Jurnal Ilmiah Sinus (JIS) Vol : 19, No. 1, Januari 2021
ISSN (Print) : 1693-1173, ISSN (Online): 2548-4028

Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Pada Masa Pandemi Covid-19

Moch Bagoes Pakarti[1*)], Dhomas Hatta Fudholi[2)], Yudi Prayudi[3)]
[1)] Magister Teknik Informatika, Univesitas Islam Indonesia
[2, 3)] Teknik Informatika, Univesitas Islam Indonesia
[1)] bmovyz@gmail.com, [2)] hatta.fudholi@uii.ac.id, [3)] prayudi@uii.ac.id

ABSTRACT

Covid-19 has a major impact on human life, including the process of managing digital evidence. Management of digital evidence requires special handling that can store and maintain the integrity of digital evidence. The current problem is there is no concept of storing digital evidence that can be accessed online in 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 using MD5 and SHA1 hash functions in order to maintain the properties 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 application in Digital Forensics Laboratory. This research had successfully implemented the concept of online chain of custody. It is expected, with the concept of Online Digital Evidence Management, this digital evidence control and all activities related to it can be maintained and well documented. Moreover, it can reach a wider area accessed anywhere and any time and reduce the spread of Covid-19.

Keywords *: Digital Evidence, Chain of Custody, Accessibility*

I. PENDAHULUAN

Bukti merupakan informasi yang digunakan untuk membangun atau membantah sebuah fakta(Roscini, 2016). Barang bukti yang digunakan dapat berupa bukti digital atau bukti elektronik. Bukti elektronik dapat berupa komputer, telepon maupun hard disk. namun bukti digital berbentuk file yang tidak memiliki bentuk fisik, seperti: video, gambar digital, suara, log dan sebagainya. Tidak ada standar prosedur yang baku dalam hal penanganan kasus kejahatan komputer. Prosedur penanganan terdiri dari 5 langkah (Farmer & Venema, 2005), yaitu: mengamankan dan mencegah Tempat Kejadian Perkara (TKP) tersebut didatangi oleh orang yang tidak berkepentingan (secure and isolate), mencatat apa saja yang ditemukan di TKP (record the scene), mencari bukti yang ada di TKP secara sistematis (conduct a systematic search for evidence), mengemas barang bukti (collect and package evidence) dan membuat *chain of custody* (maintain chain of custody).

bukti digital memiliki risiko tinggi untuk digandakan, disebarluaskan, dihapus dan dimanipulasi oleh siapa saja(Prayudi, 2014). Jika terjadi akses ilegal terhadap bukti digital tersebut maka bukti digital tersebut dapat tertolak di pengadilan. Semua file bukti digital yang akan dianalisis seharusnya disimpan dalam suatu tempat dengan prosedur penyimpanan tertentu. Prosedur penyimpanan bukti digital saat ini sudah ada namun masih menemui kendala yaitu: model bisnis yang berkaitan dengan siapa saja yang akan berinteraksi dengan bukti digital tersebut, penyimpanan informasi metadata bukti digital dan akses kontrol terhadap bukti digital tersebut(Prayudi et al., 2014).

Pada saat ini sistem dituntut agar dapat diakses dari mana saja dan kapan saja. Hal ini diperlukan untuk meningkatkan kinerja investigasi yang tidak terbatas waktu dan ruang serta mengurangi risiko menularnya covid-19 pada saat proses penanganan bukti digital.

Solusi untuk kendala tersebut adalah dengan membuat sebuah sistem pengelolaan bukti digital yang prosedur penyimpanannya sama seperti bukti elektronik. Namun sistem

ini dapat diakses secara daring sehingga petugas dapat bekerja dari mana saja tanpa harus terjadi kontak fisik dengan petugas lainnya. Ketika bukti digital diunggah maka sistem akan mencatat kasus, jenis kejahatan dan siapa yang mengunggah bukti digital tersebut. Konsep ini akan memberikan pembatasan hak akses terhadap bukti digital tersebut sehingga tidak semua orang dapat mengaksesnya. Diharapkan dengan adanya konsep ini, dapat membuat bukti digital tersebut dapat memenuhi kriteria diterimanya suatu barang bukti di pengadilan (admissible, authentic, complete, reliable dan believable)(Prayudi & SN, 2015).

Pada penelitian tentang solusi *chain of custody* yang dilakukan oleh (Cosic & Baca, 2010) dan (Widatama & Yudi Prayudi, 2017) telah memberikan solusi namun belum sepenuhnya sesuai dengan kebutuhan penanganan *chain of custody*, terutama sekali dalam hal aksebilitas bukti digital yang masih sangat terbatas yang tidak dapat menghadapi tantangan di era pandemi covid-19 dewasa ini. Oleh sebab itu, makalah ini memberikan salah satu solusi yang diusulkan untuk memberikan kontribusi bagi penanganan dan penyimpanan bukti digital secara daring.

II. TINJAUAN PUSTAKA

2.1 Chain of custody

Chain of custody menjadi bagian yang sangat penting dalam proses penanganan bukti digital karena dijadikan sebagai jaminan diterimanya suatu bukti digital. Pencatatan bukti digital dilakukan sebagai dokumentasi secara aktif, proses pendokumentasian barang bukti ini disebut *chain of custody*. Ditinjau dari cara pendokumentasiannya, proses *chain of custody* tanpa menggunakan aplikasi tertentu tidak efisien dan tidak bisa menjamin saat berlangsungnya prosedur forensik. Hal ini karena prosesnya masih manual dan belum terotomatisasi dengan aplikasi(Giova, 2011).

Adapun hal-hal apa saja yang harus didokumentasikan dalam sebuah kasus adalah dengan menggunakan sebuah rumus yaitu 5W1H. Penggunaan formula ini merupakan formula standar yang sering digunakan oleh pihak kepolisian untuk membantu investigasi forensik(Cosic & Baca, 2010). Rumus ini merupakan gabungan dari 6 pertanyaan dalam Bahasa Inggris yaitu: what, when, who, why, where dan how. Implementasi formula ini pada konsep Lemari pengelolaan bukti digital adalah sebagai berikut:

A. *Who*

Merumuskan siapa saja yang memiliki kewenangan untuk berinteraksi dengan sistem. Terdapat 3 petugas yang berinteraksi langsung maupun tidak langsung dengan bukti digital tersebut, yaitu:

1) *First Responder*

First responder berperan sebagai orang yang pertama mengunggah bukti digital ke dalam pengelolaan bukti digital. Ia juga memiliki akses untuk mengisi *chain of custody.*

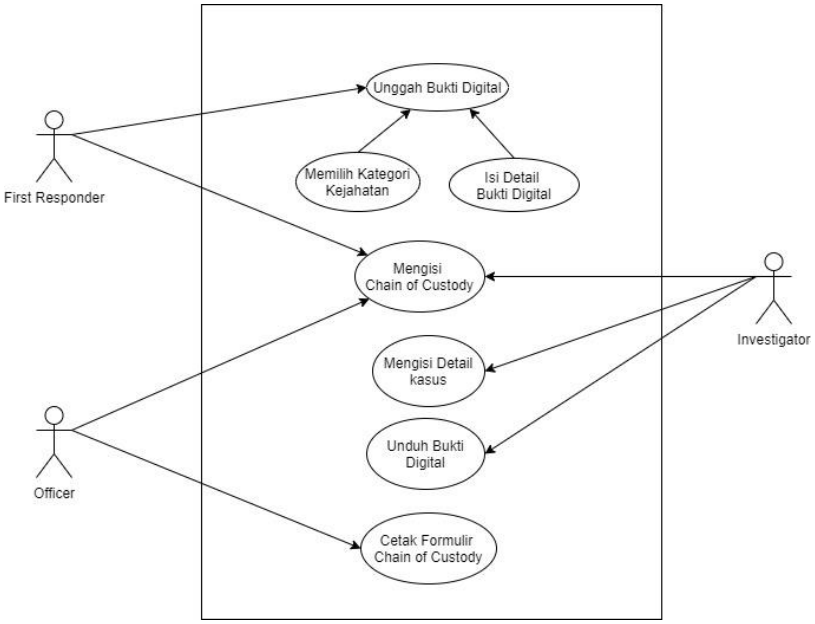
2) *Investigator*

Investigator memiliki tugas untuk melakukan investigasi bukti digital terhadap kasus yang sedang ditangani. Ia hanya diberikan akses untuk mengunduh bukti digital dari sistem pengelolaan bukti digital.

3) *Officer*

Officer memiliki peran sebagai pengatur hak akses terhadap pengelolaan bukti digital. selain itu, ia memiliki akses untuk mencetak *form chain of custody*

 DOI : https://doi.org/10.30646/sinus.v19i1.502



Gambar 1. Interaksi antara pengguna

B. *When*

Digunakan untuk merumuskan waktu terjadinya proses mengunggah, melihat, mengunduh dan mengubah bukti digital yang ditangani (chain of custody).

C. *Where*

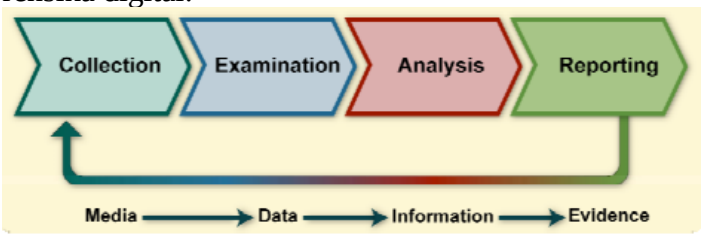
Merupakan informasi yang berisi tentang lokasi Tempat Kejadian Perkara (TKP) dimana dilakukan akuisisi bukti digital ataupun bukti elektronik.

D. *What*

Digunakan untuk menjelaskan kasus apa yang sedang ditangani.

2.2 Prosedur Penanganan Bukti 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. 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 dalam nya 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, prsedur, alat yang digunakan dan memberikan rekomendasi perbaikan kebijakan dan petunjuk dalam aspek proses forensik.

III. METODE PENELITIAN

3.1 Tempat penelitian

Penelitian dilakukan pada laboratorium digital forensik Universitas Islam Indonesia (UII) yang berada di Yogyakarta. Laboratorium tersebut digunakan untuk menganalisis bukti digital dari kasus-kasus kejahatan yang melibatkan bukti elektronik dan bukti digital. Analisis yang dilaksanakan bertujuan untuk salah satu bentuk usaha untuk pembuktian kebenaran bukti digital yang ditemukan pada tempat kejadian perkara. Di dalam laboratorium terjadi aktifitas penyimpanan bukti digital, pemerikasaan, analisis dan mencetak formulir *chain of custody.*

Tabel 1 Jenis file bukti digital

Jenis File	Ekstensi	Keterangan
Image	DD, E01, 001, ad1, raw	Hasil imaging dengan tool forensik
Multimedia	mp4, mpeg, Avi, mkv, mp3, wav, aac,	File video dan suara
Gambar	Jpg, jpeg, gif, png, bmp, tiff	File gambar
Teks	Doc, docx, xls, xlsx, ppt, pptx, rtf, txt, pdf	File office
Archive	Rar, zip, iso	

Pada laboratorium digital forensik UII telah menangani berbagai macam jenis file bukti digital. Jenis file bukti digital dapat dilihat pada tabel 1. Pada tabel tersebut disebutkan jenis file yang dikelola oleh laboratorium digital forensik UII dengan berbagai macam ekstensi. Jenis file yang dikelola adalah jenis file *image* yang merupakan hasil *imaging* dengan menggunakan tool digital forensik seperti Encase, Autopsy, FTK Imager, Oxygen, Paraben dan Belkasoft. Hal ini bertujuan untuk memudahkan investigasi dan proses pembuatan laporan. Namun tidak menutup kemungkinan untuk mengelola jenis file yang lain karena terkadang bukti digital ditemukan di sosial media, *email* dan sebuah laman tertentu yang tidak memungkinkan untuk melakukan proses *imaging.*

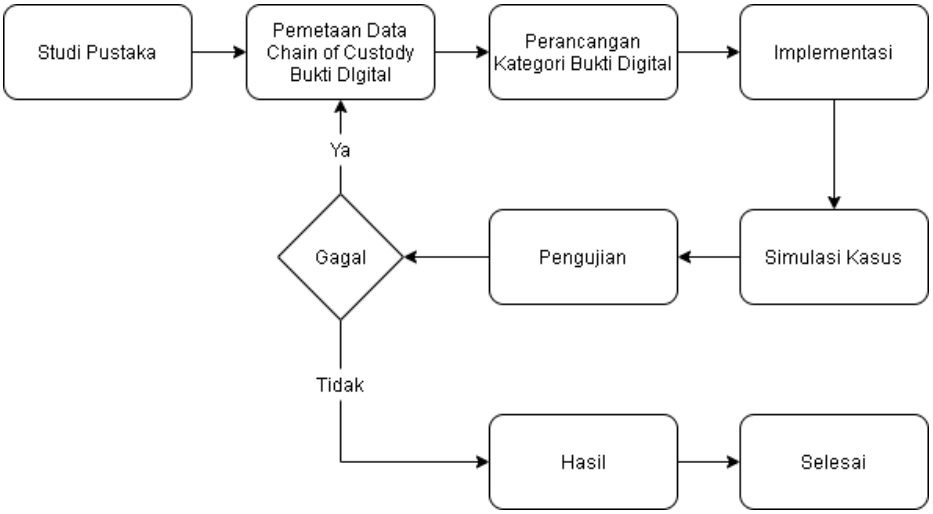
3.2 Alur Penelitian

Penelitian ini bertujuan untuk membangun sebuah sistem yang dapat menyediakan akses pengelolaan bukti digital namun tetap menjaga keaslian bukti digital yang dikelola supaya hasil keluaran dari sistem ini yang berupa formulir *chain of custody* dapat diterima dalam persidangan. Untuk menjaga keaslian perlu diterapkan sebuah fungsi hash. Fungsi hash yang digunakan adalah fungsi SHA1 dan MD5. Saat bukti digital diunggah pada sistem maka bukti digital dicek nilai hashnya dan dicatat untuk kemudian akan dibandingkan dengan fungsi hash ketika bukti digital selesai di analisis dan dibawa di persidangan sebagai barang bukti. Dengan demikian bukti digital dapat dipastikan keasliannya karena tidak ada modifikasi pada bukti digital.

Pada gambar 3 dapat dilihat alur penelitian yang dimulai dengan studi pustaka pada penelitian sebelumnya kemudian memetakan kebutuhan data *chain of custody* nya. Tahap selanjutnya adalah merancang kategori bukti digital yang sesuai dengan hukum yang berlaku di Indonesia. Kemudian dilakukan tahap implementasi terhadap rancangan yang sudah dibuat. Selanjutnya dilakukan simulasi kasus dengan bukti digital yang ada pada

 DOI : https://doi.org/10.30646/sinus.v19i1.502

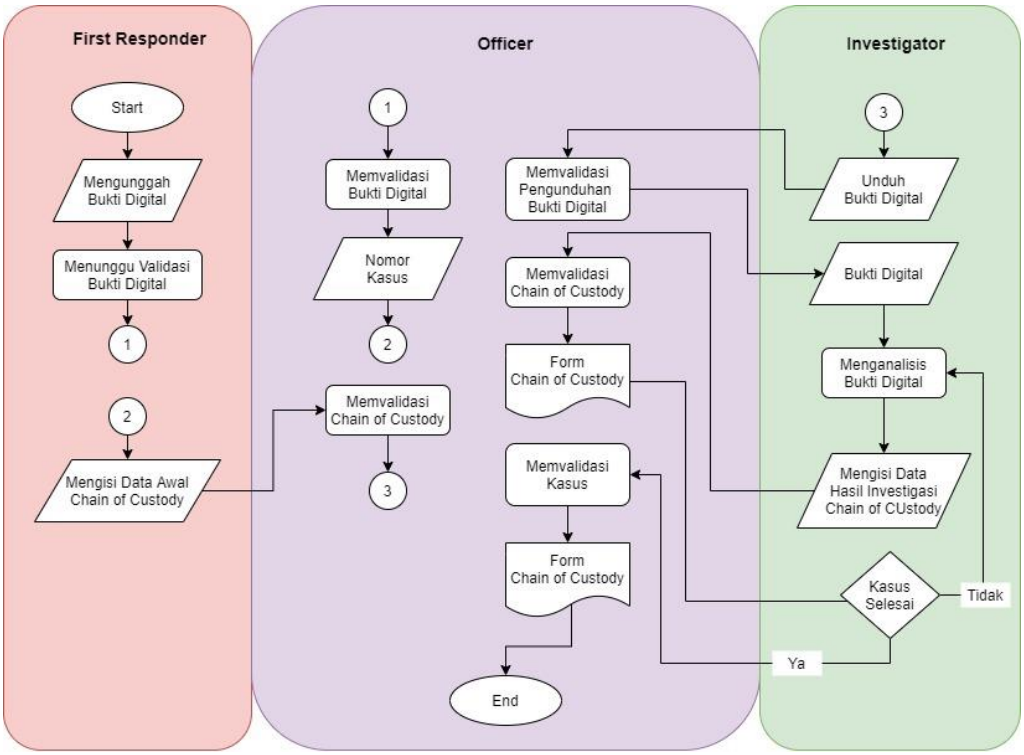
laboratorium digital forensik UII agar proses pengujian yang dilakukan benar-benar valid. Pengujian dilakukan dengan membandingkan dengan sistem yang sudah ada.



Gambar 3.Alur Penelitian

3.3 Rancangan Sistem

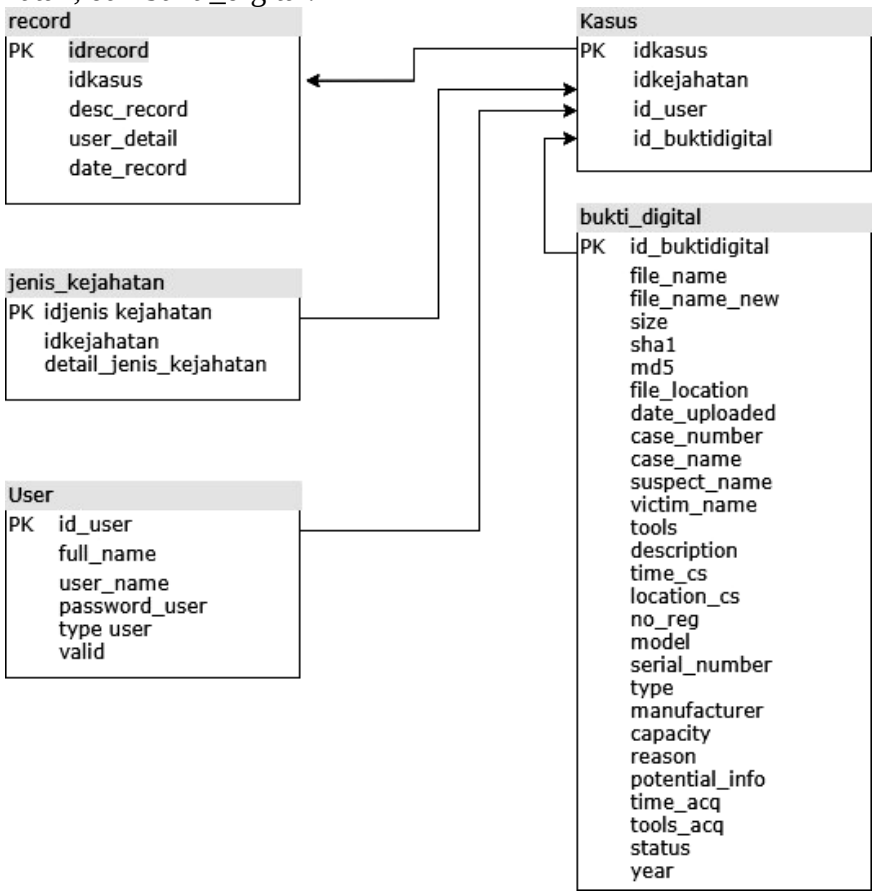
Berdasarkan konsep pengelolaan bukti digital yang telah dibuat, berikut adalah usulan model pada *chain of custody* dan penyimpanan informasi bukti digital. Bukti digital diawali dengan *first responder* mengunggah bukti digital kemudian diterima oleh *officer* yang kemudian akan diunduh oleh *investigator* untuk dianalisis dan disimpulkan hasilnya. *Officer* akan mengunduh formulir *chain of custody* yang dihasilkan oleh sistem untuk dibawa ke persidangan sebagai lampiran informasi bukti digital untuk memberikan gambaran alur penanganan bukti digital dan memberikan informasi keaslian bukti digital Gambar 4 menjelaskan tentang usulan model pada penyimpanan informasi metadata bukti digital.



Gambar 4.Alur Penanganan bukti digital

Pada tahap awal *first responder* mengunggah bukti digital kedalam sistem, kemudian setelah divalidasi oleh *officer* maka *first responder* dapat melanjutkan mengisi data awal *chain of custody* yang berupa detail bukti digital dan detail bukti elektronik, setelah data awal divalidasi maka investigator dapat mengunduh bukti digital yang sudah diunggah beserta data yang melekat pada bukti digital tersebut. *Investigator* menganalisis bukti digital dan mengisi data hasil investigasi ke dalam sistem. Setelah kasus selesai maka *officer* dapat memvalidasi kasus dan kemudian mencetak formulir *chain of custody* yang sudah lengkap. *Chain of Costudy* berisi detail bukti digital dan aktifitas dari para petugas terhadap sistem sehingga dapat digunakan pada persidangan.

Untuk memenuhi fungsi penyimpanan data bukti digital yang diunggah maka disusun sebuah *database* dengan struktur yang memiliki 5 tabel, yaitu; tabel record, kasus, user, jenis_kejahatan, dan bukti_digital.



Gambar 5. Tabel Penyimpanan Pada Server

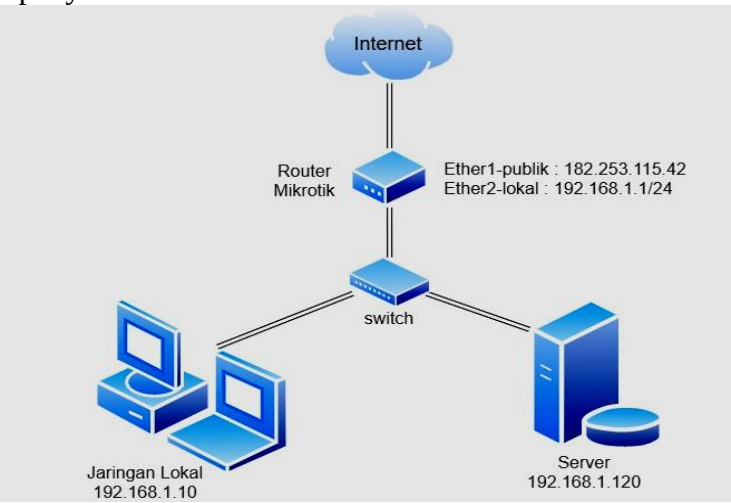
Tabel record menyimpan data *chain of custody* berupa riwayat penangan oleh petugas terhadap bukti digital yang dikelola. Tabel jenis_kejahatan menyimpan data kategori kejahatan yang telah disesuaikan dengan kategori kejahatan di Indonesia dan dapat disubah sesuai dengan kebutuhan. Tabel user berisi data petugas yang menggunakan aplikasi yang dirancang. Tabel bukti_digital berisi data detail bukti digital yang disimpan sedangkan tabel kasus menyimpan data kasus yang melibatkan bukti digital yang dikelola oleh laboratorium digital forensic UII.

Pada tahap selanjutnya adalah pembuatan kategori kejahatan yang disesuaikan dengan Kitab Undang-Undang Hukum Pidana (KUHP) yang merupakan dasar hukum pidana yang berlaku di Indonesia. Kategori tersebut dibagi menjadi tujuh kejahatan utama yaitu; Kejahatan terhadap harta benda Kejahatan terhadap jiwa seseorang, Kejahatan terhadap badan seseorang, Kejahatan terhadap kehormatan seseorang, Kejaahatan mengenai pemalsuan, Kejahatan mengenai kesusilaan dan Kejahatan terhadap negara.

 DOI : https://doi.org/10.30646/sinus.v19i1.502

Untuk meningkatkan aksesibilitas dan mengurangi kontak fisik terkait pandemi covid-19 maka sistem yang dirancang harus dapat diakses dimana saja dan kapan saja dengan membuat sistem tersebut terhubung dengan internet. Pada gambar 5 dapat diliat konfigurasi IP server dimana server terhubung pada jaringan dengan IP lokal 192.168.1.120 sedangkan untuk memenuhi kebutuhan akses yang lebih luas maka server duihubungkan dengan internet dengan IP publik 182.253.115.42 yang dapat diakses dari mana saja.

Dengan kemampuan sistem yang dapat diakses melalui internet maka kontak fisik antara para petugas dapat diminimalisir. Petugas dapat melaksanakan tugasnya masing masing dengan tetap dirumah ataupun dilapangan. Tentu saja hal ini sesuai dengan anjuran pemerintah untuk melakukan pekerjaan dari rumah atau *work from home* dengan tujuan untuk memutus rantai penyebaran covid-19.



Gambar 6. Konfigurasi IP Server

IV. HASIL DAN PEMBAHASAN

Pada penelitian ini pengujian dilakukan dengan metode *black box* dan membandingkan hasil keluaran sistem yang diusulkan dengan sistem sistem yang sudah ada sebelumnya sebagai acuan supaya sistem tetap memiliki fungsi dan peran yang sesuai dengan kebutuhan. Tahapan pengujian dapat dilihat pada table 2.

Tabel 2 Tahap Pengujian

Kelas Uji	Butir Uji	Jenis Pengujian
Sign In	Verifikasi Password	*Black Box*
Pengolahan Data Pengguna	Tambah Data Pengguna	*Black Box*
	Ubah Data Pengguna	*Black Box*
Pengolahan Data Bukti Digital (first responder)	Unggah Bukti Digital	*Black Box*
	Input Data Kelengkapan Bukti Digital	*Black Box*
Pengolahan Data Bukti Digital (officer)	Aktivasi Status Kasus	*Black Box*
	Unduh Form *Chain of Custody*	*Black Box*
Pengolahan Data Bukti Digital (investigator)	Unduh Bukti Digital	*Black Box*
	Melengkapi data kasus	*Black Box*
Pengolahan Data Kasus	Perubahan Data Statistik Dashboard	*Black Box*
Pengolahan Data Interaksi Bukti Digital	Penambahan Data Interaksi Bukti Digital	*Black Box*
Keaslian data	Membandingkan hasil fungsi hash dari sistem yang disusulkan dengan fungsi hash sistem lain	Perbandingan Hasil Fungsi Hash SHA1 dan MD5
Kelengkapan data *chain of custody*	Membandingkan kelengkapan formulir *chain of custody*	Perbandingan Kelengkapan data dengan kebutuhan

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.

Hasil pengujian

Tabel 3 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
Kesimpulan Hasil Perbandingan Nilai *Hash*	
SHA1	Sama
MD5	Sama

Pengujian nilai *hash* pada bukti digital dengan nama 19111200113UQ0F file dengan jenis mp4. Tabel 3 menunjukkan perbandingan hasil nilai *hash* antara sistem pengelolaan bukti digital dengan hasil nilai *hash* dari Autopsy dan sha1-online. Pada Pengujian nilai *hash* dengan metode SHA1 sistem yang dirancang menghasilkan nilai *hash* edffba1cfb0d90f1dc71f099526b0bcc06a929c3, kemudian file yang sama diunggah pada aplikasi Autopsy menghasilkan nilai *hash* edffba1cfb0d90f1dc71f099526b0bcc06a929c3 demikian juga dengan laman sha1-online.com menghasilkan nilai *hash* yang sama yaitu edffba1cfb0d90f1dc71f099526b0bcc06a929c3.

Kemudian penguian selanjutnya dilakukan dengan membandingkan nilai *hash* MD5 yang dihasilkan oleh system yang dirancang. Sistem yang dirancang menghasilkan nilai *hash* b5ea72348b6250de46876a2b9ad38504, file yang sama diunggah pada aplikasi autopsy menghasilkan nilai *hash* b5ea72348b6250de46876a2b9ad38504 kemudian pada laman sha1-online.com juga menghasilkan nilai *hash* yang sama yaitu b5ea72348b6250de46876a2b9ad38504. Hal ini menunjukkan bahwa sistem dapat menghasilkan fungsi *hash* yang sesuai dengan standar dan dapat diterima keabsahannya.

Pengamatan selanjutnya dilakukan dengan menguji kelengkapan data *chain of custody* pada sistem yang dirancang dengan sistem yang sudah ada. Dari hasil pengamatan yang dilakukan dapat diketahui bahwa sistem yang diusulkan memiliki kelengkapan data yang lebih banyak dari penelitian sebelumnya. Data baru yang disimpan pada sistem yang baru ialah; Kategori Kejahatan, Deskripsi *tools*, Nama *first responder*, Nama Institusi dan Nomor kasus.

 DOI : https://doi.org/10.30646/sinus.v19i1.502

CHAIN OF CUSTODY OF DIGITAL EVIDENCE

To be completed by First Responder and Investigator

Crime Scene	
Category	Kejahatan terhadap kehormatan seseorang
Suspect	Dina Rahmawati
Victim	Rian Septiawan
Location	Sleman
Time	14.00
Tools (Live Forensics)	autopsy
Tools Description	live forensics
First Responder	bagoes pakarti
Institution	UII
Tools Description	live forensics
Electronic Evidence	
Register Number	SL22155
Type	Smartphone
Model	Xiami Note 10
Manufacture	Xiaomi
Serial Number	25104866541285
Foreclosure Reasons	Alat Untuk Mengupload Status Pencemaran
Digital Evidence	
Case Number	SL20200712
File Name	07072020.E01
Time (Acquisition)	02/02/2020
Device (Acquisition)	Autopsy
Size (Byte)	66726
Hashing MD5	e8ac66df253f5904b3db8744f30b98ea
Hashing SHA1	276548b070d46fde3b3d9afc82c63e23e6cfe603
Source	C:\xampp\tmp\php50B0.tmp
Potential Information	Upload dengan aplikasi Instagram
Date Uploaded	25-07-2020 03:09
Validator	Officer

Gambar 7. Formulir *Chain of Custody*

Pada gambar 7 merupakan formulir *chain of custody* yang berisikan detail kasus yang dihasilkan oleh sistem. Pada formulir tersebut dibagi menjadi tiga bagian data, yakni *crime scene* yang berisi detail kasus kejahatan, kemudian bagian kedua merupakan *electronic evidence* yang berisi detail bukti elektronik atau perangkat yang menyimpan bukti digital dan bagian ketiga *digital* evidence yang berisi detail dari bukti digital yang dikelola. Pada form ini dapat ditemukan data Kategori Kejahatan, Deskripsi tools, Nama first responder, Nama Institusi dan Nomor kasus yang merupakan data baru pada sistem yang dibuat.

Tabel 3 Perbandingan Chain of Custody dengan Peneltian Sebelumnya

No.	Informasi	Ketersediaan Dalam *Form*			
		Sistem Baru		Penelitian Sebelumnya	
		Ada	Tidak Ada	Ada	Tidak Ada
Informasi Olah TKP					
1.	Nama kasus	✓		✓	
2.	Kategori kejahatan	✓			✓
3.	Nama tersangka	✓		✓	
4.	Nama korban	✓		✓	
5.	Lokasi	✓		✓	
6.	Waktu	✓		✓	
7.	Nama *tools* (*live forensic*)	✓		✓	
8.	Deskripsi *tools*	✓			✓
9.	Nama *first responder*	✓			✓
10.	Nama Institusi	✓			✓
	Jabatan		✓	✓	
Informasi Bukti Elektronik					
10.	Nomor registrasi	✓		✓	

No.	Informasi	Ketersediaan Dalam *Form*			
		Sistem Baru		Penelitian Sebelumnya	
		Ada	Tidak Ada	Ada	Tidak Ada
11.	Tipe	✓		✓	
12.	Nama Model	✓		✓	
13.	Nama Produsen	✓		✓	
14.	Nomor serial	✓		✓	
	Deskripsi Fisik		✓	✓	
15.	Alasan utama penyitaan	✓		✓	
Akuisisi Bukti Digital					
16.	Waktu	✓		✓	
17.	Nama *tools*	✓		✓	
18.	Tanggal	✓		✓	
19.	Nama Petugas	✓		✓	
20	Device	✓		✓	
Informasi Bukti Digital					
21.	Nomor kasus	✓			✓
22.	Nama *file*	✓		✓	
23.	Ukuran *file*	✓		✓	
23.	Nilai *hash* (SHA1)	✓		✓	
24.	Nilai *hash* (MD5)	✓		✓	
25	Nilai *hash* (SHA 256)		✓	✓	
26.	Lokasi penyimpanan	✓		✓	
27.	Lokasi penyimpanan	✓		✓	
28	Tanggal/waktu simpan	✓		✓	
	Validator	✓		✓	
29.	Informasi yang ingin didapatkan	✓		✓	
30.	Status kasus	✓		✓	

Dengan rancangan sistem yang diusulkan, petugas dapat melaksanakan tugas mereka masing-masing tanpa perlu datang ke laboratorium forensika digital UII dan melakukan kontak fisik dengan petugas yang lain sehingga dapat membatu untuk memutus rantai penyebaran covid-19.

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. Perbandingan ini dapat dilihat pada tabel 4.

Tabel 4 Perbandingan Aksesibilitas Bukti Digital

No	Aktifitas	Sistem Pengelolaan Bukti Digital	
		Penelitian sebelumnya	Sistem baru
1.	Penyerahan Bukti Digital	1. Membutuhkan waktu yang lama 2. Berisiko rusak atau hilangnya data dalam perjalanan. 3. Memungkinkan terjadinya sabotase fisik oleh pihak tertentu.	Dilakukan secara daring, meminimalisir risiko 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 perlengakapan 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 *chain of custody*	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.

 DOI : https://doi.org/10.30646/sinus.v19i1.502

Hal ini memberikan solusi atas masalah dan risiko 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.

V. 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 risiko kerusakan pada bukti digital dan keselamatan petugas.
2. Sistem yang diusulkan dapat digunakan secara bersamaan dan terpisah tanpa perlu bergantian antara pengguna satu dengan pengguna yang lain dalam satu perangkat yang sama.
3. Dengan sistem yang dapat diakses secara daring maka petugas dapat bekerja tanpa harus datang ke laboratorium forensika digital UII dan menghindari kontak antar petugas sehingga dapat membantu memutus rantai penyebaran Covid-19.

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

Cosic, J., & Baca, M. (2010). Do we have full control over integrity in digital evidence life cycle? *Proceedings of the International Conference on Information Technology Interfaces, ITI*, 429–434.

Dogan, S., & Akbal, E. (2017). Analysis of mobile phones in digital forensics. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 1241–1244. https://doi.org/10.23919/MIPRO.2017.7973613

Farmer, D., & Venema, W. (2005). *Forensic Discovery*. http://www.informit.com/store/forensic-discovery-paperback-9780321703255

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. http://paper.ijcsns.org/07_book/201101/20110101.pdf

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

Prayudi, Y., Ashari, A., & K Priyambodo, T. (2014). Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*. https://doi.org/10.5120/18781-0106

Prayudi, Y., & SN, A. (2015). Digital Chain of Custody: State of The Art. *International*

Journal of Computer Applications, *114*(5), 1–9. https://doi.org/10.5120/19971-1856

Roscini, M. (2016). Digital evidence as a means of proof before the international court of justice. *Journal of Conflict and Security Law*, *21*(3), 541–554. https://doi.org/10.1093/jcsl/krw016

Widatama, K., & Yudi Prayudi. (2017). Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML. *Seminar Nasional Informatika Dan Aplikasinya Ke-3*, *September*, 23.