ini berjalan dengan prosedur *copy file* yang mengharuskan petugas untuk saling bertemu atau datang ke laboratorium. Penyerahan bukti digital dapat dilakukan secara daring dengan mengirim lewat *email* atau memanfaatkan penyimpanan *cloud storage*, namun cara ini sangat beresiko dan sulit untuk melakukan pencatatan dalam melengkapi formulir *chain of custody*. Aktivitas ini memerlukan waktu yang tidak sedikit dan terbatas pada lokasi tertentu, hal ini sangat berpengaruh terhadap proses investigasi. Proses Aktivitas ini dapat dilihat pada gambar 4.1.



Gambar 4. 1 Alur Akses Bukti Digital

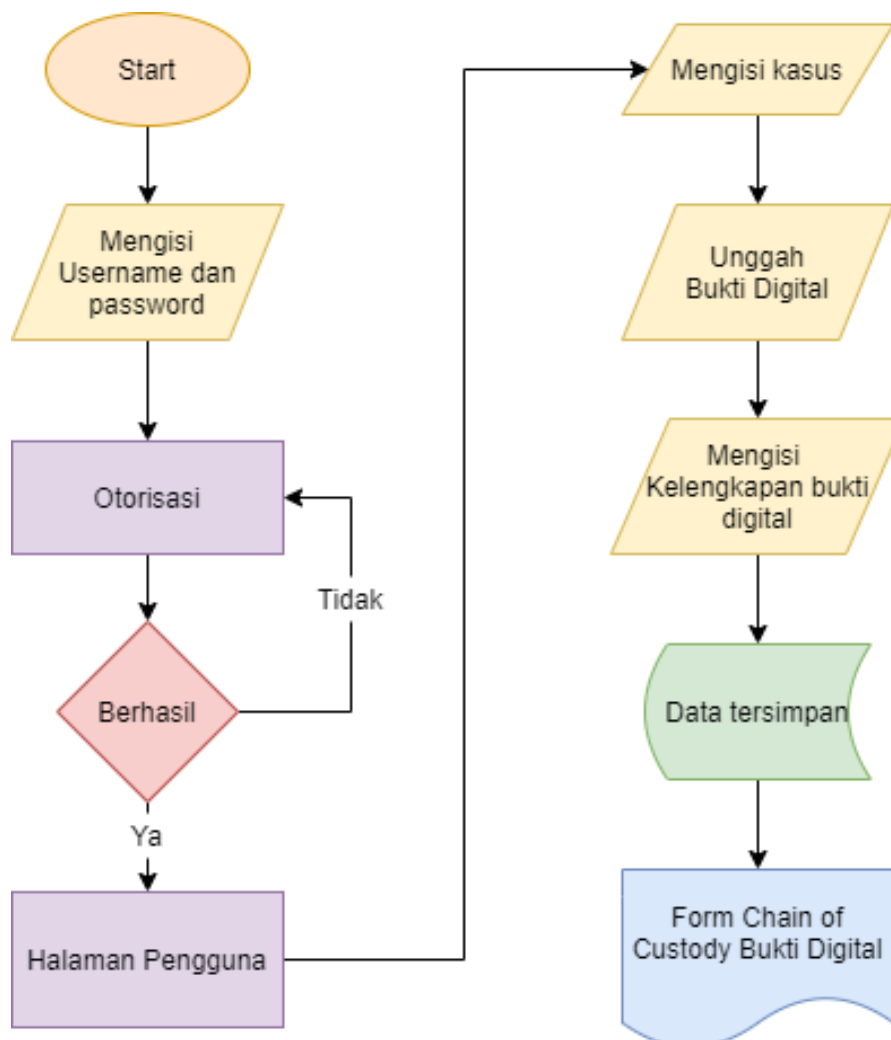
Untuk meningkatkan aksesibilitas bukti digital maka perlu dirancang sebuah sistem yang dapat memberikan kemudahan dalam mengakses bukti digital dan memiliki fitur pencatatan aktivitas terhadap bukti digital secara otomatis dan sistematis. Sistem yang dirancang hendaknya dapat mengatasi masalah batasan waktu dan tempat menyediakan akses yang lebih mudah dan menjangkau area yang lebih luas. Gambar konsep akses bukti digital dapat dilihat pada gambar 4.2.



Gambar 4. 2 Konsep Alur Akses Bukti Digital

Pada sistem yang diusulkan akses bukti digital dilakukan secara langsung tanpa melalui tahap *copy files* manual karena bukti digital sudah disimpan pada sistem yang dapat diakses melalui internet sehingga akses lebih mudah dan cepat.

4.1.2 Alur Sistem



Gambar 4. 3 Alur Kerja Sistem

Sistem ini memiliki alur kerja yang diawali dengan memasukkan *field username* dan *password*. Pengguna dapat memasukkan *username* dan *password* yang telah dibuat oleh *officer*. Apabila proses otorisasi pengguna berhasil maka pengguna akan memasuki halaman utama pengguna sesuai jenis penggunanya, namun jika proses otorisasi gagal maka sistem akan menampilkan sebuah pesan yang *error* yang mengharuskan pengguna untuk mengisi kembali data *username* dan *password*.

Setelah proses otorisasi pengguna berhasil dan dapat memasuki sistem, *First Responder* mengisi data kasus baru dan mengunggah bukti digital, *Investigator* dan *Officer* dapat mengisi kelengkapan data. Data tersebut akan tersimpan pada database sistem dan akan di proses dengan keluaran berupa *Form Chain of Custody* yang menggunakan format pdf.

CHAIN OF CUSTODY OF DIGITAL EVIDENCE	
To be completed by First Responder and Investigator	
Crime Scene	
Case Name	Case Name
Suspect	Suspect Name
Victim	Victim Name
Location	Location
Time	Time
Tools (Live Forensics)	Tools Name
Tools Description	Description Tools
First Responder	Krisna Widatama
Institution	Institusi Krisna Widatama
Tools Description	Description Tools
Electronic Evidence	
Register Number	No. Reg
Type	Type
Model	Model
Manufacture	Manufacturer
Serial Number	Serial Number
Foreclosure Reasons	Reasons
Digital Evidence	
Case Number	Case Number
File Name	opens132_judul.sql
Time (Acquisition)	Time Acq
Device (Acquisition)	Tools/Device
Size (Byte)	3997
Hashing MD5	3144b2adb67266e37423926a0484c360
Hashing SHA1	35853319a6b9438257ebfd1798339ec166bc76fb
Source	C:\xampp\tmp\phpC370.tmp
Potential Information	Potential Info
Date Uploaded	15-12-2019 03:58
Validator	Officer

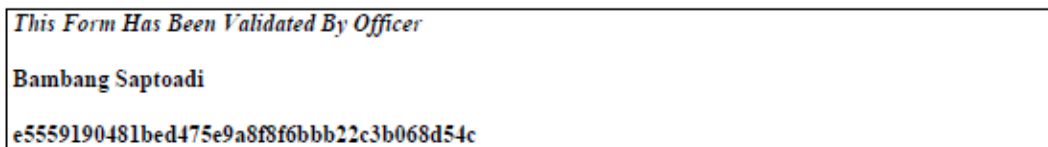
Gambar 4. 4 Form Chain of Custody Halaman Pertama

Pada tabel 4.5 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 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 dicatat 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 responder* 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 diinputkan 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. *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 berisikan 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*.



This Form Has Been Validated By Officer

Bambang Saptoadi

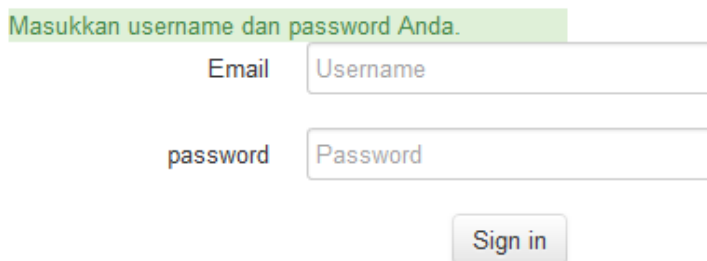
e5559190481bed475e9a8f8f6bbb22c3b068d54c

Gambar 4. 5 Form Chain of Custody halaman kedua

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

4.1.3 Implementasi Antar muka

Tampilan awal sistem diawali dengan menampilkan *form login Sistem* berisi *username* dan *password*. *Form* tersebut digunakan, *officer*, *first responder* dan *investigator* 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 4.4 menunjukkan menu *login* pada sistem tersebut.



Masukkan username dan password Anda.

Email

password

Gambar 4. 6 Menu Login

Setelah pengguna berhasil *Login*, pengguna akan masuk pada halaman utama sesuai otoritasnya masing-masing. Gambar 4.5 menunjukkan tampilan halaman beranda untuk *first responder*.

Insert New Case

USERS DETAIL

Type of Crimes
 -- Select Type of Crimes --

Detail of Crimes
 -- Select Detail of Crimes --

Investigator
 -- Select Investigators --

Jaksa
 -- Select Jaksa --

Pengacara
 -- Select Pengacara --

Penyidik
 -- Select Penyidik --

Upload Digital Evidence
 Tidak ada berkas dipilih.

Gambar 4. 7 Halaman Beranda *first responder*

Type of Crimes
 Kejahatan Terhadap Badan Seseorang

Detail of Crimes
 Penganiayaan Ringan

Digital Evidence
 Ztable.pdf

Case Status
 ACTIVE

Gambar 4. 8 Halaman input data *first responder*

Gambar 4.6 menunjukkan halaman awal setelah *first responder* masuk sistem. Pada halaman ini *first responder* memasukkan data awal sebuah kasus dengan memilih jenis kejahatan beserta turunannya kemudian menunjuk pihak-pihak yang berperan pada kasus tersebut mulai dari investigator, pengacara, jaksa dan penyidik. Kemudian file bukti digital diunggah supaya dapat dilanjutkan prosesnya oleh *officer* dan *investigator*.

Diasumsikan bahwa *first responder* sudah masuk kedalam sistem dan selesai mengunggah bukti digital dan *officer* melakukan aktivasi. Halaman aktivasi dapat dilihat pada gambar 4.7. Setelah itu, *First responder* dapat melanjutkan proses pengisian bukti digital pada halaman data seperti yang ditampilkan pada gambar 4.8. Selanjutnya, *First*

Responder memasukkan data *Chain of Custody* dan menyimpannya untuk kemudian *Form Chain of Custody* akan dicetak oleh *Officer*.

First Responder

Faiz

Type of Crimes

Kejahatan Mengenai Pemalsuan

Detail of Crimes

Sumpah Palsu

Digital Evidence

rararable.pdf

Status

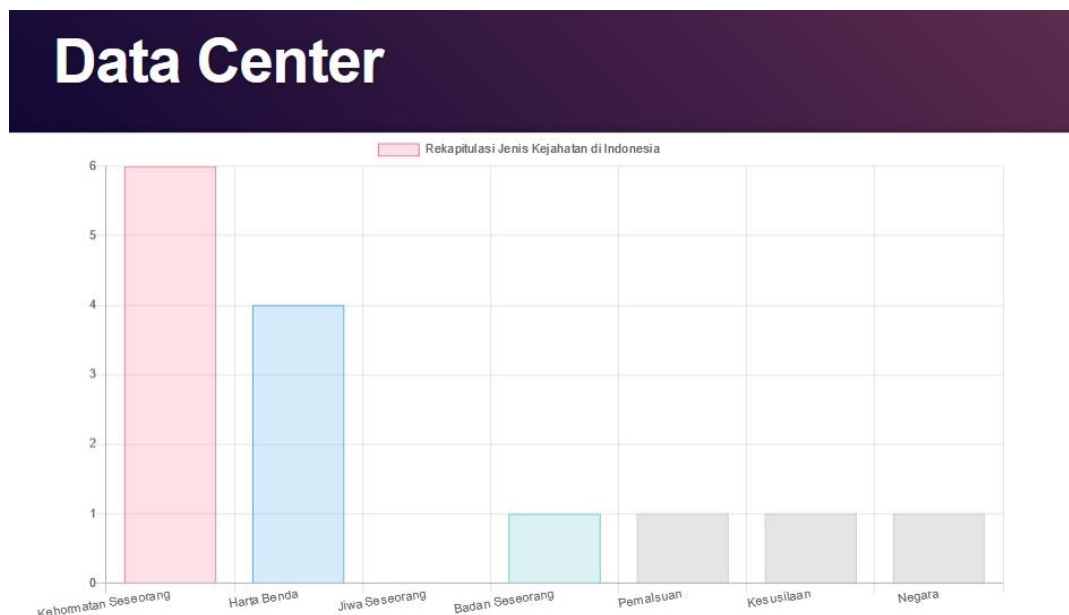
INACTIVE

Activate

CASE DESCRIPTION	FILE INFORMATION
Case Number	File Name
	rararable.pdf
Case Name	Size

Gambar 4. 9 Halaman *officer*

Aplikasi pengelolaan bukti digital menyajikan data berupa grafik yang memunculkan perbandingan tingkat kejahatan yang melibatkan bukti digital. Grafik tersebut terdiri atas tujuh kategori utama kejahatan yang sudah dirumuskan sebelumnya. Dengan seiring bertambahnya data maka grafik tersebut akan mengalami pertumbuhan semngikuti jenis kejahatan yang ditangani. Grafik tersebut dapat dilihat pada gambar 4.9.



Gambar 4. 10 Grafik Kejahatan

List of Users				
No.	Full Name	Institution	Position	Action
1	Krisna Widatama	Institusi Krisna Widatama	First Responder	Detail
2	Syarippudin	Institusi Imam Samudera	Investigator	Detail
3	Sri Victorinasari	ILC	Pengacara	Detail
4	Dimas Sasana	Kejaksaaan	Jaksa	Detail
5	Sarimin, SE.	Inspector	Penyidik	Detail
6	Faiz	Ull	First Responder	Detail
7	Reza Audiansyah	Ull	Investigator	Detail
8	Robert Ratubulu	Ull	Pengacara	Detail
9	Martin Surya	Ull	Investigator	Detail

Insert New User

Full Name

Institution

Username

Password

Gambar 4. 11 Management Pengguna

4.1.4 Implementasi Database

Dalam perancangan sistem pengelolaan bukti digital maka perlu dibuat database untuk memenuhi kebutuhan penyimpanan data. Dalam database sistem pengelolaan bukti digital ini terdiri dari 5 tabel, yaitu; tabel Kejahatan, jenis_kejahatan, user, record dan kasus.

4.1.4.1 Tabel Kejahatan

Tabel kejahatan merupakan tabel yang berisi data 7 kategori utama kejahatan yang telah dirancang sebelumnya. Tabel ini berkaitan dengan aktifitas penyimpanan bukti digital serta sebagai indikator dalam perancangan diagram pada menu visualisasi dengan tujuan supaya memudahkan dalam memonitor tingkat kejahatan berdasarkan kategori kejahatan. Tabel kejahatan dapat dilihat pada gambar 4.10.

Kejahatan
PK idkejahatan
detail_kejahatan

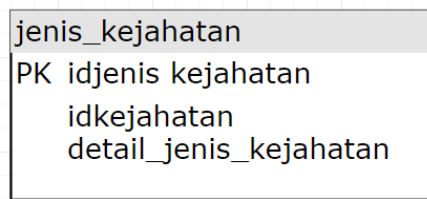
Gambar 4. 12 Tabel Kejahatan

Pada gambar 4.11 memperlihatkan tabel kejahatan dengan atribut yang sederhana, dimana tabel ini menjabarkan jenis atau sub kasus yang dimiliki oleh 7 kategori kejahatan yang berfungsi untuk membagi jenis kasus sehingga memudahkan dalam pengelolaan bukti digital nantinya.

Tabel 4. 1 Komponen Tabel Kejahatan

No	Nama Kolom	Jenis Data	Panjang Karakter	Key
1	idkejahatan	Integer	11	Primary Key
2	Detail_kejahatan	varchar	255	-

4.1.4.2 Tabel jenis_kejahatan



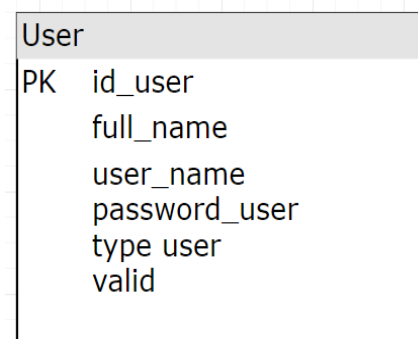
Gambar 4. 13 Tabel jenis_kejahatan

Pada gambar 4.11 dapat dilihat bahwa tabel jenis_kejahatan terdiri dari idjenis_kejahatan, idkejahatan dan detail_jenis_kejahatan. Tabel ini sangat berkaitan dengan tabel kejahatan yang sudah dibahas sebelumnya. Tabel ini menampung atribut dari jenis_kejahatan yang dimana kolom idkejahatan terhubung dengan tabel kejahatan, yang menunjukkan bahwa struktur kategori kejahatan telah diimplementasikan pada database.

Tabel 4. 2 Komponen Tabel jenis_kejahatan

No	Nama Kolom	Jenis Data	Panjang Karakter	Key
1	idjenis_kejahatan	Integer	11	Primary Key
2	idkejahatan	varchar	255	Foreign Key
3	detail_jenis_kejahatan	varchar	255	-

4.1.4.3 Tabel User



Gambar 4. 14 Tabel User

Tabel User tersusun atas id_user, full_name, user_name, password_user, type user, valid. Setiap atribut memiliki peran yang sangat penting dalam sistem ini. Untuk data pertama adalah data id_user, data ini merupakan *primary key* yang bersifat unik dan dihasilkan oleh sistem, bukan hasil dari masukkan pengguna. Kolom fullname berisi nama lengkap dari pengguna. Selanjutnya user_name dan password_user menyimpan data *username* dan *password* yang akan digunakan pengguna ketika setiap akan kali memsauki sistem. Data type_user bertugas membedakan jenis pengguna berdasarkan otorisasinya, karena setiap pengguna memiliki tugas dan wewenang yang berbeda-beda, kolom valid menunjukkan kebenaran data dalam akun user yang dibuat.

Tabel 4. 3 Komponen Tabel User

No	Nama Kolom	Jenis Data	Panjang Karakter	Key
1	Id_user	Integer	11	Primary Key
2	full_name	varchar	255	-
3	user_name	varchar	255	-
4	password_user	varchar	255	-
5	type_user	varchar	32	-
6	valid	text	-	-

4.1.4.4 Tabel Record

record	
PK	idrecord
	idkasus
	desc_record
	user_detail
	date_record

Gambar 4. 15 Tabel record

Tabel record terdiri dari data idrecord, idkasus, desc_record, user_detail, date_record. Idrecord menyimpan nomor urut record yang merupakan data unik yang dihasilkan oleh sistem secara otomatis. Idkasus merujuk pada kolom idkasus yang berada pada tabel kasus. Sedangkan desc_record menyimpan data deskripsi kegiatan pengguna yang dicatat oleh sistem terhadap bukti digital. Kolom user_detail menyimpan data pengguna yang aktifitasnya dicatat. Date_record menyimpan data waktu aktifitas pengguna.

Tabel record memiliki fungsi utama sebagai pencatatan aktifitas pengguna terhadap bukti digital. Dimana aktifitas tersebut akan didaftar dan dicantumkan pada lembar *chain of custody* yang dihasilkan oleh sistem pada halaman kedua. Halaman ini berfungsi sebagai kendali atas akses bukti digital yang dikelola dan memberikan laporan yang lengkap atas aktifitas yang dilakukan terhadap bukti digital yang memberikan kekuatan hukum bukti digital pada persidangan.

Tabel 4. 4 Komponen tabel record

No	Nama Kolom	Jenis Data	Panjang Karakter	Key
1	idrecord	Integer	11	Primary Key
2	idkasus	Integer	11	Foreign Key
3	Desc_record	text	-	-
4	user_detail	varchar	255	-
5	date_record	text	-	-

4.1.4.5 Tabel Kasus

Tabel kasus merupakan tabel yang memiliki kolom yang paling banyak. Kolom pada tabel kasus terdiri atas 35 data yang merupakan komponen dari formulir *chain of custody*. Tabel ini berisi data lengkap dari kasus sekaligus dengan data bukti digital yang dikelola oleh sistem pengelola bukti digital.

Data ini terbagi menjadi beberapa kelompok data yang berbeda. Kelompok pertama adalah data kasus yang berisi informasi tentang kasus, jenis kejahatan, pengguna yang terlibat di dalamnya, nomor kasus, nama korban, nama tersangka. Pada kelompok kedua berisi data olah tempat kejadian perkara, yakni alat yang digunakan, waktu dan lokasi olah kejadian perkara. Kelompok ketiga berisi detail dari bukti digital yang diunggah. Kolom data dari tabel kasus dapat dilihat pada gambar 4.14.

Kasus	
PK	idkasus
	idkejahatan
	idjeniskejahatan
	idfr
	idininvestigator
	idjaksa
	idpengacara
	idpenyidik
	file_name
	file_name_new
	size
	sha1
	md5
	file_location
	date_uploaded
	case_number
	case_name
	suspect_name
	victim_name
	tools
	description
	time_cs
	location_cs
	no_reg
	model
	serial_number
	type
	manufacturer
	capacity
	reason
	potential_info
	time_acq
	tools_acq
	status
	year

Gambar 4. 16 Tabel Kasus

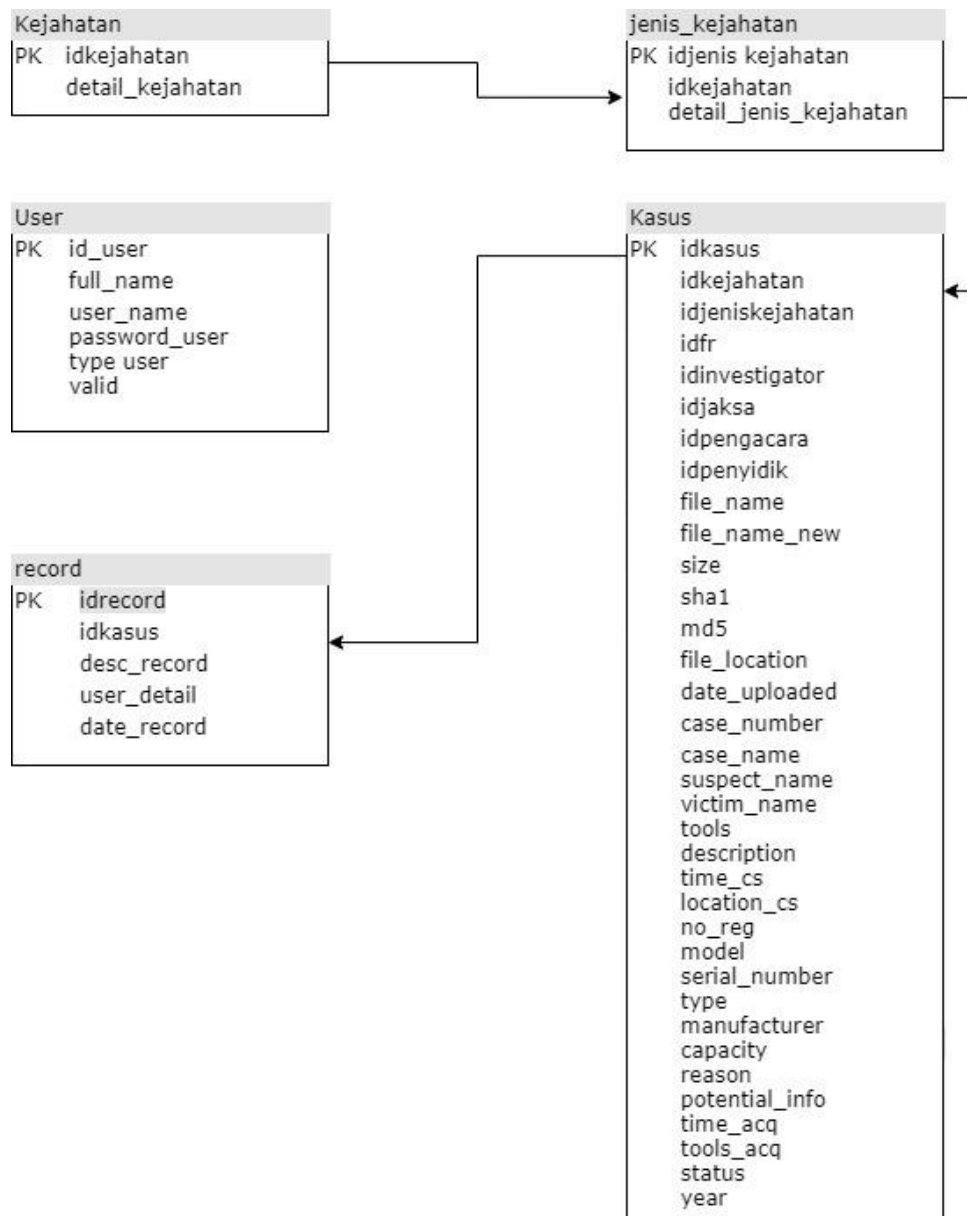
Atribut pada tabel kasus memiliki karakteristik yang berbeda-beda baik tipe datanya maupun panjang karakternya disesuaikan dengan data yang akan disimpan. Data `id_kasus` merupakan data unik yang dihasilkan oleh sistem yang merupakan primary key. Kemudian ada 7 data yang merupakan foreign key yaitu; `idkejahatan`, `idjeniskejahatan`, `idfr`, `idininvestigator`, `idjaksa`, `idpengacara` dan `idpenyidik`.

Tabel 4. 5 komponen tabel kasus

No	Nama Kolom	Type Data	Panjang Karakter	Key
1.	id_kasus	Integer	11	Primary key
2.	Idkejahatan	id_kasus	Integer	Foreign Key
3.	Idjeniskejahatan	id_kasus	Integer	Foreign Key
4.	idfr	id_kasus	Integer	Foreign Key
5.	Idinvestigator	id_kasus	Integer	Foreign Key
6.	Idjaksa	id_kasus	Integer	Foreign Key
7.	idpengacara	id_kasus	Integer	Foreign Key
8.	idpenyidik	id_kasus	Integer	Foreign Key
9.	file_name	varchar	255	-
10.	File_name_new	Text	-	-
11.	Size	varchar	8	-
12.	sha1	varchar	255	-
13.	md5	varchar	255	-
14.	file_location	Text	-	-
15.	date_uploaded	varchar	255	-
16.	case_number	varchar	255	-
17.	case_name	varchar	255	-
18.	suspect_name	varchar	255	-
19.	victim_name	varchar	255	-
20.	Tools	varchar	64	-
21.	description	Text	-	-
22.	time_cs	varchar	32	-
23.	location_cs	Text	-	-
24.	no_reg	varchar	128	-
25.	Model	varchar	64	-
26.	serial_number	varchar	128	-
27.	Type	varchar	128	-
28.	Manufacturer	varchar	64	-
29.	Capacity	varchar	8	-
30.	reason	Text	-	-
31.	Potential_info	Text	-	-
32.	Time_acq	varchar	64	-
33.	Tools_acq	varchar	255	-
34.	status	varchar	16	-
35.	year	Integer	4	-

4.1.4.6 Relasi Antar Tabel

Database sistem pengelolaan bukti digital ini memuat lima tabel, antara satu tabel dengan tabel lainnya saling memiliki hubungan. Hal ini terjadi karena data-data yang disimpan memang memiliki keterkaitan antara data satu dengan data yang lain. Hubungan ini yang disebut relasi antar tabel. Dengan menentukan jenis hubungan satu tabel dengan tabel lainnya untuk memaksimalkan penggunaan tabel yang ada.



Gambar 4. 17 Relasi Antar Tabel

4.2 Perangkat Pendukung Penelitian

Pada bab ini akan dijelaskan tentang bagaimana sistem diuji pada ke tahap analisis terhadap hasil dari sistem. Pengujian sistem dilakukan dengan menggunakan 3 simulasi kasus yang pernah terjadi di Indonesia, namun nama dan barang bukti yang diperoleh adalah Perangkat Pendukung

Dalam implementasi sistem manajemen pengelolaan bukti digital ini perlu dijelaskan spesifikasi perangkat keras dan perangkat lunak yang digunakan untuk menjalankan sistem sebagai acuan dalam implementasi yang lebih luas.

4.2.1 Perangkat Keras

Dalam perancangan, pembuatan dan pengujian sistem menggunakan Laptop dan PC server, berikut adalah spesifikasi laptop dan PC server yang digunakan:

Tabel 4. 6 Spesifikasi Laptop yang Digunakan

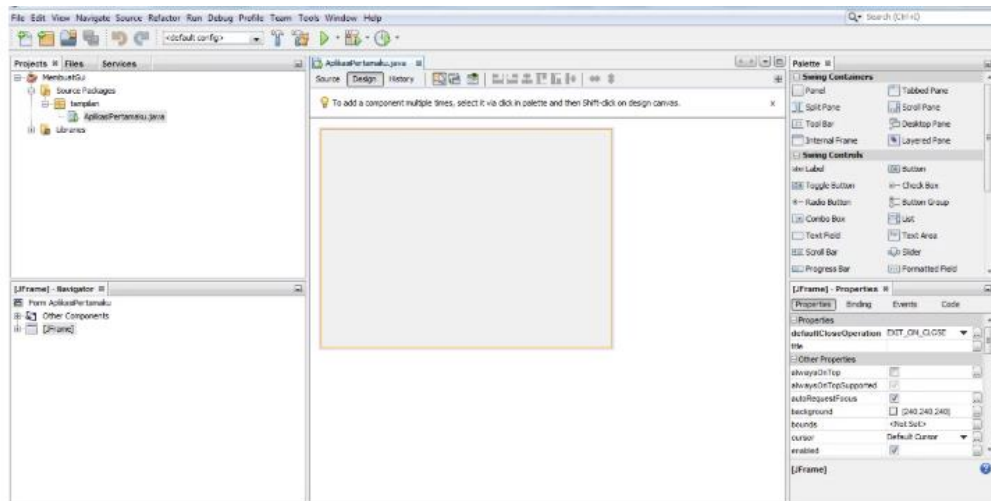
No.	Komponen	Deskripsi
1.	Nomor Serial Laptop	X452EA-VX027D
2.	Ukuran Layar	14 inch
3.	Grafis	Radeon HD graphics 1.4 GHz
4.	Resolusi	1366 x 768
5.	Prosesor	AMD E1-2500 APU
6.	Kapasitas RAM	DDR3 4GB
7.	Harddisk	500GB
8.	Port USB	2x Port USB 2.0
9.	Koneksi	IEEE 802.11 b/g/n dan Bluetooth V4.0
10.	Optical Drive	DVDRW
11.	Berat	2 Kg

Tabel 4. 7 Spesifikasi PC Server yang Digunakan

No.	Komponen	Deskripsi
1.	Grafis	Inter® HD Graphics
2.	Resolusi	1366 x 768
3.	Prosesor	Intel® Core™ i5-4460 3.20 GHz
4.	Kapasitas RAM	DDR3 8GB
5.	Harddisk	1000GB
6.	Port USB	6x Port USB 3.0
7.	Koneksi	LAN
8.	Optical Drive	DVDRW

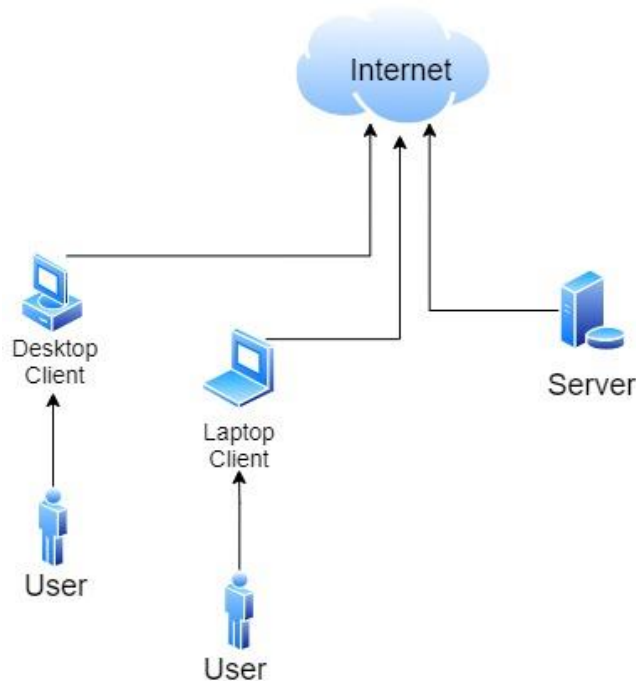
4.2.2 Perangkat Lunak

Perangkat lunak yang digunakan dalam penelitian ini menggunakan Sistem Operasi Microsoft Windows 10 Pro. Serta menggunakan aplikasi untuk menerjemahkan bahasa pemrograman (*source code*) kedalam bahasa objek (*object code*). *Compiler* yang digunakan untuk membuat adalah NetBeans IDE 8.2. Gambar 4.4 menunjukkan tampilan NetBeans IDE 8.2. Untuk membuat sistem pengelolaan bukti digital ini dapat diakses melalui internet maka sistem dirancang dengan aplikasi server XAMPP dengan versi 3.2.4.



Gambar 4. 18 Halaman NetBeans IDE 8.2

4.2.3 Arsitektur Jaringan

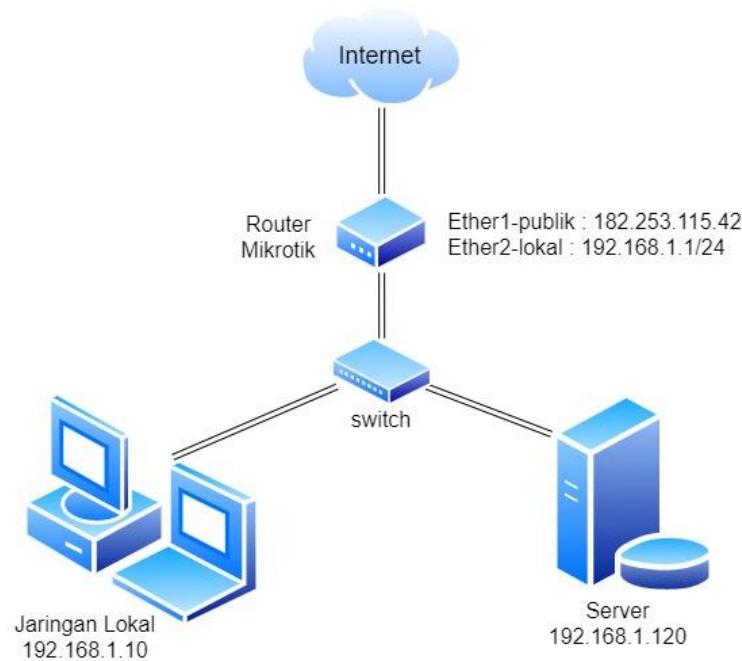


Gambar 4. 19 Arsitektur Jaringan

Untuk memenuhi kebutuhan akses yang luas maka aplikasi harus dapat diakses melalui jaringan internet. Dengan demikian sistem dapat digunakan dimana saja dan kapan saja. Adapun kebutuhan sistem untuk mendukung jaringan ini adalah; *user*, perangkat *client*, akses internet dan *server*. Untuk gambaran rancangan arsitektur dapat dilihat pada gambar 4.17.

Untuk akses melalui internet *user* dapat mengakses dengan membuka halaman dengan alamat IP 192.168.1.120 yang merupakan IP webserver lokal dari sistem pengelolaan bukti digital. Agar dapat diakses melalui internet maka harus menggunakan

internet dengan IP publik, pengaturan akses menggunakan modem mikrotik untuk meneruskan akses ke alamat IP publik 182.253.115.42. Untuk konfigurasi IP dapat dilihat pada gambar 4.18



Gambar 4. 20 Konfigurasi IP

Dengan dapat diaksesnya server dengan IP publik maka sistem pengelolaan bukti digital dapat diakses dari mana saja dan kapan saja

4.3 Simulasi Kasus

Bagian ini adalah subbab yang berisi simulasi cerita mengenai beberapa kasus yang ditangani sistem. Simulasi kasus ini juga dibuat sebagai bentuk pratinjau dari kasus yang akan digunakan. Tahap ini akan menunjukkan bagaimana alur kerja sistem serta pihak-pihak yang terlibat dalam kerja sistem. Pada simulasi kasus ini akan menggunakan 3 contoh kasus, yaitu kasus pemerasan, penghinaan tertulis dan penyebaran konten pornografi.

Kasus pemerasan yang digunakan sebagai simulasi kasus adalah sebuah kasus tentang pemerasan yang dilakukan oleh oknum polisi kepada seorang warga sipil dengan mengancam akan dimasukkan ke dalam penjara bila tidak diberi sejumlah uang yang diminta oleh tersangka. Barang bukti yang ditemukan dalam kasus ini adalah sebuah handphone milik korban yang berisi percakapan antara korban dengan pelaku melalui media aplikasi WhatsApp.

Bukti digital yang didapat kemudian diakusisi oleh Faiz sekaligus sebagai first responder berupa file backup chat yang belum terhapus, yang menjadi investigator adalah Reza Audiansyah dan Baskoro Aditomo sebagai officer.

Kasus berikutnya merupakan kasus pencemaran nama baik yang dilakukan melalui media sosial facebook. Bukti elektronik yang ditemukan berupa satu unit laptop. Bukti digital yang ditemukan adalah sebuah gambar hasil tangkapan layar yang tersimpan pada laptop korban. Bukti digital tersebut berisi unggahan status pelaku yang bermuatan fitnah dan mencemarkan nama baik korban. First responder dipegang oleh Krisna Widatama, Syarippudin sebagai investigator dan Baskoro Aditomo sebagai officer.

Kasus ketiga adalah penyebaran konten pornografi. Kasus ini berupa penyebaran video porno yang diunggah melalui media penyimpanan online yang linknya disebarakan melalui situs pribadinya. Video tersebut disinyalir direkam secara diam-diam tanpa sepengetahuan korban.

First responder pada kasus ketiga adalah Faiz, investigator adalah Martin Surya dan officer Baskoro Aditomo. Tabel 4.12 menunjukkan deskripsi simulasi kasus untuk pengujian sistem.

Tabel 4. 8 Deskripsi Simulasi Kasus

No.	Kasus	Jumlah Barang Bukti		Nama Petugas		
		Jenis Elektronik	Nama Bukti Digital	<i>First Responder</i>	<i>Investigator</i>	<i>Officer</i>
1.	Pemerasan	Smartphone	ss_whatsa pp.pdf	Faiz	Reza Audiansyah	Baskoro Aditomo
2.	Pencemaran nama baik	Komputer Smartphone	ss_whatsa pp.pdf	Krisna Widatama	Syarippudin	
3.	Video Porno	Komputer	mv_youtu be.mp4	Faiz	Martin Surya	

4.4 Pengujian Sistem

Pada bab pengujian ini menggunakan pengujian dengan metode *black box*, Pengujian *black box* berfokus pada persyaratan fungsional yang dimiliki perangkat lunak dengan mengamati proses input data yang dilakukan serta mengamati hasil output yang dihasilkan. Selain itu pengujian juga dilakukan dengan membandingkan hasil keluaran sistem yang dirancang dengan sistem yang sudah ada sebelumnya baik secara kelengkapan fungsi pencatatan pada *form chain of custody* maupun hasil keluaran fungsi hash MD5 dan SHA1 yang dihasilkan oleh tools tertentu.

Dari pengujian ini diharapkan menemukan kelemahan sistem yang telah dirancang kemudian menyusun solusi atas kelemahan tersebut.

4.4.1 Pengujian Dengan Metode *Black Box*

Untuk memudahkan dalam tahap pengujian ini maka dibuat sebuah tabel dengan membagi menjadi beberapa kelas dan butir-butir pengujian. Tabel rencana pengujian dapat dilihat pada tabel 4.13

Tabel 4. 9 Rencana Pengujian

Kelas Uji	Butir Uji	Jenis Pengujian
Sign In	Verifikasi Password	<i>Black Box</i>
Pengolahan Data Pengguna	Tambah Data Pengguna	<i>Black Box</i>
	Ubah Data Pengguna	<i>Black Box</i>
Pengolahan Data Bukti Digital (first responder)	Unggah Bukti Digital	<i>Black Box</i>
	Input Data Kelengkapan Bukti Digital	<i>Black Box</i>
Pengolahan Data Bukti Digital (officer)	Aktivasi Status Kasus	<i>Black Box</i>
	Unduh Form <i>Chain of Custody</i>	<i>Black Box</i>
Pengolahan Data Bukti Digital (investigator)	Unduh Bukti Digital	<i>Black Box</i>
	Melengkapi data kasus	<i>Black Box</i>
Pengolahan Data Kasus	Perubahan Data Statistik Dashboard	<i>Black Box</i>
Pengolahan Data Interaksi Bukti Digital	Penambahan Data Interaksi Bukti Digital	<i>Black Box</i>

Pengujian dilakukan dengan memasukkan data yang memiliki dua kondisi yang berbeda yakni data normal dan data salah, hal ini dimaksudkan untuk melihat hasil pengolahan data yang dilakukan oleh sistem telah sesuai dengan harapan atau tidak tanpa melihat proses didalamnya. Hal ini dilakukan untuk mendapatkan hasil pengujian yang cepat berbasis pada hasil keluaran sistem yang dirancang.

4.4.1.1 Pengujian Sign In

Saat pertama kali membuka sistem pengelolaan bukti digital ini pengguna akan dihadapkan pada halaman *sign in*. halaman ini diibaratkan sebagai sebuah pintu masuk kedalam sebuah ruangan, hanya orang yang memiliki kunci saja yang bisa memasukinya. Hal ini dilakukan bukan tanpa alasan melainkan untuk menjaga sistem agar sistem ini hanya bisa diakses oleh orang yang memiliki otoritas saja. Berikut ini adalah tabel pengujian login untuk verifikasi nama pengguna dan *password*:

Tabel 4. 10 Pengujian Sign In

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Username dan password yang telah terdaftar	Nama pengguna tercantum pada teks nama pengguna, password tercantum pada teks password	Nama pengguna tercantum pada teks nama pengguna, ***** tercantum pada teks password	Diterima
Klik tombol sign in	Masuk ke halaman menu sesuai otorisasi pengguna, muncul nama pengguna di halaman utama	Masuk ke halaman menu sesuai otorisasi pengguna, Muncul pemberitahuan sign in berhasil, muncul nama pengguna di halaman utama	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
username dan password yang belum terdaftar	Nama pengguna tercantum pada teks nama pengguna, password tercantum pada teks password	Nama pengguna tercantum pada teks nama pengguna, ***** tercantum pada teks password	Diterima
Klik tombol sign in	Gagal memasuki halaman pengguna	Gagal memasuki halaman pengguna, muncul pemberitahuan sign in gagal	Diterima

Pada tabel pengujian sign in dapat dilihat bahwa hanya pengguna yang telah terdaftar saja yang dapat masuk ke dalam sistem, dan menu yang ditampilkan akan menyesuaikan dengan otoritas masing-masing pengguna. Hal ini dimaksudkan supaya pengguna yang tidak memiliki otoritas tidak dapat mengakses data bukti digital yang dikelola. Dengan keterbatasan akses tersebut diharapkan bukti digital yang disimpan tetap aman dan tidak dimanipulasi oleh pihak tertentu sehingga bukti digital yang dikelola tetap terjamin keasliannya dan dapat dipertanggungjawabkan di dalam persidangan.

4.4.1.2 Pengujian Pengolahan Data Pengguna

Tahap ini menguji kemampuan sistem untuk menambahkan data pengguna baru. Sistem diharapkan dapat mengelola data pengguna dengan baik yaitu dengan cara menambahkan pengguna baru dan memberikan otoritas yang sesuai dengan tugas yang dimiliki.

Tabel 4. 11 Pengujian Tambah Data Pengguna

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Nama lengkap pengguna, asal institusi, username, password, otorisasi pengguna	Data tampil pada kolom sesuai masukan pengguna	Dapat mengisi kolom yang disediakan dan data muncul pada kolom sesuai masukan	Diterima
Klik tombol save	Semua data tersimpan dalam <i>database</i>	Semua data tersimpan dalam database dan nama pengguna baru muncul pada daftar pengguna	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Salah satu data atau semua data tidak diisi	Data tidak disimpan dan muncul pesan kesalahan	Muncul pesan perintah untuk mengisi kolom yang masih kosong, tidak dapat melanjutkan proses menambahkan pengguna baru	Diterima

Tabel 4. 12 Pengujian Ubah Data Pengguna

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol detail pengguna	Menampilkan data pengguna yang akan dirubah	Menampilkan data pengguna dan tombol <i>reset password</i>	Diterima
Klik tombol save	Data perubahan tersimpan di tabel pengguna.	Tidak dapat merubah data pengguna namun bisa melakukan <i>reset password</i> .	Tidak diterima
Klik tombol batal	Data perubahan tidak tersimpan. Kembali ke halaman pengolahan data pengguna.	Data perubahan tidak tersimpan. Kembali ke halaman pengolahan data pengguna.	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Salah satu data atau semua data tidak diisi	Data tidak disimpan dan muncul pesan kesalahan	Kembali ke menu pengolahan data pengguna dan data tidak disimpan.	Diterima

4.4.1.3 Pengujian Pengolahan Data Bukti Digital (first responder)

Pada tahap ini pengujian sistem dilakukan dengan mengunggah bukti digital dimana tahap ini merupakan tahap permulaan dalam pengelolaan bukti digital. Bukti digital yang diunggah harus dilengkapi dengan data kasus yang menyangkut bukti digital tersebut supaya dapat menghasilkan *form chain of custody* yang sesuai dengan kebutuhan.

Bukti digital yang diunggah nantinya akan diberikan nilai fungsi hash dengan metode SHA1 dan MD5 oleh sistem secara otomatis. Hal ini bertujuan untuk membuktikan bahwa bukti digital yang disimpan merupakan bukti digital yang asli tanpa melalui tahap rekayasa. Bukti digital yang akan digunakan untuk persidangan hendaknya sama dengan bukti digital yang diakuisisi oleh *first responder* hal ini dapat dikonformasi dari nilai fungsi hash yang sama, karena ketika ada sedikit perubahan pada bukti digital tersebut maka nilai fungsi hash bukti digital tersebut otomatis akan berubah dan akan melemahkan kekuatan bukti digital tersebut sebagai barang bukti di dalam persidangan.

Tabel 4. 13 Unggah Bukti Digital

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Memilih Kasus, sub kasus, officer, investigator, jaksa, pengacara, penyidik, memilih file bukti digital	Menampilkan isian data yang sudah disimpan dan disediakan oleh sistem, dapat menelusuri berkas file bukti digital yang akan diunggah	Menampilkan isian data yang sudah disimpan dan disediakan oleh sistem, dapat mencari berkas file bukti digital dengan berbagai macam ekstensi	Diterima
Klik tombol save	Data tersimpan pada database, bukti digital disimpan pada server.	Data tersimpan pada database bukti digital, berkas bukti digital telah tersimpan pada server	diterima
Klik tombol batal	Data perubahan tidak tersimpan. Kembali ke halaman utama.	Data perubahan tidak tersimpan. Kembali ke halaman utama.	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Salah satu data atau semua data tidak diisi	Data tidak disimpan dan muncul pesan kesalahan	Tidak dapat menyimpan data dan muncul pesan perintah untuk mengisi pilihan atau memilih berkas untuk diunggah	Diterima

Tabel 4. 14 Input Kelengkapan Data Bukti Digital

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol proses (Kasus telah diaktivasi oleh officer)	Menampilkan kolom data bukti digital yang akan dilengkapi datanya	Menampilkan data bukti digital yang akan dilengkapi datanya	Diterima
Data olah TKP, data bukti elektronik, data akuisisi, data keterangan	Menampilkan data sesuai masukan pada komom olah TKP, data bukti elektronik, data akuisisi, data keterangan	Menampilkan data sesuai masukan pada komom olah TKP, data bukti elektronik, data akuisisi, data keterangan	Diterima
Klik tombol save	Perubahan atau penambahan data tersimpan pada database	Perubahan atau penambahan data tersimpan pada database	Diterima
Klik tombol batal	Data perubahan tidak tersimpan.	Data perubahan tidak tersimpan.	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol proses (Kasus belum diaktivasi oleh officer)	Tidak dapat mengisi kelengkapan data bukti digital	Kolom kelengkapan bukti digital tidak muncul.	Diterima

4.4.1.4 Pengujian Pengolahan Data Bukti Digital (officer)

Tabel 4. 15 Aktivasi Status Kasus

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Memilih Kasus, sub kasus, first responder, bukti digital	Menampilkan status kasus	Menampilkan status kasus dan muncul tombol aktivasi	Diterima
Klik tombol aktif	Status berubah dari tidak aktif menjadi aktif	Status berubah dari tidak aktif menjadi aktif	Diterima
Klik tombol tidak aktif	Status berubah dari aktif menjadi tidak aktif	Tombol tidak aktif tidak muncul	Tidak diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan

Tabel 4. 16 Aktivasi Status Kasus (lanjutan)

Klik tombol aktif pada data yang sudah aktif	Tidak dapat mengaktifkan data bukti digital dan muncul pesan kesalahan	Tombol aktif tidak muncul pada data yang sudah aktif	Diterima
--	--	--	----------

Tabel 4. 17 Unduh Form Chain of Custody

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Memilih Kasus, sub kasus, first responder, bukti digital	Menampilkan data bukti digital dan tombol unduh	Tombol unduh ditampilkan pada tabel data bukti digital	Diterima
Klik tombol unduh	Mengunduh file form Chain of custody dalam format .pdf	Muncul pesan konfirmasi unduh form chain of custody dan dapan menyimpan file dalam format .pdf	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol unduh pada data yang belum lengkap	Tidak dapat mengunduh dan muncul pesan kesalahan	Tombol unduh tidak muncul	Diterima

4.4.1.5 Pengujian Pengolahan Data Bukti Digital (investigator)

Pada tahap ini pengujian dilakukan untuk melihat kemampuan sistem dalam memberikan akses pada bukti digital yang dikelola oleh sistem.

Tabel 4. 18 Unduh Bukti Digital

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Memilih Kasus, sub kasus, first responder, bukti digital	Menampilkan data bukti digital dan tombol unduh	Tombol unduh ditampilkan pada tabel data bukti digital	Diterima
Klik tombol unduh	Mengunduh file bukti digital sesuai dengan file yang diunggah	Dapat mengunduh file yang telah diunggah oleh first responder	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol unduh pada data yang belum lengkap	Tidak dapat mengunduh dan muncul pesan kesalahan	Tombol unduh tidak muncul	Diterima

Tabel 4. 19 Melengkapi Data Kasus

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Memilih Kasus, sub kasus, first responder, bukti digital	Menampilkan data bukti digital dan muncul data kasus sesuai yang diinputkan	Tombol unduh ditampilkan pada tabel data bukti digital	Diterima
Klik tombol save	Menyimpan data kelengkapan kasus pada database	Menyimpan data kelengkapan kasus pada database	Diterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Salah satu data atau semua data tidak diisi	Data tidak disimpan dan muncul pesan kesalahan	Tidak dapat menyimpan data dan muncul pesan perintah untuk mengisi kolom yang masih kosong	Diterima

4.4.1.6 Pengujian Pengolahan Data Kasus

Tabel 4. 20 Perubahan Data Statistik Dashboard

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Menambahkan satu kasus baru; kejahatan terhadap jiwa seseorang	Data statistik kasus kejahatan terhadap jiwa seseorang meningkat sebanyak 1 kasus	Data statistic kasus kejahatan terhadap jiwa seseorang meningkat sebanyak 1 kasus	Diterima
Menghapus satu kasus kejahatan terhadap jiwa seseorang	Data statistik kasus kejahatan terhadap jiwa seseorang berkurang sebanyak 1 kasus	Tidak ada menu menghapus kasus	Tidak diiterima
Kasus dan Hasil Uji (Data salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Menambahkan satu kasus baru tanpa mengisi jenis kejahatan	Muncul pesan kesalahan dan data statistic tidak berubah	Tidak dapat menyimpan data dan muncul pesan perintah untuk mengisi kolom yang masih kosong	Diterima

Sistem ini juga menyajikan data dalam berupa grafik, meskipun masih sangat sederhana diharapkan data yang disajikan dapat memberikan kontribusi dalam pengambilan keputusan terkait kejahatan yang melibatkan bukti digital.

4.4.1.7 Pengujian Pengolahan Data Interaksi Bukti Digital

Tabel 4. 21 Perubahan Data Interaksi Bukti Digital

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
First responder melihat detail bukti digital	Terjadi penambahan data pada form <i>chain of custody</i>	Terjadi penambahan data pada form <i>chain of custody</i> dengan keterangan “melihat detail”	Diterima
First responder merubah detail bukti digital	Terjadi penambahan data pada form <i>chain of custody</i>	Terjadi penambahan data pada form <i>chain of custody</i> dengan keterangan “edit detail”	Diterima

Pengujian ini dilakukan dengan mengamati perubahan data pada interaksi dengan bukti digital yang dicatat oleh sistem, dimana setiap interaksi ini akan disajikan *pada form chain of custody* yang dihasilkan oleh sistem pengelolaan bukti digital.

4.4.2 Pengujian Nilai Hash

Sistem ini secara otomatis telah menghasilkan 2 nilai fungsi *hash*, yaitu fungsi *hash* MD5 dan fungsi *hash* SHA1 yang akan diuji dengan membandingkan dengan fungsi *hash* yang dihasilkan tools lain. Pengujian ini menggunakan 3 jenis *file* dengan format E01, Mp4 dan jpg yang sebelumnya telah diunggah pada sistem pengelolaan bukti digital, yaitu: BB hp.E01, 19111200113UQ0F.mp4 dan Picture 001.jpg. Ketiga bukti digital tersebut dapat dikatakan asli apabila nilai *hash* dari kedua bukti digital tersebut sama dengan nilai *hash* yang dihasilkan dari *tools* lain sehingga dapat disimpulkan tidak ada perubahan data pada bukti digital tersebut. Tabel 4.19 menunjukkan perbandingan antara nilai *hash* yang dihasilkan oleh sistem pengelolaan bukti digital dengan hasil nilai *hash* yang dihasilkan Autopsy dan sha1-online pada *file* BB hp.E01.

Tabel 4. 22 Perbandingan Hasil Nilai hash pada File BB hp.E01.

Nilai Hash Sistem Pengelolaan Bukti Digital	
SHA1	82a549a4682ed051ed633ece537fc18e4d10c089
MD5	c288fbabd6fe35faba3cebb210a047b6
Nilai Hash Autopsy	
SHA1	82a549a4682ed051ed633ece537fc18e4d10c089
MD5	c288fbabd6fe35faba3cebb210a047b6
Nilai Hash sha1-online.com	
SHA1	82a549a4682ed051ed633ece537fc18e4d10c089
MD5	c288fbabd6fe35faba3cebb210a047b6

Pengujian nilai *hash* selanjutnya adalah bukti digital dengan nama 19111200113UQ0F.mp4. Tabel 4.20 menunjukkan perbandingan hasil nilai *hash* antara sistem pengelolaan bukti digital dengan hasil nilai *hash* dari Autopsy dan sha1-online.

Tabel 4. 23 Perbandingan Hasil Nilai hash pada File 19111200113UQ0F.mp4

Nilai Hash Sistem Pengelolaan Bukti Digital	
SHA1	edffba1cfb0d90f1dc71f099526b0bcc06a929c3
MD5	b5ea72348b6250de46876a2b9ad38504
Nilai Hash Autopsy	
SHA1	edffba1cfb0d90f1dc71f099526b0bcc06a929c3
MD5	b5ea72348b6250de46876a2b9ad38504
Nilai Hash sha1-online.com	
SHA1	edffba1cfb0d90f1dc71f099526b0bcc06a929c3
MD5	b5ea72348b6250de46876a2b9ad38504

Pengujian nilai yang ketiga adalah bukti digital dengan format jpg dengan nama file Picture 001.jpg. Tabel 4.21 menunjukkan perbandingan hasil nilai *hash* antara sistem pengelolaan bukti digital dengan hasil nilai *hash* dari Autopsy dengan sha1-online.

Tabel 4. 24 Perbandingan Hasil Nilai hash pada File file Picture 001.jpg.

Nilai Hash Sistem Pengelolaan Bukti Digital	
SHA1	3512bf44e554020c6786f7f370180c4612a38b09
MD5	c5a768fa444e40927b891657f8f0e4d2
Nilai Hash Autopsy	
SHA1	3512bf44e554020c6786f7f370180c4612a38b09
MD5	c5a768fa444e40927b891657f8f0e4d2
Nilai Hash sha1-online.com	
SHA1	3512bf44e554020c6786f7f370180c4612a38b09
MD5	c5a768fa444e40927b891657f8f0e4d2

4.4.3 Pengujian Form Chain of Custody Hasil Keluaran

Pengujian *form digital chain of custody* dari hasil *output* sistem pengelolaan bukti digital dilakukan dengan cara membandingkan *field* yang ditampilkan pada *form digital chain of custody* dari sistem pengelolaan bukti digital dengan *form digital chain of custody* yang sebelumnya telah dilakukan oleh Devi Ratnasari (Ratnasari et al., 2018). Pembuatan *form digital chain of custody* pada penelitian sebelumnya dibuat berdasarkan rumus 5W1H, yaitu: When, Where, Who, What, Why dan How. Tabel 4.28 menunjukkan perbandingan *output* format laporan *chain of custody* antara sistem pengelolaan bukti digital dengan penelitian terdahulu.

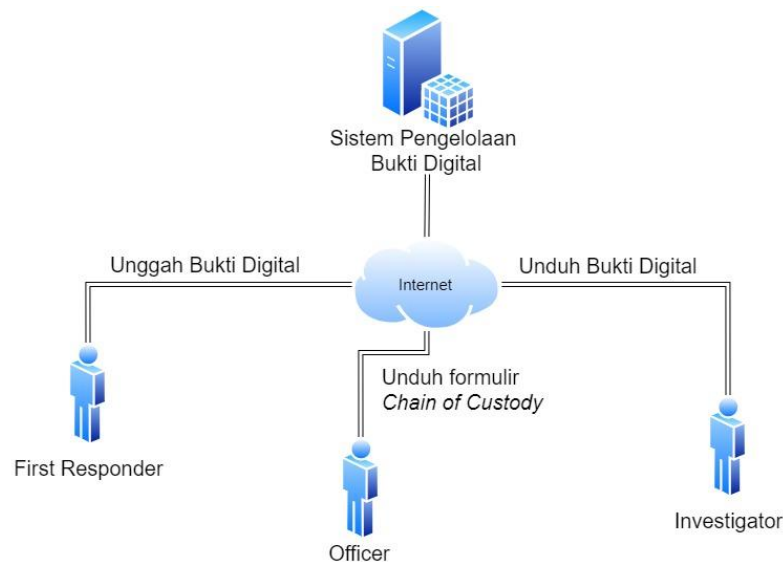
Dengan membandingkan formulir yang dihasilkan oleh sistem yang dirancang dengan formulir yang sudah diteliti sebelumnya maka dapat diketahui perbedaan dan peningkatan yang dimiliki oleh sistem yang dirancang namun tetap memenuhi aspek kebutuhan kelengkapan data yang digunakan dalam pelaporan investigasi.

Tabel 4. 25 Perbandingan *Chain of Custody* dengan Penelitian Sebelumnya

No.	Informasi	Ketersediaan Dalam <i>Form</i>			
		Sistem Baru		Penelitian Sebelumnya	
		Ada	Tidak Ada	Ada	Tidak Ada
Informasi Olah TKP					
1.	Nama kasus	✓		✓	
2.	Jenis Kejahatan	✓			✓
3.	Nama tersangka	✓		✓	
4.	Nama korban	✓		✓	
5.	Lokasi	✓		✓	
6.	Waktu	✓		✓	
7.	Nama <i>tools</i> (live forensic)	✓		✓	
8.	Deskripsi <i>tools</i>	✓			✓
9.	Nama <i>first responder</i>	✓			✓
10.	Nama Institusi	✓			✓
11.	Jabatan		✓	✓	
Informasi Bukti Elektronik					
12.	Nomor registrasi	✓		✓	
13.	Tipe	✓		✓	
14.	Nama Model	✓		✓	
	Nama Produsen	✓		✓	
15.	Nomor serial	✓		✓	
16.	Deskripsi Fisik		✓	✓	
17.	Alasan utama penyitaan	✓		✓	
Akuisisi Bukti Digital					
18.	Waktu	✓		✓	
19.	Nama <i>tools</i>	✓		✓	
20.	Tanggal	✓		✓	
21.	Nama Petugas	✓		✓	
22.	Device	✓		✓	
Informasi Bukti Digital					
23.	Nomor kasus	✓			✓
23.	Nama <i>file</i>	✓		✓	
24.	Ukuran <i>file</i>	✓		✓	
25.	Nilai <i>hash</i> (SHA1)	✓		✓	
26.	Nilai <i>hash</i> (MD5)	✓		✓	
27.	Nilai <i>hash</i> (SHA 256)		✓	✓	
28.	Lokasi penyimpanan	✓		✓	
29.	Lokasi penyimpanan	✓		✓	
30.	Tanggal/waktu simpan	✓		✓	
31.	Validator	✓		✓	
32.	Informasi yang ingin didapatkan	✓		✓	
33.	Status kasus	✓		✓	

4.4.4 Aksesibilitas Bukti Digital

Untuk memberikan solusi atas kendala yang dihadapi petugas pada sistem yang telah ada saat ini, maka dalam perancangan sistem ini juga mempertimbangkan aksesibilitas bukti digital yang dikelola pada sistem. Aksesibilitas ini berupa fitur yang memungkinkan untuk mengunggah, mengunduh dan *generate* formulir *chain of custody* secara daring. Konsep aksesibilitas dapat dilihat pada gambar 4.19.



Gambar 4. 21 Konsep aksesibilitas sistem

Dengan rancangan sistem yang diusulkan, petugas dapat melaksanakan tugas mereka masing-masing tanpa perlu datang ke laboratorium forensika digital. *First Responder* dapat mengunggah bukti digital, *Investigator* mengunduh bukti digital dan *officer* mengunduh formulir *chain of custody* melalui sistem yang disediakan secara daring melalui internet.

Hal ini memberikan solusi atas masalah dan resiko yang dihadapi para petugas pada sistem yang sudah ada selama ini. Masalah yang dihadapi dapat berhubungan langsung dengan bukti digital maupun terhadap pribadi petugas itu sendiri. Hal ini perlu diperhatikan karena sangat berpengaruh dalam keberlangsungan proses investigasi kasus dan proses persidangan terhadap kasus yang terkait pada bukti digital. Perbandingan ini dapat dilihat pada tabel 4.29.

Dari tabel 4.29 dapat disimpulkan bahwa aksesibilitas bukti digital berperan sangat penting dalam suatu sistem bukti digital. Dimana aspek inilah yang dikembangkan pada usulan sistem yang baru sebagai upaya untuk memberikan solusi atas masalah yang ada pada sistem sebelumnya.

Tabel 4. 26 Perbandingan Aksesibilitas Bukti Digital

No	Aktifitas	Sistem Pengelolaan Bukti Digital	
		Penelitian sebelumnya	Sistem baru
1.	Penyerahan Bukti Digital	1. Membutuhkan waktu yang lama 2. Beresiko rusak atau hilangnya data dalam perjalanan. 3. Memungkinkan terjadinya sabotase fisik oleh pihak tertentu.	Dilakukan secara daring, meminimalisir resiko yang ada.
2.	Investigasi Bukti Digital	1. Memerlukan waktu untuk datang ke laboratorium. 2. Investigasi terbatas dengan peralatan yang ada di laboratorium. 3. Investigator harus membawa perlengkapan yang dimiliki ke laboratorium jika investigasi dilakukan di laboratorium	Data dapat diakses secara daring dan diinvestigasi di laboratorium milik pribadi. Sehingga dapat menggunakan perlengkapan pribadi investigator yang lebih canggih.
3.	Penyimpanan Bukti digital	Bukti digital disimpan pada penyimpanan lokal sehingga hanya bisa diakses di laboratorium bukti digital.	Bukti digital disimpan pada server dan dapat diakses dari mana saja dan kapan saja.
4.	Unduh formulir <i>chain of custody</i>	Harus datang langsung ke laboratorium meskipun file sudah berupa pdf.	Dapat diunduh kapanpun dan dimanapun sehingga persiapan untuk persidangan menjadi lebih efisien.
5.	Kontak Fisik antar petugas	Harus menerapkan protokol pencegahan penularan Covid-19.	Tidak ada kontak fisik.

4.4.5 User Acceptance

Sistem yang dirancang hendaknya diujikan kepada pengguna supaya dapat diketahui apakah sistem yang dirancang sudah memenuhi kebutuhan pengguna dan sesuai dengan proses yang berjalan.

Proses penilaian dengan melakukan simulasi pengelolaan bukti digital secara daring dengan mengunggah bukti digital, mengisi jenis kejahatan, mengisi detail kasus, mengunduh bukti digital, mengunduh formulir *chain of custody*. Dari beberapa penguji secara bergantian *log in* kedalam sistem dengan hak otorisasi yang berbeda-beda kemudian mengamati proses yang berjalan.

Sedangkan penilaian hasil simulasi dicatat menggunakan *google form*. Penilaian dibagi menjadi empat bagian utama, yaitu; Keseuaian alur, Kemudahan dalam mengakses bukti digital, kelengkapan data *chain of custody* dan manfaat sistem dalam pengelolaan bukti digital. Hasil penilaian dapat dilihat pada tabel 4.30.

Tabel 4. 27 Tabel Penilaian *expert*

No	Poin Penilaian	Hasil
1	Kesesuaian alur / bisnis proses	Alur yang ditunjukkan oleh sistem telah memenuhi kebutuhan pada alur penanganan bukti digital yang telah berjalan. Dimulai dari petugas yang berada di lapangan (first responder) melakukan upload bukti digital dan mengirim laporan dari TKP secara langsung. Petugas menerima laporan dan menugaskan penyidik untuk proses investigasi. Penyidik dapat mendownload bukti digital, melakukan investigasi dan mengisi hasil investigasi pada sistem. Kemudian sistem memberikan laporan berupa form coc yang dapat dicetak oleh petugas. Namun perlu diperhatikan dalam proses pengisian nomor kasus sebaiknya diintegrasikan dengan sistem yang sudah ada supaya tidak terjadi kesalahan dalam penulisan nomor kasus.
2	Kemudahan dalam mengakses bukti digital	Bukti digital yang sudah disimpan dalam sistem dapat diakses dengan cepat tanpa harus datang ke laboratorium dan copy bukti digital secara manual. Namun perlu diperhatikan keamanan datanya, sehingga data tidak diakses oleh orang yang tidak berwenang dan disalahgunakan.
3	Kelengkapan data CoC	Formulir coc yang dihasilkan oleh sistem dapat dibilang telah memenuhi kebutuhan proses pelaporan dan persidangan. baik dari kelengkapan data bukti digital, kelengkapan petugas yang menangani dan dokumentasi interaksi bukti digital
4	Manfaat sistem dalam pengelolaan bukti digital	Sistem yang dirancang sangat membantu dalam proses pengelolaan bukti digital, memberikan kemudahan dalam mengakses bukti digital yang selama ini berjalan secara manual dan offline menjadi online. Proses investigasi dapat berjalan lebih cepat. Namun perlu disederhanakan dalam tahap input data, jenis data yang dapat diinput disesuaikan dengan kebutuhan data.

Dari tabel 4.30 dapat disimpulkan bahwa sistem yang dirancang telah memenuhi kebutuhan dalam pengelolaan bukti digital serta menyediakan akses bukti digital yang lebih luas dengan tetap memperhatikan alur yang berlaku. Namun demikian sistem ini masih memerlukan sedikit peningkatan keamanan data.

4.4.6 Analisis Kelebihan dan Kekurangan Sistem

Setelah proses implemtasi 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.

1. Penyimpanan bukti digital dan informasi bisa diakses secara daring, bukti digital dapat diunduh dari mana saja, *generate form CoC* lebih mudah sehingga dapat

mengisi data dari manapun dan kapanpun dan proses investigasi dapat berjalan lebih cepat.

2. Pembuatan kategori bukti digital berdasarkan jenis kejahatan secara umum dan khusus yang kemudian diakumulasi agar dapat diketahui jumlah kejahatan yang terjadi yang nantinya data ini dapat dimanfaatkan untuk keterkaitan bukti digital dengan jenis kejahatan yang dilakukan dengan harapan mampu memberi masukan dalam penyusunan undang-undang informasi dan teknologi.
3. Sistem *login* yang digunakan dalam sistem ini telah mampu mendeteksi pengguna yang masuk berdasarkan tugas mereka dalam penanganan bukti digital. Selain itu, sistem ini juga memiliki *log* yang dapat mencatat pengguna yang masuk. Hal ini dapat mencegah terjadinya *unauthorized access* terhadap pengguna yang masuk.

Selain memiliki kelebihan, sistem ini juga memiliki kelemahan. Kelemahan ini merupakan kekurangan sistem yang dapat digunakan sebagai bahan penelitian selanjutnya untuk meningkatkan kinerja sistem ini dalam penanganan bukti digital. berikut adalah kekurangan sistem pengelolaan bukti digital.

1. Dashboard yang disediakan masih sangat sederhana, sehingga belum mampu memberikan informasi yang lebih lengkap dan menarik.
2. Penyimpanan bukti digital yang terpusat dalam satu komputer akan membutuhkan ruang penyimpanan yang sangat besar. Pada praktiknya, bukti digital yang tersimpan membutuhkan ruang penyimpanan yang sangat besar terutama bukti digital hasil akuisisi dari perangkat Harddisk.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan data yang didapat dari proses implementasi hingga ke tahap pengujian, maka didapat beberapa kesimpulan, yaitu:

1. Sistem pengelolaan bukti digital yang diusulkan dapat meningkatkan aksesibilitas bukti digital yang sangat berpengaruh dalam proses investigasi. Mulai dari tahap penyerahan bukti digital, unduh bukti digital penyimpanan hingga proses unduh formulir *chain of custody* dilakukan secara daring tanpa harus datang ke laboratorium forensika digital sehingga proses investigasi berjalan lebih cepat dan meminimalisir resiko kerusakan pada bukti digital dan keselamatan petugas.
2. Formulir digital *chain of custody* terdiri dari 3 halaman. Halaman pertama berisi informasi bukti elektronik, metadata bukti digital hingga akuisisi. Halaman kedua berisi interaksi antara pengguna terhadap bukti digital melalui sistem pengelolaan bukti digital. Halaman ketiga berisi validasi untuk pengesahan formulir digital *chain of custody* yang dihasilkan oleh sistem bukti digital.
3. Bukti digital dikategorikan berdasarkan jenis kejahatan yang disesuaikan dengan perundang-undangan yang berada di Indonesia, sehingga aplikasi ini sesuai untuk digunakan untuk membantu proses hukum yang berjalan di Indonesia.

5.2 Saran

Adapun saran-saran yang perlu diberikan dalam penelitian ini adalah:

1. Memperkaya komponen pada dashboard dengan informasi yang lebih variatif dan menarik serta dilengkapi dengan sistem analisis dari data yang sudah dikumpulkan sehingga dapat digunakan sebagai sistem pendukung keputusan.
2. Menyediakan enkripsi data bukti digital untuk meningkatkan keamanan dan akuntabilitas bukti digital yang dikelola.

Daftar Pustaka

- 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.
- Dogan, S., & Akbal, E. (2017). Analysis of Mobile Phones in Digital Forensics. *2017 40th Convention on Information and Communication Technology, Electronics 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 Systems. *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.
- 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.
- 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>