First Respond Framework Untuk Forensik CCTV

Danang Mulyadipa Suratno
Program Studi Teknik Informatika
Universitas Islam Indonesia
Yogyakarta
dadangmuldip@gmail.com

Imam Riadi
Program Studi Sistem Informasi
Universitas Ahmad Dahlan
Yogyakarta
imam.riadi@is.uad.ac.id

Yudi Prayudi
Program Studi Teknik Informatika
Universitas Islam Indonesia
Yogyakarta
prayudi@uii.ac.id

***Abstrak*—Ketika petugas berwenang melakukan aktivitas investigasi forensik digital, ada hal penting yang harus diperhatikan adalah untuk menggunakan dan mengikuti proses di setiap tahapan yang ada pada framework investigasi. Saat akan mengambil bukti digital tidak hanya mengikuti mekanisme yang tepat tetapi juga harus mengikuti aturan hukum yang berlaku. Namun ternyata terdapat kejadian saat barang bukti yang dihadirkan dipersidangan ditolak pada perkara nomor: 85/PID.B/2012/PN.pwt penyebabnya karena hasil rekaman *CCTV* tidak diajukan alat bukti surat yang merupakan proses hashing yang dicetak dalam bentuk surat untuk melihat keaslian dari suatu file. Hal ini menunjukkan bahwa pihak pengadilan tidak bisa menerima begitu saja bukti yang diserahkan jika mereka tidak bisa memastikan bagaimana bukti tersebut ditangani. Oleh karena hal tersebut dilakukan penelitian untuk menghasilkan framework penanganan awal untuk forensik *CCTV* melalui identifikasi ketentuan dan proses penting dari standar yang berlaku. Pada penelitian ini menggunakan dokumen SNI 27037:2014 dan SWGIT v1.0 2013.09.27. Sehingga nantinya mampu menghasilkan bukti digital rekaman *CCTV* yang sah di persidangan.**

Kata kunci—framework investigasi, CCTV, SNI/ISO, SWGIT

I. PENDAHULUAN

Pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam aspek sistem digital, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab pada sistem digital beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli dan salinannya tidak dapat lagi dibedakan. Barang bukti elektronik dan digital bersifat *volatile* yang artinya rentan untuk berubah, rusak bahkan hilang karena kegiatan yang sengaja maupun tidak sengaja. Jika penanganan barang bukti tersebut dilakukan secara tidak prosedural maka berkemungkinan nantinya barang bukti yang tersimpan dalam barang bukti elektronik dapat berubah, rusak, bahkan hilang sehingga tidak dapat di-*recover* kembali dan tidak layak untuk dihadirkan di persidangan.

Barang bukti untuk sebuah kasus bisa berupa bentuk barang elektronik dan berupa digital. Sebuah penyelidikan yang terjadi terkadang menjadikan file data tersimpan dari peralatan elektronik sebagai alat bukti potensial[1]. Hal ini dikarenakan pada file data tersebut mengandung informasi mengenai kronologis kejadian yang bisa dijadikan bukti dalam penyelidikan untuk menjadikan file data tersebut sebagai penunjang alat bukti dalam memperoleh informasi penyelidikan suatu perkara.

Terkadang penyidik di daerah mengalami tertolak barang bukti digital yang dihadirkannya saat di hadapan sidang peradilan karena tidak bisa menunjukkan keasliannya. Maka diperlukan adanya perlakuan khusus agar terjaga keutuhan dan keaslian bukti digital karena biasanya yang dipertanyakan dari barang bukti digital tersebut adalah mengenai keasliannya. Diperlukan adanya suatu mekanisme yang harus dilakukan untuk memastikan keamanan dan privasi dan integritas dari data yang diolah sesuai standar yang berlaku[2]. Mekanisme untuk pengambilan barang bukti digital tersebut diperlukan cara yang spesifik supaya bisa dipertanggungjawabkan keasliannya.

Pada perkara nomor: 85/PID.B/2012/PN.PWT disebutkan terdapat barang bukti elektronik berupa 3 (tiga) kepingan CD rekaman *CCTV* yang tidak mempunyai kekuatan hukum yang mengikat dikarenakan tidak diajukannya alat bukti surat yang merupakan hasil proses hashing yang dicetak dalam bentuk surat untuk melihat keaslian dari suatu file. Oleh karena hal tersebut agar bisa dipertanggung-jawabkan di persidangan. Maka penting untuk menerapkan panduan penerapan aktivitas khusus dalam penanganan bukti digital potensial yang tahapan tahapannya telah diatur dalam standar yang berlaku[3].

Sebagai bagian dari metode ilmiah maka diperlukan framework yang dapat menuntun proses pembuktian yang prosedural[4][5]. Berdasarkan hal tersebut maka tujuan pada penelitian ini adalah untuk memperoleh *framework* investigasi untuk penanganan awal forensik *CCTV* yang sesuai dengan standar SNI/ISO 27037:2014 dan standar penangan yang terdapat pada SWGIT *version* 1.0 2013.09.27. Penelitian ini menghasilkan *framework* forensik investigasi yang disebut *First Respond Framework* untuk Forensik *CCTV*. Diharapkan nantinya dapat digunakan sebagai acuan dalam mempertimbangkan langkah-langkah yang dilakukan untuk memperoleh bukti digital potensial yang tidak diragukan keasliannya. Mempertahankan integritas dari bukti digital adalah hal yang penting untuk proses pemeriksaan forensik[6].

II. LANDASAN TEORI

A. Forensik Digital

Forensik digital merupakan ilmu dan metode yang digunakan dalam pelestarian, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan presentasi

barang bukti digital yang diperoleh dari sumber digital dengan tujuan untuk memfasilitasi atau membuat kemajuan dalam proses rekonstruksi kejadian kriminal, atau membantu dalam antisipasi tindakan yang mengganggu jalannya investigasi yang telah direncanakan[7]. Berdasarkan definisi tersebut dapat diketahui bahwa forensik digital berguna dalam proses investigasi suatu tindak kejahatan kriminal yang melibatkan adanya barang bukti elektronik dan digital.

Ada dua istilah barang bukti yang sering digunakan dalam forensik digital yaitu barang bukti elektronik dan barang bukti digital. Kedua istilah ini memiliki arti yang berbeda. Barang bukti elektronik yang bisa juga disebut perangkat digital lebih berupa kepada barang bukti yang berwujud secara fisik dan dapat dikenali secara visual yang berupa perangkat elektronik seperti komputer, handphone, laptop, dan lain sebagainya yang memiliki bentuk fisik sedangkan barang bukti digital merupakan data digital yang tersimpan di dalam perangkat elektronik tersebut dan baru akan muncul setelah barang bukti elektronik tersebut diakusisi dan di-*imaging*[8].

B. Investigasi Forensik Digital

Investigasi Forensika Digital atau yang lebih dikenal dengan *Digital Forensics Investigation* (DFI) adalah sebuah tindakan atau upaya penyelidikan, pengusutan, pencarian, pemeriksaan dan pengumpulan data, informasi dan temuan lainnya berdasarkan tahapan per tahapan dimana prosedur ilmiah dan teknik khusus digunakan untuk dapat menemukan barang bukti digital yang dapat diterima di pengadilan[9] .

C. Live Forensik

Pengambilan data digital yang tersimpan dalam peralatan elektronik harus bisa menyesesuaikan metode praktis yang digunakan terhadap karakteristik setiap peralatan digital, ada peralatan elektronik yang tidak perlu atau tidak bisa dimatikan dikarenakan kondisi yang tidak memungkinkan[5].

Live forensik adalah sebuah metode forensik yang digunakan ketika sistem sedang dalam keadaan menyala[10] dikarenakan untuk mengkondisikan peralatan digital elektronik tetap menyala saat diakuisisi[11].

Metode *live* forensik bertujuan untuk penanganan insiden lebih cepat, integritas data terjamin dan penggunanan kapasitas media penyimpanan yang lebih sedikit dibandingkan metode statik forensik[12].

D. SNI/ISO 27037:2014

Pada dokumen SNI/ISO 27037:2014 terdiri dari 7 klausul pembahasan secara terurut dari klausul yang pertama, yaitu: *Scope, Normative Reference, Terms and definittions, Abbreviated Terms, Overview, Key components of identification collection acquisition and preservation of digital evidence, Instance of Identification collection acquisition and preservation*. Klausul pada urutan pertama hingga ke empat membahas mengenai pengenalan tentang jenis peralatan elektronik yang bisa ditangani menggunakan isi dokumen ini acuan normative, glosarium, dan singkatan istilah. Kemudian di klausul ke lima membahas prinsip-prinsip dasar digital forensik. Klausul ke enam membahas mengenai perihal yang diperlukan saat melakukan penyelidikan. Klausul terakhir membahas spesfiik mengenai motode penanganan bukti elektronik[13].

Pada SNI/ISO 27037:2014 ini memberikan panduan untuk kegiatan khusus dalam menangani bukti digital potensial. Proses ini adalah: identifikasi, pengumpulan, akuisisi dan pelestarian bukti digital potensial. Proses ini diperlukan dalam investigasi yang dirancang untuk menjaga integritas bukti digital melalui metodologi yang dapat diterima untuk memperoleh bukti digital yang akan berkontribusi untuk tindakan hukum. Standar ini juga memberikan panduan umum untuk mengumpulkan bukti nondigital yang mungkin bisa membantu dalam tahap analisis potensi bukti digital[13].

E. SWGIT v1.0 2013.09.27

SWGIT merupakan wadah dari berbagai organisasi internasional yang didirikan pada bulan februari 1998 oleh The Federal Crime Labortory Directors Group. SWGIT secara aktif terlibat dalam bidang bukti digital dengan tujuan untuk mendorong komunikasi dan kerjasama serta menjamin kualitas dan konsistensi dalam komunitas forensik. SWGIT mengeluarkan beberapa dokumen mengenai panduan dalam penanganan barang bukti digital yang diantaranya adalah dokumen SWGIT v1.0 2013.09.27 *Retrival of Digital Video*. Pada dokumen tersebut berisi metode yang bisa digunakan untuk mengambil bukti video dari kamera pengawas *CCTV* dengan cara yang tetap bisa menjaga integritasnya. Pada dokumen ini menjelaskan jika proses pengambilan data dari alat perekam *CCTV* tidak perlu dilakukannya pemeriksaan terhadap keseluruhan sistem. Pada dokumen ini juga disampaikan bahwa tidak menjelaskan hingga kepada analisis forensik video dan audio[14].

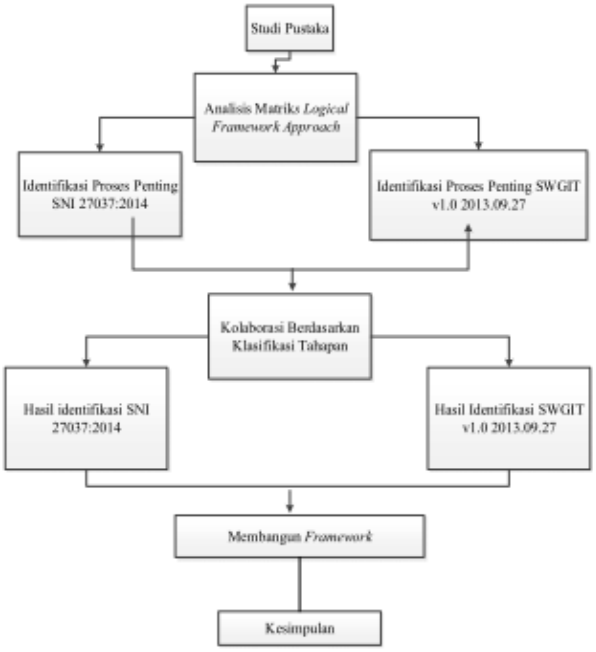
F. Logical Framework Approach

Menurut EU Integration Office[15] dalam buku yang berjudul "*Guide To The Logical Framework Approach*" menjelaskan bahwa *Logical Framework Approach* sebagai *tool* dan sebuah proses analisis yang digunakan untuk membangun hierarki kerangka logis yang sistematis dan terstruktur berorientasi pada tujuan dan digunakan untuk perencanaan, monitoring, maupun evaluasi sebuah kegiatan.

Proses pengevaluasian suatu kegiatan dengan menggunakan *Logical Framework Approach* / LFA terdiri dari beberapa tahapan yang menjadi fokus dari penerapan, antara lain memahami hubungan antara tujuan, sasaran, keluaran dan aktivitas yang disusun dalam matriks yang disebut *logframe* matriks. Matriks akan menjelaskan keterkaitan hirarki logis mulai dari masukan, aktivitas, keluaran, sasaran dan tujuan dari project. Matriks juga menerangkan setiap hierarki logis tersebut dengan indikator, alat verifikasi indikator dan asumsi yang digunakan.

III. METODE PENELITIAN

Pada bagian ini menerangkan mengenai cara penelitian dilakukan sehingga dapat diketahui apa saja tahapan pengerjaan yang dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan serta kendala yang dihadapi. Urutan langkah pemecahan masalah penelitian dapat dilihat pada Gambar 1.



Gambar 1 Metode peneltian

Ada beberapa kegiatan yang dilakukan dalam melakukan analisis menggunakan *Logical Framework Approach* ini. Diantaranya menyusun *logframe* matriks untuk perencanaan seluruh kegiatan evaluasi yang dilakukan. Kemudian nantinya akan dirinci kembali menjadi beberapa bagian matriks sehingga diperoleh alur aktivitas yang terstruktur untuk mencapai tujuan yang telah ditetapkan. Tabel 1 *logframe* matriks yang digunakan.

TABEL 1 LOGFRAME MATRIKS

Deskripsi	**Indikator**	**Verifikasi**	**Asumsi**
Tujuan *First Respond Framework* Untuk Forensik *CCTV*	*Framework* investigasi untuk forensik *CCTV*	Memenuhi kebutuhan penyelidik	Dapat diterapkan bila digunakan untuk mengambil bukti digital dari sistem *CCTV*
Sasaran *Framework* investigasi untuk forensik *CCTV*	*Framework* memenuhi ketentuan yang berlaku	Memenuhi instrument evaluasi forensik digital	Mengikuti standar yang diakui untuk digunakan dalam penyelidikan forensik digital.
Keluaran *Framework* hasil kolaborasi	*Framework* hasil perbaikan dan evaluasi	Memenuhi instrument evaluasi Memenuhi kebutuhan penyelidik	Ketika aktivitas dilakukan maka keluaran diperoleh
Aktivitas Melakukan aktivitas metode penelitian	Semua aktivitas telah dilakukan	Tidak ada	Ketika data tersedia maka aktivitas bisa dilakukan

Langkah awal untuk menerapkan *logframe* matriks dalam penelitian ini, pertama melakukan proses identifikasi proses penting dari dokumen yang digunakan sebagai dasar penelitian ini berdasarkan terminologinya. Hal ini dilakukan untuk memfasilitasi pemodelan logis yang mengklasifikasikan tahap-tahap ini berdasarkan kesamaan terminologi.

Setelah melakukan proses identifikasi terhadap dokumen yang digunakan maka tindakan yang selanjutnya dilakukan adalah melakukan kolaborasi atau penggabungan antar dokumen tersebut kedalam beberapa tahapan menurut variable output yang terbagi menjadi identifikasi, pengumpulan, akuisisi dan preservasi berdasarkan dari penjelasaan terminologi.

Berdasarkan tahapan dari dokumen SWGIT hasil identifikasi proses pentingnya terkait forensik *CCTV* akan diberikan indikator *role model* berdasarkan penjelasan pada prosesnya atau terminologi dengan mengadaptasi dari pendekatan logika agar mempermudah penyusunannya saat dilakukan kolaborasi. Bila terdapat kesamaan terminologi maka tahapan tersebut dikatakan "implies". Selanjutnya bila tahapan tersebut merupakan tahapan yang dianggap penting dan tidak ada pada dokumen SNI/ISO maka dikatakan sebagai "prohibit". Terakhir dikatakan sebagai "don't care" jika tahapan tersebut tetap berada pada tahapan semula karena tidak dapat dikolaborasikan dan tidak memiliki terminologi yang sama dengan tahapan pada dokumen SNI/ISO.

Pada proses kolaborasi sebagai indikator utama yang diikuti. Jika terdapat kesamaan kegiatan yang diterapkan tetapi memiliki perbedaan dalam penamaan maka akan dieliminasi menjadi satu. Pada tahapan ini seluruh tahapan yang awalnya telah diidentifikasi akan dikolaborasikan menjadi tahapan tahapan utama yang nanti akan digunakan untuk menyusun hierarki aktivitas tiap tahapan untuk menyusun *First Respond Framework* untuk Forensik *CCTV*.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini akan membahas mengenai hasil analisis dan evaluasi *First Respond Framework* untuk Forensik *CCTV* yang diperoleh dengan mengkolaborasikan hasil identifikasi ketentuan penting dari SNI/ISO 27037:2014 dan SWGIT v1.0 2013.09.27.

A. Ringkasan Hasil Identifikasi SNI/ISO 27037:2014

Terdapat 4 tahapan utama kegiatan penyelidikan secara berurutan yang dibahas pada klausul terakhir yaitu Identifikasi, Pengumpulan, Akuisisi dan Preservasi. Melalui penelitian menyeluruh terhadap proses identifikasi ketentuan standar berkaitan dengan forensik *CCTV* yang terdapat dalam SNI diperoleh hasil identifikasi yang ditunjukkan pada Tabel 2.

TABEL 2 HASIL IDENTIFIKASI SNI/ISO 27037:2014

Identifkasi	**Pengumpulan**	**Akuisisi**	**Preservasi**
Pengarahan	Memastikan isi	Penetuan Media Akuisisi	Verifikasi akuisisi
Persiapan dan Perencanaan	Pastikan kamera	*Live* akusisi	Segel bukti
Tindak Pencegahan di	Jadwal *overwrite*	Pemeriksaan Akuisisi	Pemeriksaan Aspek

Identifkasi	Pengumpulan	Akuisisi	Preservasi
lokasi perkara			Keamanan Pemindahan Bukti
Pencarian Bukti	Dokumentasi	Label Bukti	Pemindahan Bukti
Dokumentasi	Keterangan Verbal	Dokumentasi	Penyimpanan Bukti
Chain of Custody			Dokumen Pemindahaan

Berdasarkan dari hasil identifikasi yang dilakukan diperoleh proses penting terkait dengan forensik *CCTV* yang mana nantinya akan dijadikan acuan untuk melakukan pengembangan terhadap *framework* yang akan disusun. Proses selanjutnya adalah mengidentifikasi proses penting pada SWGIT terkait pengangkatan video digital.

B. Hasil Identifikasi SWGIT v1.0 2013.09.27

Pengklasifikasian berdasarkan variabel keluaran dilakukan untuk membantu penyusunan saat melakukan kolaborasi nantinya, karena variabel keluaran merupakan tahapan utama dari tahapan-tahapan yang diperoleh melalui identifikasi proses penting terkait pengambilan video digital sehingga ditetapkan sebagai kerangka awal penyusunan instrumen *framework*, sedangkan pengklasifikasian dengan indikator *role model* dilakukan untuk mempermudah kolaborasi pada aktivitas selanjutnya. Berikut ditampilkan hasil identifikasi SWGIT pada Tabel 3.

TABEL 3 HASIL IDENTIFIKASI SWGIT

Identifikasi	Pengumpulan	Akuisisi	Preservasi
Mengamati	Catat	Tes ambil	Audit trail
Type *CCTV*	Melihat rekaman	Output tersedia	Penyerahan bukti
Feature *CCTV*	Jadwal Maintance	Waktu tersedia	Menyimpan bukti
	Time Display	Evaluasi Output	
	Native File	Legal Output	
	Metadata	Chain of Custody	
	Bantuan Operator		
	Kontak Lokasi		
	Foto Sistem		
	Sketsa posisi kamera		

Keterangan warna

Tahapan dengan *role model Implies*
Tahapan dengan *role model Prohibit*
Tahapan dengan *role model Don't Care*

Secara penulisannya dokumen SWGIT berbeda dengan dokumen SNI yang secara jelas menyampaikan ketentuan investigasinya ke dalam 4 tahapan utama. Untuk mempermudah dalam melihat proses penting termuat maka terlebih dahulu dilakukan ekstraksi dan identifikasi proses penting terkait dengan forensik *CCTV*. Setelah melakukan ekstraksi terhadap dokumen yang digunakan maka tindakan selanjutnya yang dilakukan adalah melakukan klasifikasi tahapannya berdasarkan penjelasan terminologi. Setiap tahapan yang diperoleh dari ekstraksi akan diklasifikasikan menurut variabel keluaran yaitu identifikasi, pengumpulan, akusisi, preservasi. Kemudian pada tahapan yang telah diklasifikasi akan digolongkan berdasarkan indikator *role model.* Berdasarkan hasil dari identifikasi yang dilakukan terhadap SNI diperoleh proses penting terkait dengan forensik *CCTV* kemudian juga diterapkan *role model* pada tahapan-tahapannya agar mudah untuk melakukan kolaborasi, tahapan yang akan dikolaborasikan hanyalah tahapan dengan *role model implies* dikarenakan memiliki kesamaan terminologi.

Terdapat beberapa klausul yang tidak bisa dimasukkan menjadi tahapan investigasi dikarenakan tidak menjelaskan mengenai proses pengangkatan video digital dalam forensik *CCTV*. Berdasarkan tabel diatas terlihat terdapat tahapan dengan *role model implies* yaitu Mengamati, Catat, Melihat rekaman, Jadwal *maintance*, Evaluasi *output*, Legal *output, chain of custody*, Penyerahan bukti, Menyimpan bukti. Tahapan dengan *role model prohibit* yaitu Tipe *CCTV*, Fitur *CCTV, Time display, Native file, Metadata, Output* tersedia, *Audit trail.* Tahapan *dengan role model don't care* yaitu Bantuan Operator, Kontak lokasi, Foto sistem, Sketsa posisi kamera, Tes ambil, Waktu tersedia.

C. Hasil Kolaborasi

Dari setiap proses identifikasi yang telah dilakukan dan diklasifikasikan berdasarkan variabel *output* dan indikator *role* model maka proses selanjutnya adalah mengkolaborasikan setiap tahapan dengan indikator *role model implies* menjadi satu tahapan karena memiliki kesamaan terminologi. Pada tahapan dengan terminologi yang sama tersebut akan diberikan penamaan sesuai dengan literatur, buku maupun dokumen resmi. Pada bagian ini bukan proses eliminasi tetapi proses penggabungan.

Berdasarkan hasil identifikasi SWGIT ada beberapa tahapan dengan *role* model *implies* oleh karena itu agar tidak melakukan tahapan yang sama secara berulang maka dilakukan penggabungan dan diberikan penamaan istilah yang sesuai. Berikut proses penggabungan yang dilakukan:

1) Pengabungan tahapan Pencarian Bukti dengan tahapan Mengamati menjadi tahapan Pencarian Bukti. Kedua tahapan tersebut memiliki kesamaan terminologi yaitu memeriksa keadaan sekitar untuk memperoleh bukti digital potensial.

2) Penggabungan tahapan Dokumentasi dengan tahapan Catat menjadi tahapan Dokumentasi. Kedua tahapan tersebut memiliki terminologi yang sama yaitu mencatat temuan dan tindakan yang dilakukan.

3) Penggabungan tahapan Memastikan Isi dengan tahapan Melihat Rekaman menjadi tahapan Memastikan Isi. Memiliki terminologi yang sama yaitu mengamati konten video untuk memastikan jika peristiwa terkait perkara yang dimaksudkan terekam oleh *CCTV*.

4) Penggabungan tahapan Jadwal *Overwrite* dengan tahapan Jadwal *Maintance* menjadi tahapan Jadwal *Overwrite.*

Kedua tahapan memiliki terminologi yang sama yaitu mencari tahu kapan saat data di media penyimpanan tertimpa data baru.

5) Penggabungan tahapan Penentuan Media dengan tahapan Evaluasi *Output* menjadi tahapan Evaluasi *Output*. Memiliki kesamaan tindakaan untuk memilih media penyimpaan untuk hasil akuisisi.

6) Penggabungan tahapan Pemeriksaan Akuisisi dengan tahapan Legal *Output* menjadi tahapan Pemeriksaan Akuisisi. Memiliki terminilogi yang sama yaitu untuk memeriksa hasil akuisisi.

7) Penggabungan 2 tahapan *Chain of Custody* menjadi 1 tahapan *Chain of Custody*. Mencatat barang bukti sesuai aturan setiap instansi.

8) Penggabungan tahapan Pemindahan Barang Bukti dengan tahapan Penyerahan Bukti menjadi tahapan Pemindahan Barang Bukti. Proses pemindahan barang bukti ke tempat penyimpanan atau laboratorium.

9) Penggabungan tahapan Penyimpanan Barang Bukti dengan tahapan Menyimpan Bukti menjadi tahapan Penyimpanan Barang Bukti. memiliki kesamaan terminologi yaitu mengamankan barang bukti ditempat penyimpanan yang aman.

Berikut tabel hasil kolaborasi dari dokumen yang dijadikan landasan penelitian ini yang di runut berdasarkan hasil dari proses pengklasifikasian. ditampilkan pada Tabel 4.

TABEL 4 HASIL KOLABORASI

Identifikasi	**Pengumpulan**	**Akuisisi**	**Preservasi**
Pengarahan	Memastikan isi	Tes ambil	Verifikasi akusisi
Persiapaan dan perencanan	Memastikan kamera	Output tersedia	Memberikan segel barang bukti
Tindak pencegahan dilokasi perkara	Jadwal overwrite	Waktu tersedia	Dokumen perjalanan
Penliaian resiko	Dokumentasi	Evaluasi output	Pemindahan barang bukti
Pencarian bukti	Time display	*Live* akuisisi	Penyimpanan barang bukti
Tipe *CCTV*	Metadata	Pemeriksaan akusisi	Pemeriksaan aspek keamanan pemindahan barang bukti
Fitur *CCTV*	Native file	Label bukti	Audit trail
Dokumentasi	Keterangan verbal	Chain of Costudy	
	Sketsa posisi kamera		
	Kontak Lokasi		
	Foto Sistem		
	Bantuan Operator		

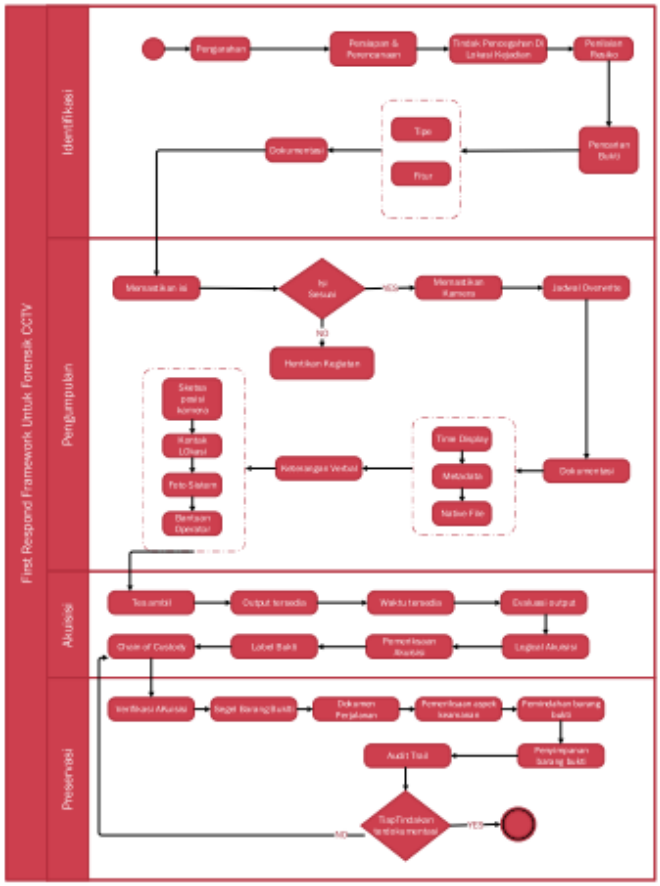
Selain tahapan berindikator *implies* juga terdapat tahapan yang bersifat *prohibit* yang memiliki istilah tahapan yang bersifat subjektif dan belum tergeneralisasi. Bila ditinjau dari sifat *role* model *prohibits* yang artinya tahapan tersebut memiliki terminologi umum dan belum dimiliki oleh *framework* lain. Tahapan tersebut dapat diasumsikan sebagai tahapan utama dalam penyusunan *framework* yang akan disusun. Menurut tabel diatas peroleh hasil kolaborasi dari identifikasi proses penting dalam SNI/ISO dan SWGIT didapatkan proses penting yang menjadi penyusun *First Respond Framework* untuk Forensik *CCTV* yang berfokus untuk mengangkat video digital dari peralatan sistem *CCTV* sesuai dengan ketentuan standar yang berlaku.

Begitu telah berhasil diperoleh hasil identifikasi dan mengkolaborasikannya, maka tahapannya selanjutnya adalah menyusunnya kedalam diagram alur sehingga dapat dengan mudah untuk dipahami alur dari setiap prosesnya.

Tahapan hasil kolaborasi yang ditampilkan pada tabel 4 telah berurut dan memiliki hirarki yang sesuai dikarenakan telah disusun berdasarkan indikator keluaran dan indikator *role mode*. Dimana indikator keluaran akan ditetapkan sebagai tahapan utama dari *framework.*

D. Membangun Framework

Pada bagian ini akan disusun hasil indentifikasi proses penting yang telah dikolaborasikan kedalam diagram alur proses sehingga bisa dengan mudah untuk dipahami dan diikuti setiap alur tahapannya. Berikut diagram alur proses *framework* penelitian ini ditampilkan pada Gambar 2.



Gambar 2 First respond *framework* untuk forensic *CCTV*

Adapun penjelasaan dari alur tahapan yang terdapat dalam diagram ini antara lain:

1) Identifikasi : Proses pencarian untuk mengenali dan mendokumentasikan bukti digital potensial. Mengidentifikasi media penyimpanan digital dan perangkat pengolahan yang mungkin mengandung bukti digital potensial yang relevan dengan peristiwa. Terdapat beberapa tahapan yaitu :

a. Pengarahan: Sesi pengarahan mengenai perkara/kejadian, lokasi, peran dan tanggung jawab. Mandat/surat perintah investigasi. Menpersiapakan rencana investigasi, alat khusus, peralatan dan manual terkait bukti digital yang menjadi fokus. Menpersiapakan rencana investigasi, alat khusus, peralatan dan manual terkait bukti digital yang menjadi fokus.
b. Pencarian bukti: Merupakan proses pencarian barang bukti di sekitar lokasi kejadian yang bisa menjadi bukti potensial.
c. *Type CCTV*: Mengetahui jenis dvr yang digunakan *stand alone* atau *pc based* dan mengetahui *serial number*.
d. *Feature CCTV*: Fitur yang terpasang pada dvr, seperti *multiplexer, transactional data, network capabilitis*.
e. Dokumentasi: Mencatat temuan yang diperoleh selama proses pencarian. Mendokumentasi dari jenis peralatan dan seting waktu yang tertera, *unique identifier*, siapa yang mengkases, siapa yang memeriksa. Mengumpulkan informasi terkait kondisi system setting peralatan *CCTV*, seperti model dan *serial number, multiplexer model, playback software name password* dan *version.*

2) *Pengumpulan:* Setelah peralatan digital yang berkemungkinan berisi bukti digital potensial teridentifikasi. Penyidik harus menentukan untuk melanjutkan atau tidak ke proses selanjutnya.

a. Memastikan isi: Memeriksa hasil rekaman untuk memastikan bahwa peristiwa terkait dalam video relevan telah terekam dan pemeriksaan diupayakan dilakukan oleh yang paham alat *recording* saat melakukan *playback*.
b. Memastikan kamera: Memastikan posisi peletakan dan kondisi kamera aktif merekam kejadian.
c. Jadwal *overwrite*: Memastikan ukuran penyimpanan video terkait pada sistem, untuk diperkirakan jadwal *overwrite*, dengan cara menentukan tanggal rekaman paling awal untuk memperkirakan waktu tersisa sebelum *overwrite*.
d. Dokumentasi: Mencatat temuan yang diperoleh dari sistem kamera pengawas *CCTV* berserta tindakan yang diambil.
e. *Time display*: Mencari tahu durasi dan waktu kejadian saat di lokasi dan yang tercatat dalam sistem.
f. *Metadata*: Mencatat metadata dari file rekaman berupa *image quality, frame size, firmware version, event log,password*, resolusi.
g. *Native file*: Mencari tahu format file yang dipergunakan oleh sistem *CCTV*.
h. Keterangan verbal: Hal ini dilakukan untuk mendapatkan petunjuk lebih melalui mencari informasi atau ketrangan saksi dilokasi kejadian terkait peristiwa yang terjadi, dan sistem *CCTV* seperti *password* admin, agar memperoleh opsi lebih untuk pengambilan video yang hanya tersedia melalui akses admin.
i. Sketsa posisi kamera: Membuat sketsa dari posisi kamera diruang lokasi kejadian.
j. Kontak lokasi: Mengumpulkan info alamat kejadian, jam operasi, kontak/telepon pemilik dan kontak intaslle r. Hal ini dimaksudkan bila tidak bisa mendapatkan player media untuk memutar video dengan *native* file.
k. Foto sistem: Foto sistem bagian depan dan belakang.

3) *Akuisisi:* Melakukan *live* akuisisi ketika perangkat menyala.Suatu proses yang membuat *copy* atau salinan dari bukti digital menggunakan metode *logical* akusisi dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan. Investigator harus mengaplikasikan metode akuisisi berdasarkan situasi dan *tools* yang tersedia.

a. Tes ambil: Melakukan tes pengambilan apakah peralatan menyediakan opsi untuk bisa mengambil *native* file beserta *playback software*.
b. Output tersedia: Memilih metode yang sesuai untuk mengambil video berdasarkan ukuran file dan durasi yang diperlukan. Serta mampu mengambil file video dalam format asli atau native serta playback software nya.
c. Waktu tersedia: Mencari tahu waktu atau durasi yang diperlukan untuk akusisi file video yang perlukan sehingga tidak memilih metode *output* yang memerlukan durasi panjang.
d. Evaluasi output: Memutuskan menggunakan metode *output* yang sesuai berdasarkan hasil tahapan *Output* tersedia dan tahapan Waktu tersedia.
e. *Live* akuisisi: Melakukan tindakan logikal akusisi menggunakan sistem pada peralatan *CCTV* dalam kondisi peralatan menyala. Karena tidak menyita dan tidak mengambil keseluruhan data.
f. Pemeriksaan akuisisi: Memeriksa hasil akuisisi, apakah konten hasil akusisi sesuai dengan keperluan.
g. Label bukti: Media penyimpanan hasil akuisisi dan ditandai sebagai *master digital evidence copy*. Kemudian membuat salinannya.
h. *Chain of custody*: Mencatat kedalam dokumen investigasi terkait kronologi dari penangan untuk pengangkatan barang bukti. Disertakan pula dengan berita acara pengambilan barang bukti.

4) *Preservasi:* Bukti digital potensial harus dalam kondisi preservasi atau dipelihara untuk memastikan kegunaannya dalam investigasi. Oleh karena itu menjadi hal yang penting untuk menjaga integrititas atau keutuhan dari barang bukti, dengan mampu menunjukan jika bukti tersebut tidak dimodifikasi sejak diperoleh.

a. Verifikasi akuisisi: Menggunakan fungsi verifikasi sebagai segel keaslian pada master evidence seperti

digital signature berupa nilai *hash* dari algoritma md5. Untuk mengaplikasikan prinsip preservasi yang menjamin kerahasian, keutuhan dan ketersedian.

b. Memberikan segel barang bukti: Barang bukti yang telah dikemas, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.

c. Dokumen perjalanan: Menyiapkan dokumen atau surat perjalan untuk perpindahan bukti digital dari penyidik ke laboratorium atau ruang penyimpanan. Pada *Chain of Cutody* diperbarui kegiatan yang dilakukan.

d. Pemeriksaan aspek keamanan pemindahan barang bukti: Pemeriksaan aspek keamanan dilakukan untuk memastikan barang bukti aman selama proses pemindahan barang bukti dari TKP ke tempat penyimpanan ataupun laboratorium. Pemeriksaan aspek keamanan mencakup pemeriksaan pengemasan barang bukti untuk menjaga pengemasan yang dilakukan tidak merusak barang bukti.

e. Pemindahan barang bukti: Saat proses pemindahan barang bukti, petugas harus berhati-hati dan selalu memperhatikan keamanan barang bukti. Selain itu juga harus melakukan update di *form chain of custody*.

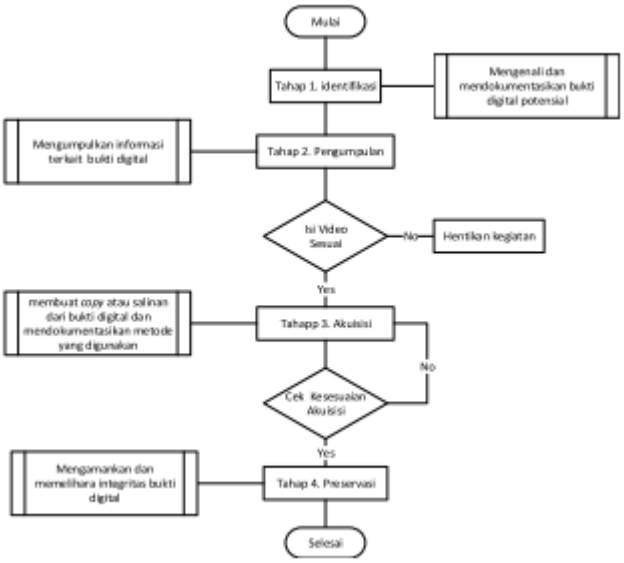
f. Penyimpanan barang bukti: Barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang baik. Sebagai contoh harus memiliki fasilitas untuk menjaga suhu ruangan penyimpanan tidak terlalu panas atau tidak terlalu dingin sehingga dapat menyebabkan kerusakan barang bukti.

g. *Audit trail*: Memeriksa kembali dokumen apakah telah mencatat detail tindakan yang dilakukan. Hal ini bertujuan untuk mempermudah bila adanya permintaan investigasi ulang oleh penyidik yang berbeda.

E. Ilustrasi penggunaan Framework

Pada bagian ini, untuk mempermudah dalam memahami penggunaan *framework* maka akan dijelaskan secara sederhana mengenai alur penggunaan *framework* tersebut melalui sebuah alur *flowchart* sederhana.

Melalui gambar tersebut maka dapat dilakukan penjelaskan ilustrasi pengggunaan *framework* yang telah disusun oleh peneliti secara sederhana sehingga para pengguna nanti dapat memahami maksud dari tiap tahapan yang dilakukan secara terurut. Pada alur *flowchart* tersebut terdapat kotak *subprocess* bukan berati terdapat dua kegiatan yang berbeda tetapi dimaksudkan untuk membantu menjelaskan secara terperinci pada proses utama yang ada terdapat proses yang telah ditentukan sebelumnya. Berikut alur *flowchat* ditampilkan pada Gambar 3.



Gambar 3 Ilustrasi penggunaan *framework*

Langah investigasi pada *framework* ini secara berurutan dimulai dari tahap 1 hingga tahap 4. Berikut dibawah ini penjelasan *flowchart* dari gambar 3.

Tahap 1. Idenifikasi: Proses awal penyelidikan untuk mengenali dan mendokumentasikan bukti digital potensial. Mengidentifikasi media penyimpanan digital dan perangkat pengolahan yang mungkin mengandung bukti digital potensial yang relevan dengan peristiwa.

Tahap 2. Pengumpulan: Setelah peralatan digital yang berkemungkinan berisi bukti digital potensial teridentifikasi. Penyidik menggali informasi yang terkandung didalam sistem digital *CCTV* untuk menemukan keterkaitannya dengan perkara yang terjadi, dalam hal ini penyidik memeriksa rekaman video secara visual untuk memastikan jika terdapat potongan video yang merekam keadaan sekitar ketika suatu peristiwa yang terkait penyelidikan sedang terjadi. Kemudian ditentukan untuk melanjutkan atau tidak ke proses selanjutnya.

Tahap 3. Akuisisi: Suatu proses yang membuat *copy* atau salinan dari bukti digital dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan. Penyidik harus mengaplikasikan metode akuisisi berdasarkan situasi, biaya dan waktu, dan *tools* yang tersedia.

Tahap 4. Preservasi: Bukti digital potensial harus dalam kondisi preservasi atau dipelihara untuk memastikan kegunaannya dalam investigasi. Oleh karena itu mejadi hal yang penting untuk menjaga integrititas atau keutuhan dari barang bukti, dengan mampu menunjukan jika bukti tersebut tidak dimodifikasi sejak diperoleh.

V. KESIMPULAN

Berdasarkan hasil penelitian, diperoleh kesimpulan bahwa metode teknik analisa LFA dapat diterapkan dalam menyusun sebuah *framework* forensik untuk penanganan awal forensik barang bukti sistem kamera pengawas CCTV, dengan cara mengidentifikasi, mengklasifikasi dan mengkolaborasi dokumen forensik yang berbeda dengan menggunakan

pemodelan logika berdasarkan terminologi. Hasil identifikasi tersebut maka dilakukan kolaborasi terhadap proses penting yang diperoleh sehingga dapat diperoleh sebuah *framerwork* perbaikan untuk penangan awal dilokasi kejadian perkara yang berfokus pada pengambilan video dari sistem *CCTV*. Sehingga *framework* tersebut mampu memenuhi ketentuan standar yang berlaku dalam menjaga integritas data, sehingga dapat diakui keasliannya.

REFERENSI

[1] Panende et al., "Konsep Attribute Based Access Control (Abac) Pada Lemari Penyimpanan Bukti Digital (Lpbd)," *Jurnal Teknik Informatika*, vol. 11, no. 1, pp. 85–94, 2018.

[2] Kurniawan, Endang, and I. Riadi, "Security Level Analysis Of Academic Information System Based On Standard ISO 27002 : 2013 Using SSE-CMM," *arXiv preprint arXiv:1802.03613*, vol. 16, no. 1, pp. 1–9, 2018.

[3] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan Sni 27037:2014," *JISKa Jurnal Informatika Sunan Kalijaga*, vol. 1, no. 2, 2016.

[4] N. Lizarti, B. Sugiantoro, and Y. Prayudi, "Penerapan Composite Logic Dalam Mengkolaborasikan," *JISKa Jurnal Informatika Sunan Kalijaga*, vol. 2, no. 1, pp. 26–33, 2017.

[5] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," *Seminar Nasional SENTIKA*, 2014.

[6] Wahyudi et al., "Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, no. 2, pp. 1–7, 2018.

[7] G. Palmer, "The First Digital Forensic Research Workshop," *The First Digital Forensic Research Workshop (DFRWS)*, vol. 1, pp. 15–18, 2001.

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

[9] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated Digital Forensic Process Model," *Computers & Security*, 38, pp. 103–115, 2013.

[10] M. A. Zulkifli and U. A. Dahlan, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *International Journal of Computer Applications*, vol. 180, no. 35, pp. 23–30, 2018.

[11] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 2, pp. 406–410, 2017.

[12] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, pp. 207–211, 2016.

[13] *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Badan Standarisasi Nasional, 2014.

[14] SWGIT, "Section 24 Best Practice For Retrieval of Digital Video," *Scientific Working Group on Imaging Technology (SWGIT)*, 2013. [Online]. Available: SWGIT, https://www.swgit.org/pdf/Section%2024%20Best%20Practices%20for%20the%20Retrieval%20of%20Digital%20Video?docID=141.

[15] EU Integration Office, "Guide to The Logical Framework Approach," *Intersectoral Development Assistance Coordination Network (ISDACON)*, 2011. [Online]. Available: Isdacon, http://www.evropa.gov.rs/Evropa/ShowDocument.aspx?Type=Home&Id=525.