First Respond Framework Untuk Forensik CCTV

Danang Mulyadipa Suratno

14917113

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Foresnik Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

Lembar Pengesahan Pembimbing

First Respond Framework Untuk Forensik CCTV

Danang Mulyadipa Suratno
14917113

Yogyakarta, Juni 2018

Pembimbing

Dr. Imam Riadi, M.Kom.

i

Lembar Pengesahan Penguji

First Respond Framework Untuk Forensik CCTV

Danang Mulyadipa Suratno

14917113

Yogyakarta, Agustus 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom.
Ketua

Yudi Prayudi, M.Kom.
Anggota I

Erika Ramadhani, M.Eng.
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, S.T.,M.Sc

ii

Abstrak

First Respond Framework Untuk Forensik CCTV

Bukti digital yang diakui oleh sidang peradilan diperoleh tidak hanya dengan mengikuti mekanisme yang tepat tetapi juga harus mengikuti aturan standar yang berlaku oleh karena itu penyidik yang melakukan investigasi forensik untuk sistem peralatan kamera pengawas CCTV diharapkan mampu menerapakan aturan standar yang berlaku. Berdasarkan hal tersebut dilakukan penelitian untuk menghasilkan penangan awal untuk forensik CCTV melalui identifikasi ketentuan dan proses penting dari standar yang berlaku. Pada penelitian ini menggunakan Logical Framework Approach sebagai tool untuk menganalisis kegiatan yang diperlukan untuk mengkolaborasikan dokumen SNI 27037:2014 dan SWGIT v1.0 2013.09.27 sehingga menghasilkan framework untuk forensik CCTV yang mampu menunjukan langkah kerja untuk mengambil bukti digital berupa rekaman CCTV yang sesuai dengan standar yang berlaku, untuk mengetahui kesesuaianya dengan ketentuan standar maka dilakukan evaluasi instrumen investigasi forensic untuk CCTV agar dapat memeriksa proses investigasi forensik yang disusun telah memenuhi standar yang diatur dalam ISO 27037:2014. Uji validasi kemudian dilakukan terhadap kalangan penegak hukum, praktisi dan akademisi mengenai kelayakannya. Berdasarkan hasil uji validasi yang dilakukan digunakan untuk memperbaiki framework sesuai kebutuhan penyidik untuk pengambilan bukti digital berupa rekaman CCTV. Hasil perbaikan yang diperoleh berupa First Respond Framework untuk CCTV yang telah memenuhi kebutuhan standar yang berlaku dan bila digunakan pada kasus nyata dapat diterapkan.

Kata kunci

Framework Investigasi, CCTV, SNI/ISO, SWGIT

Abstract

First Respond Framework For Forensic CCTV

Digital evidence that is recognized by the court is obtained not only by following the appropriate mechanism but also by following the applicable standard rules, therefore investigators who conduct forensic investigations for CCTV surveillance camera equipment systems are expected to be able to apply the applicable standard rules. Based on this, a research was conducted to produce an initial handling of CCTV forensics through identification of important provisions and processes of applicable standards. In this study using the Logical Framework Approach as a tool to analyze the activities needed to collaborate the SNI 27037: 2014 document and SWGIT v1.0 2013.09.27 so as to produce a framework for CCTV forensics that is able to show the work steps to take digital evidence in the form of CCTV recordings that correspond to applicable standards, in order to find out the conformity with the standard provisions, an evaluation of forensic investigation instruments for CCTV is carried out so that it can examine the forensic investigation process that has been compiled to meet the standards set out in ISO 27037: 2014. Validation tests were then carried out on law enforcement, practitioners and academics regarding their feasibility. Based on the results of the validation test, it was used to improve the framework according to the needs of investigators for taking digital evidence in the form of CCTV footage. The results of improvements obtained in the form of First Respond Framework for CCTV that have met the requirements of applicable standards and if used in real cases can be applied.

Keywords

Investigation Framework, CCTV, SNI/ISO, SWGIT

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, Agustus 2018

Danang Mulyadipa Suratno, S.Kom

Daftar Publikasi

Suratno, D. M., Riadi, I., & Prayudi, Y. (2018). First Respond Framework Untuk Forensik CCTV. *Hacking and Digital Forensics Exposed (H@dfex) 2018*, 13–20.

Publikasi yang menjadi bagian dari tesis

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Danang Mulyadipa Suratno	Mendesain eksperimen (60%) Menulis *paper* (70%)
Imam Riadi	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)
Yudi Prayudi	Melakukan analisis statistik dari data di tabel 2 dan tabel 3

Halaman Kontribusi

Ada beberapa pihak terkait yang memiliki kontribusi dalam penyelesaian penyusunan penelitian tesis ini:

1. Bapak Dr. Imam Riadi, M.Kom., selaku Pembimbing I dan Ketua Penguji yang telah memberikan arahan kepada penulis, sehingga penyusunan tesis ini dapat diselesaikan dengan baik.
2. Bapak Yudi Prayudi, S.Si., M.Kom., selaku Pembimbing II dan Anggota penguji yang telah memberikan arahan kepada penulis, sehingga penyusunan tesis ini dapat diselesaikan dengan baik.

Halaman Persembahan

Tesis ini penulis persembahkan untuk:

1. Papa dan Mama tersayang yang tak henti-hentinya mendukung baik moril maupun materil serta selalu memdoakan dan memberikan semangat sehingga dapat menyelesaikan program pascasarjana di Universitas Islam Indonesia Konsenstrasi Forensika Digital.
2. Calon istri yang penulis cintai yang telah memberikan doa dan dukungannya yang membuat penulis lebih semangat dalam menyelesaikan tesis ini.
3. Seluruh rekan-rekan magister teknik informatika angkatan X (sepuluh) dan angkatan XI (sebelas) yang membanggakan atas kerjasama dan bantuannya yang telah diberikan kepada penulis dalam penyelesaian tesis ini.
4. Seluruh rekan-rekan COLAYER yang selalu memberikan semangat dan dukungan kepada penulis dalam penyelesaian tesis ini.
5. Almamater tercinta Universitas Islam Indonesia

Kata Pengantar

Puji syukur kehadirat Allah SWT atas segala limpahan rahmat dan karunia-Nya sehingga dapat diselesaikannya tesis yang berjudul "Analisis dan Evaluasi First Respond Framework Untuk Forensik CCTV Berdasarkan SNI/ISO 27037:2014 dan SWGIT v1.0 2013.09.27 Menggunakan Logical Framework Approach".

Tesis ini diajukan sebagai bagian dalam rangka memperoleh gelar Magister pada Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia bidang keahlian Forensika Digital.

Penulis mengucapkan terima kasih yang sebesar-besarnya atas bimbingan dalam proses penyusunan laporan tesis ini kepada:

1. Bapak Dr. R. Teduh Dirgahayu, S.T., M.Sc., selaku Direktur Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
2. Bapak Dr. Imam Riadi, M. Kom., selaku Pembimbing I dalam penyususan tesis.
3. Bapak Yudi Prayudi, S.Si., M.Kom., selaku Pembimbing II dalam penyusunan tesis.
4. Papa dan Mama tersayang, yang selalu memotivasi dan memdoakan sehingga tesis ini dapat terselesaikan.
5. Serta semua pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu dan mendukung selesainya penyusunan tesis ini.

Yogyakarta, Agustus 2018

Danang Mulyadipa Suratno, S.Kom

Daftar Isi

Halaman

Daftar Tabel

Daftar Gambar

Glosarium

SNI	- Standar Nasional Indonesia
SWGIT	- Sciencetific Working Group Imaging Technology
CCTV	- Closed Circuit Television
Examiner	- Investigator
TKP	- Tempat Kejadian Perkara
DCCTV	- Digital CCTV
LFA	- Logical Framework Approach
COC	- Chain of Custody
LOGFRAME	- Logical Framework
UU ITE	- Undang Undang Informasi dan Teknologi
SOP	- Standard Operating Procedure

BAB I
Pendahuluan

1.1 Latar Belakang

Sebuah kasus kriminal yang terjadi terkadang menjadikan sebuah file rekaman video sebagai alat bukti contohnya saja kasus yang menjadikan peralatan kamera pengawas CCTV sebagai penunjang alat bukti dalam pengungkapan suatu perkara di sidang peradilan, akan tetapi diperlukan perlakuan khusus untuk memperoleh rekaman video tersebut agar terjaga keutuhan dan keasliannya karena biasanya yang diminta dari barang bukti rekaman video tersebut adalah mengenai keaslian datanya. Sebagaimana yang disampaikan oleh (Sinambela, 2016) mengenai Video CCTV forensik merupakan teknik analisis dan invesigasi untuk mengidentifikasikan/menemukan, mengumpulkan, memeriksa petunjuk dan bukti digital yang berupa video atau rekaman CCTV.

Barang bukti untuk sebuah kasus bisa berupa bentuk fisik dan berupa digital seperti kamera pengawas CCTV. Mekanisme untuk pengambilan barang bukti tersebut diperlukan cara yang spesifik supaya bisa dipertanggung jawabkan. Namun sayangnya mekanisme ini belum dibakukan sehingga banyak penyidik di daerah mengalami tertolak barang bukti yang dihadirkannya saat di hadapan sidang peradilan. Sebagai contoh pada perkara nomor: 85/PID.B/2012/PN.PWT yang dikutip dari penelitian Irman Nugraha 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*. Hal ini menunjukan bahwa pihak pengadilan tidak bisa menerima begitu saja bukti yang diserahkan jika mereka tidak bisa memastikan bagaimana bukti tersebut ditangani. Seharusnya ada solusi untuk penanganan barang bukti tersebut sehingga layak untuk dihadirkan dipersidangan.

Pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. 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 bukti digital potensial yang tersimpan dalam peralatan elektronik digital dapat berubah, rusak, bahkan hilang sehingga tidak dapat di-*recover* kembali dan tidak layak untuk dihadirkan dipersidangan.

Berdasarkan hal tersebut agar bisa dipertanggung-jawabkan di persidangan, maka penting untuk menerapkan *standard operating procedure* yang tahapan – tahapannya telah diatur dalam standar yang berlaku. Lembaga peneliti internasional seperti *Scientific Working Groupon Imaging Technology* (SWGIT, 2013) yang bergerak untuk bidang forensik digital telah membuat dokumen mengenai pedoman praktis penanganan terbaik untuk pengambilan bukti video dari sistem perekaman *Digital Closed Circuit Television* (DCCTV). Pada penelitian sebelumnya yang dilakukan oleh (Sudyana, Sugiantoro, & Luthfi, 2016) yang membuat instrument evaluasi *framework* investigasi forensik digital berdasarkan SNI 27037:2014 Teknologi informasi – Teknik keamanan – Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital. Namun bagaimana penerpananya untuk penyelidikan barang bukti berupa kamera pengawas CCTV.

Dibutuhkan sebuah prosedur penangan peralatan sistem kamera pengawas Digital CCTV yang memuat tahapan untuk mengeluarkan barang bukti yang mampu menjadi alat bukti yang sah dipersidangan. Membangun SOP yang mampu memenuhi aturan yang telah ditetapkan pada UU ITE, sehingga barang bukti yang diangkat dari sistem kamera pengawas CCTV yang berada di TKP bisa menjadi alat bukti yang tidak diragukan intergritasnya di sidang peradilan

Menurut permasalahan yang dibahas diatas maka diperlukan adanya penelitian untuk membangun sebuah *framework* untuk forensik CCTV dengan berpatokan kepada ketentuan-ketentuan dan proses penting yang terdapat dalam standar yang berlaku, dimana pada pada penelitian ini menggunakan model *Logical Framework Approach* sebagai alat untuk menganalisis rangkaian proses identifikasi dan susunan tahapannya. *Logical framework matrix* digunakan untuk menampilkan hasil analisis. Menggunakan model tersebut maka nantinya memungkinkan untuk mengekstraksi dan menghubungkan runtutan tahapan berdasarkan terminologi yang ada pada setiap dokumen sehingga memudahkan untuk dikolaborasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas, dapat diambil rumusan masalah antara lain:

a. Bagaimana penerapan konsep *Logical Framework Approach* untuk membuat perencanaan kegiatan penelitian guna menghasilkan *framework* untuk forensik CCTV.

b. Bagaimana mengkolaborasikan tahapan hasil identifikasi proses penting dari dokumen SWGIT dan SNI guna menyusun *First Respond Framework* untuk forensik CCTV.
c. Bagaimana perbaikan yang dapat dilakukan terhadap *First Respond Framework* untuk forensik CCTV tersebut.

1.3 Batasan Masalah

Beberapa batasan masalah yang ditetapkan di dalam penelitian ini agar pembahsannya tidak semakin luas adalah sebagi berikut:

a. Bahan kajian penelitian yang digunakan pada penelitian ini menggunakan dokumen pedoman *Scientific Working Group Imaging Technology* (SWGIT) *1.0 2013.09.27* terkait *Retrieval of Video Data Evidence from Digital Closed Circuit Television* (DCCTV).
b. Menggunakan SNI/ISO 27037:2014 sebagai standar forensik CCTV untuk mengikuti standar yang berlaku.
c. Pengujian dilakukan melalui wawancara kepada praktisi.

1.4 Tujuan Penelitian

Berdasarkan rumusan yang dibuat maka dapat diambil tujuan dari penelitian ini. Tujuan dari dibuatnya penelitian ini antara lain:

a. Mengetahui bagaimana perencanaan dan evaluasi yang dilakukan menggunakan *Logical Framework Approach* untuk kegiatan penelitian guna menghasilkan framework untuk forensik CCTV.
b. Mengetahui tahapan kolaborasi yang dilakukan terhadap hasil identifikasi dari dokumen SWGIT dan SNI guna menyusun *First Respond Framework* untuk forensik CCTV.
c. Melakukan perbaikan *First Respond Framework* untuk forensik CCTV tersebut.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

a. Memperluas wawasan berpikir penulis dan memberikan sumbangan pemikiran bagi perkembangan ilmu forensik digital.
b. Hasil penilitian ini diharapkan dapat menjadi bahan referensi dan acuan bagi pihak-pihak yang membutuhkan mengenai prosedur penanganan barang bukti sistem kamera pengawas *Digital* CCTV.

c. Hasil penelitian ini diharapkan bisa menjadi pedoman bagi mahasiswa UII yang ingin mempelajari *framework* investigasi foresik untuk peralatan CCTV.

1.6 *Review* Penelitian

Banyak proses model investigasi forensik yang telah dikembangkan sebagai framework investigasi forensik yang berfokus pada peralatan elektronik digital,tetapi tidak banyak yang membahas tahapan investigasi dari framework tersebut yang tahapan forensiknya memfokuskan terhadap *legal evidence* dan menghasilkan bukti digital yang sesuai ketentuan standar yang berlaku atau aturan hukum yang ada. Penelitian sebelumnya yang membahas hal tersebut adalah Domain Specific Cyber Forensic Investigation Process Mode yang dilakukan oleh (Satti & Jafari, 2015) menyatakan bahwa Framework Investigasi forensik digital harus mengikuti ketentuan hukum untuk menyediakan lingkungan komputasi yang etis, aman dan terpantau. Melakukan pengembangan *framework* investigasi forensik dengan berdasarkan dari 9 *framework* terdahulu yang berasal dari tahun 2002 hingga 2011 mengenai *digital investigation*, dan selanjutnya menerapkan metode *comparative analysis* sebagai upaya untuk menghasilkan konsep *Framework Domain Specific Cyber Forensic Investigation Process Model.* Model yang di usulkan tersebut memiliki 10 tahapan investigasi yang bisa melakukan investigasi *cybercrime* di lingkungan universitas. *Framework* tersebut dibuat untuk sebagai langkah awal untuk membangun kebijakan dan alur proses investigasi forensik untuk domain tertentu di lingkup universitas yang beroperasi dalam naungan hukum yudisial, pemerintah, aturan universitas sehingga proses investigasi *cyber* dapat berjalan secara legal karena mengikuti pembatasan dan larangan yang diberlakukan.

(Alshaikh & Sedky, 2015) yang melakukan penelitian terhadap tren perkembangan peralatan teknologi yang berpotensi sebagai alat untuk merekam video. Berdasarkan hal tersebut kemudian mengembangkan sebuah *framework* baru untuk menangangi bukti elektronik yang bisa menjaga integritas dari data didalamnya saat akan diakusisi sehingga layak untuk dihadirkan dipersidangan. Penelitian dilakukan dengan studi literatur terhadap *computer evidence* untuk mengangkat *digital video* dari bukti elektronik dengan tetap menjaga integritasnya. Perbedaan penelitian ini dengan yang akan dilakukan yaitu penelitian ini menggunakan dokumen DFRWS saja sebagai dasar untuk mengembangkan. sedangkan dalam penelitian yang dilakukan menggunakan dokumen dari SWGIT dan Dokumen SNI 27037:2014 untuk mengembangkannya khusus untuk mengangkat bukti digital yang berasal dari bukti elektronik sistem kamera pengawas CCTV.

(Sudyana et al., 2016) yang melakukan penelitian dengan membangun konsep model penyeldikan yang disesuaikan dengan aturan hukum yang berlaku, dalam pembuatannya menggunkanan SNI 27037:2014 sebagai dasar acuan yang mengatur tahapan untuk menangani bukti digital. Tahapan tersebut di bagi menjadi 4 bagian, yaitu: Identifikasi, Pengumpulan, Akuisisi, Preservasi sehingga mengahasilkan instrumen evaluasi terhadap *framework* sebelumnya dan mengubahnya menyesuaikan terhadap ketentuan yang berlaku pada SNI 27037:2014, kemudian mengaplikasikannya ke dalam *framework* IDFP sebagai media untuk mengujinya. Perbedaan penelitian ini dengan yang akan dilakukan yaitu menggunakan instrument investigasi SNI 27037:2014 tersebut untuk mengetahui standar yang berlaku kemudian mengaplikasikannya ke dalam dokumen SWGIT sebagai dasar pengembangan sehingga didapatkan sebuah *framework* untuk menangani bukti elektronik perangkat sistem kamera pengawas CCTV dengan tahapan yang di susun secara detail sehingga tidak menimbulkan kebingungan atau salah memahami kepada penggunannya.

(Lizarti, Sugiantoro, & Prayudi, 2017) yang melakukan penelitian terkait pemgembangan *framework* untuk menangangai bukti digital berupa file multimedia berdasarkan studi literature terhadap *framework* 4 (empat) sebelumnya kemudian mengkombinasikannya menggunakan metode *composite logic* sehingga menghasilkan suatu *framework* baru yang merupakan kombinasi dari kesemuanya. Membagi tahapan berdasarkan kesamaan prosesnya dan kemudian membangun *framework* baru dengan mengkombinasikan tahapannya berdasarkan terminologi dari proses penting yang dilakukan menggunakan *composite logic* untuk menganalisis proses penting dari setiap tahapan *framework.* Perbedaan penelitian ini dengan penelitian yang dilakukan yaitu penelitian ini memfokuskan hanya menangani bukti elektronik berupa sistem kamera pengawas CCTV.

(Riadi, Eko, Ashari, & -, 2013) Isu mendasar tentang pengembangan perangkat lunak yang mendukung jaringan forensik adalah bagaimana menentukan metode yang tepat memudahkan pengolahan data *log* menjadi data yang mudah diproses. Keberhasilan suatu sistem informasi yang diukur berdasarkan maksud pembuatanya tergantung pada tiga faktor utama, yaitu: keserasian dan mutu data, pengorganisasian data, serta tatacara penggunaanya untuk memenuhi permintaan penggunaan tertentu, maka struktur dan cara kerja sistem informasi berbeda-beda bergantung pada macam keperluan atau macam permintaan yang harus dipenuhi.

(Hermaduanti & Riadi, 2016) membahas mengenai kendala lain yang ditemukan adalah kerusakan peralatan sistem informasi yang dapat menyebabkan hilangnya data perusahaan dan sistem yang sering hang. Di samping itu, terjadi gangguan-gangguan yang

menyebabkan kekacauan antara lain kerusakan data, file-file yang tidak bisa dibuka, dan lain-lain. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi bagaimana penyusup dapat masuk kedalam sistem melalui jaringan yang tersedia.

(Endang; Kurniawan & Riadi, 2018) mengenai penetration test atau disebut sebagai pentes menelti mengenai tingkat keamanan dari sistem informasi suatu organisasi mengunakan dokumen ISO 27002 *information security system audit* sebagai kalausul/tahapan yang harus dilakukan untuk memberikan hasil analisis yang bisa menjadi rekomendasi peningatan sistem keamanan informasi. Di dalam penelitiannya menetapkan 13 objek control dan 43 securrity control yang harus dipenuhi berdasarkan tahapan/klausul yang ditetapkan oleh ISO 27002 *information security system audit.* Metode yang digunakan adalah *System Security Engineering* sebagai teknik pengemanannya dan *Capabilaty Maturity Model* (SSE-CMM) sebagai *framework* yang digunakan untuk mengembangkan proses yang berupa formal maupun informal. Sehingga metode tersebut menghasilkan dua bagian mengenai kemanan proses dan penilaian proses kematangan.

Tabel 1. 1 Literature Review

Paper Utama	Domain Penelitian	Metode		Uraian Singkat
		Comparative Analysis	Logical Framework Approach	
(Satti & Jafari, 2015)	Framework Investigasi forensik digital dengan mengikuti ketentuan hukum untuk menyediakan lingkungan komputasi yang etis, aman dan terpantau.	✓	-	Menganalisis 9 jenis *framework* dari tahun 2002 sampai 2011 dan menjadikannya sebagai landasan untuk mengembangkan *framework* investigasi baru untuk lingkungan universitas.
(Alshaikh & Sedky, 2015)	Framework Investigasi forensik digital untuk alat rekam video digital	-	-	Penelitian ini melakukan studi pustaka mengenai *computer evidence* untuk mengangkat *digital video* dari bukti elekteronik dengan tetap menjaga integritas nya
(Sudyana et al., 2016)	Instrumen Evaluasi Investigasi forensik digital untuk Digital Evidence First Responder berdasarkan ISO 27037:2014	-	✓	Penelitian ini melakukan studi pustaka untuk menganalisis 3 jenis *framework* dari forensik digital untuk sebagai dasar pengembangannya dengan mengvaluasi tahapannya menyesuaikan aturan SNI 27037:2014 dan menggunakan model *logical framework approach* sebagai pendekatan perencanaan.
(Lizarti et al., 2017)	Framework investigasi forensik yang terintegrasi untuk sehingga mampu digunakan untuk kondisi tertentu	✓	-	Penelitian yang melakukan studi pustaka terhadap 4 jenis *framework* forensik digital, kemudian mengusulkan sebuah *framework* baru yang merupakan kombinasi ke 4 (empat)nya. Menyatukan tahapan yang sama dari 4 jenis framework dengan menggunakan metode composite logic dengan membagi tahapan nya menjadi Identification, Extraction, Classification, Collaboration.
(Riadi et al., 2013)	Proses model Investigasi forensik untuk peralatan digital dalam kondisi menyala. Berfokus pada	-	✓	Melakukan *live* forensik untuk memperoleh data digital relevan dengan kasus yang dihadapi.

	keserasian dan mutu data, pengorganisasian data, serta tatacara penggunaanya.			
(Endang Kurniawan & Riadi, 2018)	Mengaplikasikan standar ISO 27002 untuk forensik	-	-	Mengaplikasikan tindakan investigasi pada standar ISO 27002:2013 sebagai framework untuk memperoleh informasi terkait kerentanan informasi digital dari kerusakan.

Usulan Penelitian	First Respond Framework Digital Forensik berdasarkan SNI 27037:2014 pada peralatan Kamera Pengawas CCTV	Melakukan studi *literature* terhadap *framework* investigasi hasil penelitian sebelumnya dan dokumen SWGIT v1.0 2013.09.27 kemudian mengkolaborasikannya dengan proses penting dalam SNI 27037:2014 dan menggunakan *logical framework approach* sebagai pendekatan perencanaan pembangun *framework* baru untuk investigasi kamera pengawas CCTV yang bisa menjaga keutuhannya.	Melakukan evaluasi terhadap *framework* yang digunakan sebagai dasar untuk pengembangan dengan hasil identifikasi proses penting terkait *retrieval of digital video* menyesuaikan dengan SNI 27037:2014 dan melengkapi prosesnya denggan dokumen SWGIT. Sehingga menghasilkan sebuah *framework* yang baik untuk digunakan pada investigasi kamera pengawas CCTV.

1.7 Sistematika Penulisan

Sistematika penulisan untuk memudahkan penelitian, baik proses penelitian maupun pembuatan laporan penelitian. Dibuatlah sistematika dan runtutan proses penelitian sebagai berikut:

BAB I PENDAHULUAN.

Bab ini berisi latar belakang penelitian, Rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, *review* penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI.

Pada BAB II, akan dibahas tentang landasan-landasan teori terkait dengan forensik kamera pengawas CCTV

BAB III METODOLOGI PENELITIAN.

Pada bab ini, dibahas tentang detail metodologi penelitian. Dari langkah-langkah penelitian, model pengembangan dan langkah pengujian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini, pembahasan meliputi hasil dan pembahasan dari penyelesaian masalah yang diteliti.

BAB V KESIMPULAN DAN SARAN.

Pada Kesimpulan dan Saran ini disampaikan kesimpulan dari hasil penelitian. Selain itu, diharapkan juga saran maupun masukan terkait poin-poin yang ada pada penelitian.

Lampiran dan Daftar Pustaka. Lampiran berisi gambar-gambar ataupun table terkait penelitian dan pendukungnya. Daftar pustaka berisi referensi dan buku acuan selama melakukan penelitian.

BAB II
Tinjauan Pusaka

2.1 Forensik Digital

Forensik digital (*digital forensics*) 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 (Palmer, 2001). Definisi tersebut dapat diketahui bahwa forensika digital berguna dalam proses investigasi suatu tindak kejahatan kriminal yang melibatkan adanya barang bukti elektronik dan digital.

Digital Forensik menurut (Sinambela, 2016) adalah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemukan pada sistem komputer dan media penyimpanan digital. Digital forensik merupakan penggunaan teknik analisis dan investigasi untuk mengidentifikasi/ menemukan, mengumpulkan, memeriksa dan menyimpan bukti/informasi pada sistem komputer atau media penyimpanan digital dengan sebuah standard dan dokumentasi tertentu untuk dapat diajukan sebagai bukti hukum yang sah. Setiap aktifitas dalam kegiatan forensik ada Standard yang berupa SOP/*Guidelines* yang harus diikuti setiap *examiner* atau digital forensik *investigator* dalam melakukan setiap tahapan tugas digital forensik. Kemudian ada dokumentasi yang artinya setiap tahapan aktifitas digital forensik, *examiner/investigator* harus mendokumentasikan setiap kegiatan dan temuan temuannya. Sejak mulai menerima barang bukti, akusisi, analisa hingga pelaporan. Dokumentasi ini biasanya berisi informasi-informasi teknis yang dilakukan oleh *examiner/investigator* digital forensik, sehingga jika suatu saat harus disampaikan di pengadilan dapat dijelaskan secara runtut bagaimana proses hingga menemukan informasi digital yang dapat menjadi bukti bukti untuk menjelaskan kasus tersebut. Dokumentasi ini juga akan diperlukan jika suatu saat di sidang/pengadilan harus dilakukan pemeriksaan kembali oleh *examiner* lain (*cross-examination*), sehingga dari mempelajari dokumentasi digital forensik sebelumnya si *examiner* lain dapat mengetahui bagaimana /\bukti digital pada barang bukti tersebut sebelumnya dianalisis dan ditemukan, dengan mengikuti tahapan dan petunjuk pada dokumentasi, ahli digital forensik lainnya mendapatkan hasil yang sama, ini juga yang membuktikan bahwa digital forensik adalah ilmu *exact*/ilmu pasti. Jadi pada

prinsipnya, dokumentasi memungkinkan semua kegiatan forensik menjadi *repeatable*, artinya semua proses yang dilakukan oleh *examiner/investigator* harus dapat diulang dan menghasilkan petunjuk/hasil dan kesimpulan yang sama.

Pada ilmu forensika digital terdapat prinsip-prinsip dasar. Prinsip dasar forensika digital menurut (ACPO, 2011) antara lain :

a. Sebuah lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.
b. Untuk seseorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi, dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
c. Terdapat catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisis berlangsung. Jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama.
d. *Person in charge* dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

2.2 Barang Bukti

Ada dua istilah barang bukti yang sering digunakan dalam forensika digital. Yaitu barang bukti elektronik dan barang bukti digital. Kedua istilah ini memiliki arti yang berbeda. Menurut (Al-azhar, 2012). 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. Sebagai contoh, komputer merupakan barang bukti elektronik, setelah diakusisi dan imaging, maka hasil *imaging* tersebut merupakan bukti digital. Setelah adanya barang bukti digital, barang bukti elektronik boleh disimpan ke dalam ruangan penyimpanan barang bukti. Karena yang akan dianalisa adalah barang bukti digitalnya. Barang bukti digital diklasifikasikan menjadi sebagai berikut:

2.2.1 Barang Bukti Elektronik

Barang bukti ini bersifat fisik dan dikenali secara visual, sehingga *investigator* dan analis forensik harus sudah memahami serta mengenali masing-masing barang bukti. Jenis-jenis barang bukti elektronik sebagai berikut:

a. Komputer
b. *Smartphone*
c. Flashdisk
d. Hardisk
e. CD/DVD
f. Kamera Video, perangkat CCTV
g. Kamera digital
h. Dan peralatan digital elektronik lainnya.

2.2.1 Barang Bukti Digital

Barang bukti ini bersifat digital yang diekstrak dari barang bukti elektronik. barang bukti ini harus dicari oleh analis forensik yang kemudian akan diteliti keterkaitan masing-masing *file* dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik, berikut contoh barang bukti digital.

a. *Logical file*
b. *Deleted file*
c. *Lost file*
d. *File slack*
e. *Log file*
f. *Encrypted file*
g. *Steganography file*
h. *Office file*
i. *Audio file*
j. *Video file*
k. *Image file*
l. *Email*
m. *User ID dan password*
n. *Short message service*
o. *Call logs*

2.3 Investigasi Forensika 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 (Kohn, Eloff, & Eloff, 2013) . Selain itu (Kohn et al., 2013) juga menjelaskan bahwa prosedur dasar dalam investigasi forensika digital dimulai dari persiapan, investigasi, dan presentasi.

Setiap akhir investigasi yang dilakukan, setiap penyidik harus dapat menjawab enam pertanyaan kunci. Yaitu *what, why, how, who, where* dan *when*. *What* dapat ditentukan oleh atribut data atau metadata, *why* mengacu terkait movitasi terjadinya kejahatan, *how* terkait prosedur dan proses terjadinya kejahatan, siapa terkait pelaku yang terlibat, *who* terkait siapa saja yang terlibat, *where* mengacu pada lokasi kejadian dan *when* mengacu pada waktu kejadian (Ieong, 2006).

2.4 Video CCTV Forensik

Video (CCTV) Forensik dan Computer Forensic menurut (Sinambela, 2016) merupakan sub bidang dari digital forensik. Selain video (CCTV) forensik dan *computer forensic*, ada beberapa sub bidang digital forensik lainnya seperti *mobile forensic, hacking/cyber forensic, audio forensic, image forensic, malware forensic* dan *memory forensic*. Video (CCTV) forensik merupakan teknik analisis dan investigasi untuk mengidentifikasi/ menemukan, mengumpulkan, memeriksa petuntuk dan bukti digital yang berupa video atau rekaman CCTV. CCTV sendiri ada dua jenis, yakni digital CCTV dan analog CCTV. Secara umum teknologi CCTV terbaru sudah menggunakan digital *closed circuit television* (DCCTV) merekam ke media digital (*Storage*/HDD) dengan memanfaatkan sistem DVR (*Digital Video Recording System*), sedangkan teknologi analog adalah teknologi lama yang merekam CCTV hanya dengan Kaset VHS.

Pada video (CCTV) forensik, secara umum operator/pemilik CCTV (DVR) biasanya tidak terlibat dalam kasus atau bukan merupakan pelaku kejahatan atau tersangka pada kasus yang ditangani, sehingga tidak ada keharusan penyidik ataupun *investigator* untuk mendapatkan semua sistem dan konten video yang terekam pada CCTV/DVR, hanya video rekaman dengan parameter tertentu dan berhubungan dengan kasus (orang orang yang terlibat seperti korban/saksi-saksi atau terduga pelaku) atau pada durasi waktu kejadian yang

akan dilakukan pengambilan data/akusisi oleh pihak penyidik/*investigator*. *Investigator* tidak perlu melakukan akusisi semua sistem aplikasi dan data DVR yang dapat berakibat tidak berjalannya sistem *monitoring* CCTV saat akusisi. Pada prosedur pengambilan rekaman (*retrieve video*) atau ekstraksi DVR direkomendasikan agar proses *recording system* (merekam) tetap berjalan seperti biasa. Detail prosedur dapat dibaca pada bagian pertanyaan berikutnya. Berbeda halnya dengan *computer forensic*, dimana kegiatan *computer forensic* biasanya melibatkan perangkat milik terduga seorang pelaku kejahatan/tersangka sehingga harus menggunakan metodologi *computer forensic*, yang biasanya terdapat prosedur *imaging/bit-stream copy memory system* dan seluruh *storage* dan aplikasi yang terinstall, sehingga *investigator*/examiner dapat merekonstruksi semua sistem dan aplikasi yang digunakan si pelaku kejahatan/tersangka dengan menganalisis data-data yang sudah di *imaging/bit-stream copy* (kloning) tersebut. Dari hasil *imaging/bit-stream copy* (kloning), *investigator*/examiner dapat mencari data/informasi baik yang sudah terhapus (melalui *proses recovery*) maupun yang masih tersedia di sistem komputer yang menjadi barang bukti tersebut.

2.5 Kamera Pengawas CCTV

Closed-circuit television atau CCTV adalah perangkat yang digunakan didalam rumah dan sistem keamanan bisnis untuk *electronic surveliance*. Kamera CCTV dapat membantu mengawasi banyak tempat yang berbeda diwaktu yang bersamaan, dan peralatan tersebut juga bisa membantu menyimpan rekaman dari aktifitas atau kejadian. Pada masa kini, kapan pun terjadi suatu peristiwa, baik itu berupa sebuah kejadian atau sebuah tindak kriminal, polisi selalu meminta atau mencari rekaman CCTV yang berada disekitar lokasi kejadian yang berkemungkinan menyimpan rekaman dari kejadian secara penuh atau sebagaian (Chowdhry, n.d.).

Rekaman CCTV adalah salah satu sumber *forensic intelligence*.

a. Memberikan gambaran kejadian untuk rekonstruksi.
b. Dapat digunakan untuk investigasi dilokasi kejadian perkara.
c. Memberikan bukti tidak langsung – pakaian, tas, sejanta, dll.
d. Dapat melacak pergerakan tersangka baik sebelum dan sesudah kejadian.
e. Melacak barang yang dapat di identifikasikan seperti nomor plat kendaraan, dll.

Sebelum menggunakan rekaman CCTV sebagai bukti forensik, terlebih dahulu harus memahami seluk beluk dari kamera CCTV dan *recording system*. Terdapat berbagai kategori kamera CCTV berdasarkan kegunanannya, yaitu: Kamera *indoor* dan *outdoor,* kamera *nightvision* dan *day/night* kamera. Sedangkan untuk tipe-tipe kamera nya ada beberapa tipe, yaitu:

a. *Dome Camera*
b. *Box Camera*
c. *Infra-red Camera*
d. *Bullet Camera*
e. *Wireless Camera*
f. *Pan Tilt Zoom* (PTZ) *Camera*
g. *Hidden Camera*
h. *Ip Network Camera*

Pada peralatan rekaman pengawasnya terdapat beberapa jenis yang terbagi 4 model, yaitu:

a. Analog Type System

   Sebuah peralatan VCR yang digunakan didalam sistem CCTV bersifat *time lapse* yang memiliki fungsi untuk meningkatkan atau munurunkan kecepatan rekaman pad saat *slow rate.* Ketika menggunakan peralatan ini perlu dipahami bahwa tidak semua *frame* dari tangkapan kamera akan terekam, maksudnya adalah didalam rekaman yang dengan mode perekaman 24 jam hanya 1 gambar dari 8 gambar yang akan direkam ke dalam media penyimpanan berupa *tape*. Bila ingin melihat monitor beberapa kamera diperlukan tambahan alat *multiplexer* yang berfungsi untuk membagi layar. Seperti yang ditunjukkan pada gambar 2.1.

b. PC Based DVR

   Sebuah DVR *card built* didalam perangkat komputer. Perangkat tersebut memiliki *motherboard, network card,* vga *card,* cpu, *hard drive* dan *memory.* Serta terpasang sebuah PCI DVR *Card.* Perangkat ini mampu terpasang beberapa kamera berdasarkan dari jumlah *channel* yang tersedia umumnya berjumlah 4 *channel* hingga 32 *channel*.

c. Standalone, Surveillance DVR System

   Peralatan ini adalah yang terbaik untuk perangkat DVR. Perangkat ini adalah *computer based system* yang berjalan mengguankan Linux atau system operasi

lainnya yang didesain untuk berjalan hanya pada satu aplikasi saja. Yang mana membuat perangkat ini yang hanya bisa melakukan satu hal saja. Dikatakan yang terbaik karena mudah dioperasikan, kualitas rekaman yang lebih baik, bisa terhubung dengan *network* dan bisa dipasang beberapa *harddisk* sehingga memiliki durasi rekaman yang jauh lebih lama.

2.6 Dokumen SNI 27037:2014

Standar Nasional 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 dalam tindakan hukum. Standar Nasional ini juga memberikan panduan umum untuk mengumpulkan bukti non-digital yang mungkin bisa membantu dalam tahap analisis potensi bukti digital.

Standar Nasional ini bermaksud memberikan panduan kepada orang - orang yang bertanggung jawab atas identifikasi, pengumpulan, akuisisi dan pelestarian bukti digital potensial. Individu ini termasuk *Digital Evidence First Responders* (DEFRs), *Digital Evidence Specialist* (DESs), spesialis respon insiden dan manajer laboratorium forensik. Standar nasional ini memastikan bahwa individu yang bertanggung jawab untuk mengelola bukti digital potensial secara praktis dengan cara yang bisa diterima di seluruh dunia, dengan tujuan memfasilitasi penyelidikan yang melibatkan perangkat digital dan bukti digital secara sistematis dan tidak memihak sekaligus melestarikan integritas dan keaslian (Badan Standarisasi Nasional, 2014).

2.7 Proses Penanganan Bukti Digital pada SNI 27037:2014

Bukti digital bisa rapuh dalam penyimpanan, bisa diubah, dirusak atau dimusnahkan melalui penanganan atau pemeriksaan yang tidak semestinya. Penangan bukti digital harus kompeten untuk mengidentifikasi dan mengelola resiko dan konsekuensi dari tindakan tindakan potensial kapan berurusan dengan bukti digital. Kegagalan menangani perangkat digital dengan cara yang tepat akan membuat bukti digital potensial yang terdapat pada perangkat digital tersebut tidak dapat digunakan lagi. Dengan mematuhi prinsip dasar dan persyaratan penanganan potensi digital bukti, bukti harus dipertahankan. Khususnya dalam kasus dimana tidak dapat dihindari. Perubahan harus dilakukan, semua tindakan dan

alasan perlu didokumentasikan. Setiap proses penanganan bukti digital, yaitu identifikasi, pengumpulan, akuisisi dan pelestarian, Berikut pembahasan tahapan yang disebutkan.

2.7.1 Identifikasi

Proses identifikasi melibatkan pencarian, pengakuan dan dokumentasi potensi bukti digital Proses identifikasi harus mengidentifikasi media penyimpan digital dan perangkat pengolah yang mungkin berisi bukti digital potensial yang relevan dengan kejadian tersebut. Ini Proses juga mencakup kegiatan untuk memprioritaskan pengumpulan bukti berdasarkan volatilitasnya. Volatilitas data harus diidentifikasi untuk memastikan urutan koleksi yang benar dan proses akuisisi untuk meminimalkan kerusakan pada potensi bukti digital dan untuk memperolehnya bukti terbaik.

2.7.2 Mengumpulkan

Mengumpulkan adalah proses dalam proses penanganan bukti digital dimana perangkat itu memungkinkan mengandung bukti digital potensial yang dikeluarkan dari lokasi asalnya ke laboratorium atau lingkungan lain yang terkendali untuk kemudian diakuisisi dan dianalisis.

Perangkat yang berisi bukti digital potensial mungkin ada di salah satu dari dua keadaan, saat sistem dinyalakan atau saat sistem dimatikan. Pendekatan dan alat yang berbeda diperlukan, tergantung pada keadaan perangkat. Prosedur lokal mungkin berlaku untuk pendekatan dan alat yang digunakan untuk proses pengumpulan.

Proses ini termasuk mendokumentasikan keseluruhan pendekatan, serta kemasannya perangkat sebelum transportasi. Penting untuk mengumpulkan bahan apapun yang mungkin terkait dengan informasi digital potensial (misalnya kertas dengan kata sandi dicatat, cradles dan konektor daya untuk perangkat sistem yang disematkan). Potensi bukti digital mungkin hilang atau rusak jika perawatan yang wajar tidak diterapkan.

2.7.3 Akuisisi

Proses akuisisi melibatkan pembuatan salinan bukti digital (misalnya hard disk lengkap, partisi, file yang dipilih) dan mendokumentasikan metode yang digunakan dan aktivitas yang dilakukan. menerapkan metode akuisisi yang sesuai berdasarkan situasi, biaya dan waktu, dan dokumentasikan keputusan untuk menggunakan metode atau alat tertentu

dengan tepat Sumber asli dan salinan bukti digital harus diverifikasi dengan fungsi verifikasi yang terbukti yang dapat diterima oleh individu yang akan menggunakan bukti.

Kondisi dimana proses verifikasi tidak bisa dilakukan, misalnya ketika mengakusisi sistem yang berjalan, salinan asli berisi *bad sector*, harus menggunakan metode terbaik yang tersedia dan bisa membenarkan dan mempertahankan pemilihan metode tersebut. Jika *imaging* tidak bisa diverifikasi, maka perlu didokumentasikan dan dibenarkan.

Dikeadaan saat tidak memungkinkan atau diperbolehkan untuk membuat salinan sumber bukti, seperti saat sumbernya terlalu besar. dapat melakukan *logical aquisition*, yang hanya menargetkan tipe data tertentu, direktori atau lokasi. Namun dengan cara ini, data yang telah terhapus, data di *unallocated space*,tidak akan ikut tersalin. Selain itu, metode *logical acquisition* juga dapat digunakan ketika ada sistem yang kritikal dimana sistem tersebut tidak boleh dimatikan.

2.7.4 Preservasi

Preservasi adalah proses untuk melakukan pengamanan terhadap barang bukti digital yang potensial dan perangkat digital yang memuat barang bukti digital yang juga bisa rusak dan hal hal yang bisa barang hilang. Proses preservasi harus dimulai dan dilakukan seluruh proses barang digital, yang dimulai dari proses identifikasi perangkat digital yang memuat barang bukti digital yang potensial.

2.8 Komponen penting identifikasi, koleksi, akuisisi, preservasi bukti digital

Pada dokumen SNI 27037:2014 disebutkan mengenai *Chain of Custody* yang membahas mengenai dokumentasi yang perlu dilakukan selama proses penyelidikan. Berikut penjelasanya.

2.8.1 Chain of Custody

Chain of Custody di dalam dokumen SNI 27037:2014 yaitu sebuah dokumen yang menjelaskan detail catatan perjalanan barang bukti dan siapa saja yang bertanggung jawab terhadap bukti digital tersebut, baik itu dokumen dalam format digital maupun format lain seperti dokumen kertas. *Chain of Custody* dilakukan untuk mengetahui aktivitas dan temuan yang diperoleh selama proses investigasi forensik. Semua catatan perjalanannya harus terdokumentasi dengan baik. Misalkan barang bukti yang disimpan untuk dianalisa di labor forensik, maka harus diingat dalam dokumen *Chain of Custody* tersebut. Selain itu, dengan

Chain of Custody, maka pada saat persidangan bukti yang diajukan tidak akan ragu karena semua proses terjemah barang bukti tersebut terdokumentasi dan tidak ada unsur barang bukti telah dimanipulasi. Dokumen *Chain of Custody* harus berisikan beberapa informasi sebagai berikut:

1. Kode identifikasi yang unik untuk setiap barang bukti.
2. Siapa yang menemukan barang bukti.
3. Waktu dan lokasi ditemukannya barang bukti.
4. Siapa yang melakukan pengecekkan terhadap barang bukti proses dan waktu preservasi dilakukan.
5. Tujuannya memeriksa barang bukti dan hukum yang sedang melakukan pemeriksaan barang bukti.
6. Perubahan apa yang dilakukan terhadap barang bukti, sekaligus petugas yang bertanggung jawab karena itu dan alasannya ganti hal tersebut.

2.9 Dokumen Scietific Working Group Imaging Technology (SWGIT)

SWGIT merupakan wadah dari berbagai organisasi internasional yang didirikan pada bulan ferbuari 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 *guidline* dalam penanganan barang bukti digital yang diantaranya adalah dokumen SWGIT 1.0.2013.09.27 membahas mengenai *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 berkemungkinan akan membuat sistem seting di konfigurasi ulang dan tidak perlu dilakukannya permeriksaan terhadap keseluruhan sistem. Pada dokumen ini juga disampaikan bahwa tidak menjelaskan hingga kepada analisis forensik video dan audio. Pada ilmu forensik digital terdapat bebrapa organisasi yang salah satu nya adalah Scientific Working Group Digital Evidence (SWGDE, 2014) yang dibentuk oleh The Federal Labortory Directors dan berfokus pada *forensic digital evidence*. Pada dokumennya menyebutkan tatacara mengumpulkan barang bukti, sebagai berikut:

a. Konsultasi kepada *investigator* untk memahami detail kasus dan bukti potensial yang bisa dikumpulkan.

b. Memahami peralatan yang diperlukan untuk TKP.
c. Review otoritas yang berlaku pengumpulan barang bukti, pastikan semua kegitan dicatat. Jika perlu dapatkan juga otoritas untuk memeriksa bukti yang berada diluar jangkauan.
d. Terkadang, mungkin ada kebutuhan untuk melakukan proses forensik tradisional di media (mis., DNA dan cetakan laten). Ini adalah kasus yang tergantung dan harus didiskusikan dengan penyidik untuk menentukan kebutuhan pemrosesan tersebut dan juga urutan proses yang harus dilakukan.
e. Bila bukti dari tempat kejadian tidak dapat diambil, foto harus disalin atau dicitrakan di tempat.
f. Semua individu yang tidak terlibat dalam proses pengumpulan harus dikeluarkan dari jangkauan bukti digital.
g. Individu yang mungkin memiliki informasi yang relevan (misalnya, nama pengguna, sandi, sistem operasi dan kredensial jaringan) harus diidentifikasi dan diwawancarai.
h. Lokasi kejadian harus dicari secara sistematis dan menyeluruh. Pencari harus dapat mengenali berbagai jenis perangkat yang mungkin berisi bukti digital (misalnya, *drive* USB yang baru, dan perangkat penyimpanan nirkabel).
i. Kemungkinan teknik anti-forensik (mis., Alat perusak dan perangkat lunak pembersih) harus dipertimbangkan.

2.10 Logical Framework Approach

Menurut (EU Integration Office., 2011) dalam buku yang berjudul "Guide To The Logical framework approach" menjelaskan bahwa *logical framework approach* adalah *tool* dan sebuah proses analisis yang digunakan untuk membangun hierarki kerangka logis yang sistematis dan terstruktur berorientasi pada tujuan program dan digunakan untuk perencanaan, monitoring, maupun evaluasi sebuah program atau kegiatan.

Dalam proses pengevaluasian suatu program dengan menggunakan alat analisis *Logical framework approach* / LFA terdiri dari beberapa tahapan yang menjadi fokus dari penerapan *logical framework matrix* atau biasa disebut *logframe matrix*, antara lain memahami hubungan antara *goals, purpose, outputs* dan *activities* yang disusun dalam matrix. Matrix akan menjelaskan keterkaitan hirarki logis mulai dari input, aktifitas, *output, purpose* dan *goal* dari project. Matrik juga menerangkan hirarki logis tersebut dengan

variable indikator, alat verifikasi indikator dan asumsi yang digunakan seperti tabel dibawah ini (Sania, 2014).

Tabel 2. 1 *Matriks Logframe*

Deskripsi Kegiatan	**Indikator**	**Verifikasi Indikator**	**Asumsi**
Goal / Tujuan	Indikator yang menunjukkan kondisi tercapainya tujuan	Bukti fisik/kualitatif yang digunakan untuk mengatur indikator tujuan	Asusmsi yang digunakan dengan melihat faktor eksternal
Purpose / Sasaran	Indikator yang menunjukkan kondisi tercapainya sasaran program/proyek	Bukti fisik/kualitatif yang digunakan untuk mengatur indikator sasaran	Asusmsi yang digunakan dengan melihat faktor eksternal
Outputs / Keluaran	Indikator yang menunjukkan kondisi tercapainya keluaran program/proyek	Bukti fisik/kualitatif yang digunakan untuk mengatur indikator keluaran	Asusmsi yang digunakan dengan melihat faktor eksternal
Activites / Kegiatan	Indikator yang menunjukkan kondisi tercapainya kegiatan program/proyek	Bukti fisik/kualitatif yang digunakan untuk mengatur indicator aktifitas	Asusmsi yang digunakan dengan melihat faktor eksternal

Adapun penjelasan untuk keempat elemen dasar sebagai berikut:

a. Tujuan*/Goals*

   Dalam kerangka logis (*logframe*) adalah tingkatan dengan tujuan tertinggi, merupakan hasil akhir tetapi diluar kontrol program. Bila sasaran dicapai maka berkontribusi pada tujuan.

b. Sasaran*/Purpose*

   Merupakan Rincian/Bagian dari Goal, namun objectives atau sasaran ini selalunya diluar kontrol program. Goal dan Purpose diluar kontrol program karena kegiatan-kegiatan tidak langsung mempengaruhinya tetapi dapat dicapai dengan gabungan beberapa dari program yang satu dengan program yang lainnya. Bila keluaran dihasilkan maka sasaran dcapai.

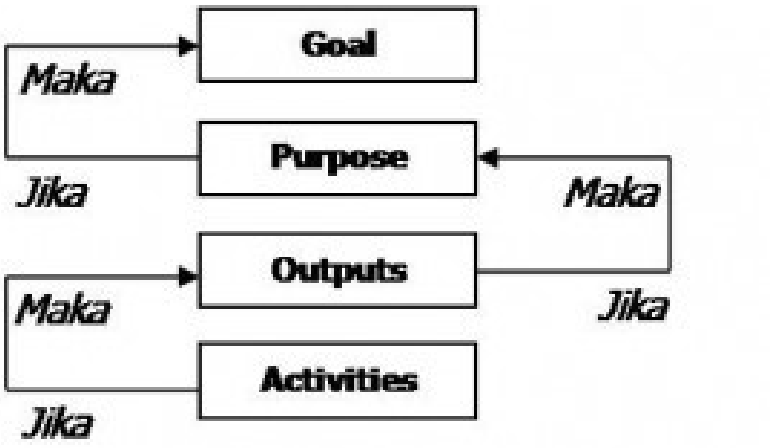
c. Keluaran*/Outputs*

   Outputs adalah hasil spesifik apa yang harus diperoleh sesudah program berakhir. Bila kegiatan dilakukan maka keluaran dihasilkan.

d. Kegiatan/*Activities*

Activities adalah kegiatan-kegiatan atau proses apa yang harus disusun untuk memperoleh outputs selama proyek/program berlangsung. Bila data atau *input* tersedia maka kegiatan bisa lakukan.

Matriks *logframe* akan menjelaskan analisis logika berpikir yang saling berkaitan antar elemennya. Ketika elemen aktivitas terpenuhi maka akan memenuhi output yang direncanakan dan begitu seterusnya, sehingga model logika berpikir dalam menjelaskan matriks *logframe* dapat dijelaskan pada Gambar 2.1 sebagai berikut:

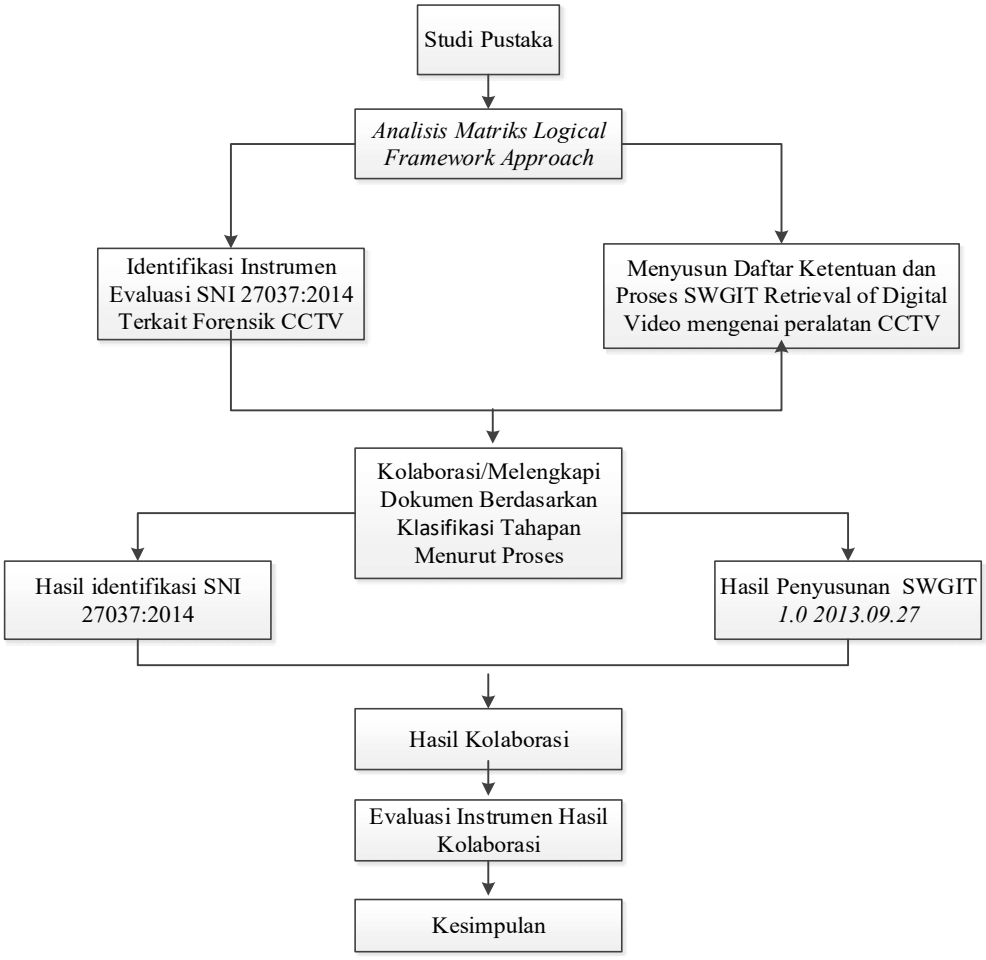


Gambar 2. 1 Model Logika Berpikir Logframe

1. Bila aktivitas dapat dilaksanakan maka output yang diharapkan dapat diharapkan dapat dicapai.
2. Bila output yang diharapkan dicapai maka sasaran program/kegiatan/proyek dapat dicapai.
3. Bila sasaran dapat dicapai maka tujuan program/kegiatan/proyek dapat dicapai.
4. Tujuan/Goal adalah target dari suatu program atau proyek yang ingin diperoleh.

BAB III
Metodologi Penelitian

Pada bab ini akan menerangkan mengenai cara penelitian dilakukan sehingga dapat diketahui apa saja tahapan pengerjaan yang dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan, membuat analisis hasil penelitian, serta kendala yang dihadapi. Berikut ini adalah langkah dari urutan tahapan pada penelitian dapat dilihat pada Gambar 3.1.



Gambar 3.1 Metodologi Penelitian

3.1. Studi Pustaka

Studi pustaka adalah tahapan yang dilakaukan untuk memelajari dan mendapatkan informasi dari topic penelitian yang bisa bersumber dari buku, dokumen, artikel, dan bentuk tertulis lainya mengenai teori ataupun penelitian sebelumnya yang bisa diperoleh dari sumber *online* maupun sumber *offline.*

Studi pustaka dilakukan terhadap penelitian yang terkait dengan topik-topik mengenai *framework* investigasi forensik digital, dokumen operasional mengenai penyelidikan barang bukti, dan teori mengenai standar forensika digital yang berlaku. Pada penelitian ini menggunakan Standar Nasional Indonesia 27037:2014 tentang pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital sehingga dapat menunjang tujuan akhir dilakukannya penelitian ini.

3.2. Analisis Matriks *Logical Framework Approach*

Pada penelitian ini untuk membantu dalam menganalisis perencanaan proses evaluasi yang akan diterapkan, maka proses yang akan dilakukan adalah menganlisis terlebih dahulu kegiatan yang akan dilakukan dan tujuannya. Pada penelitian ini menggunakan analisis *Logical Framework Approach* adalah proses dari dilakukannya analisis untuk menetapkan tujuan dan pemilihan strategi dengan menyusun matrik *Logframe* sebagai *tool* dan sebuah proses analisis yang digunakan untuk membangun urutan kerangka logis yang sistematis dan terstruktur berorientasi pada tujuan dan digunakan untuk perencanaan seluruh kegiatan yang dilakukan maupun evaluasinya.

Ada beberapa kegiatan yang dilakukan dalam melakukan analisis *Logical Framework Approach* ini. Diantaranya yaitu menyusun matrik *logframe* perencanaan seluruh kegiatan evaluasi yang dilakukan. Kemudian nantinya matrik *logframe* akan dirinci kembali menjadi beberapa bagian matrik sehingga didapat alur evaluasi yang terstruktur untuk mencapai tujuan yang telah ditetapkan.

Logical framework analisys memberikan hasil dengan menampilkan dan menganalisa lebih lanjut melalui *logframe matrix*. Matrik ini terdiri dari 4 elemen untuk membahas pokok fokus suatu *project*, elemen tersebut yaitu: tujuan (goals), sasaran (purpose), keluaran (outputs), kegiatan (activities) kemudian menjelaskan keterkaitan tiap elemen dan penjabarannya dengan indikator, verifikasi indikator, dan asumsi. Oleh karena itu matrik ini menjadi landasan untuk memahami kegiatan yang diperlukan untuk mengevaluasi *framework* sehingga menghasilkan *framework* yang dapat memenuhi

ketentuan yang yang telah disepakati didalam SNI 27037:2014 dan bisa dipergunakan berikut disampaikan bentuk matrik untuk penelitian ini melalui Tabel 3.1 dibawah ini.

Tabel 3.1 *Logframe Matrix*

Deskripsi Project	Indikator	Verifikasi Indikator	Asumsi
Tujuan/goal			
Sasaran/purpose			
Keluaran/outputs			
Kegiatan/activities			

3.3. Identifikasi Instrument Evaluasi SNI 27037:2014

Identifikasi yang diterapkan kedalam dokumen adalah suatu proses penelitian untuk memahami proses yang dipergunakan oleh dokumen SNI 27037:2014 sehingga diketahui tahapan penting apa saja yang dilakukan pada saat investigasi forensik digital. Hal ini bertujuan agar hasil identifikasi tersebut nantinya dapat diolah sebagai dasar untuk mengevaluasi *framework* yang dipergunakn sebagai dasar pengembangan *framework* sebelumnya sehingga mampu memenuhi standar aturan yang telah diatur didalamnya. Berdasarkan hal tersebut maka nantinya diharapkan mampu menghasilkan *framework* forensik CCTV yang layak dipergunakan saat dilakukkannya investigasi terhadap peralatan CCTV.

Ada 4 tahapan utama yang diatur dalam SNI 27037:2014 yaitu tahapan identifikasi, pengumpulan, akuisisi, dan preservasi. Penjelasaan tiap tahapannya beradasarkan isi dokumen yaitu: Identifikasi adalah proses yang melibatkan pencarian, pengakuan dan pendokumentasian bukti digital. Pengumpulan adalah proses mengumpulkan keterangan terkait barang fisik yang mengandung potensi bukti digital. Akuisisi adalah proses pembuatan salinan data dalam himpunan yang ditentukan. Preservasi adalah sebuah proses untuk menjaga dan mengamankan inetgritas kondisi asli dari bukti digital potensial. Kemudian dari keempat tahapan utama tersebut akan diidentifikasikan proses detail lainnya berdasarkan penjelasaan yang diberikan dalam dokumen tersebut. Kemudian seluruh hasil identifikasi dipetakan ke dalam bentuk tabel yang menampilkan detail proses dari tahapan, penejelasan proses yang dilakukan pada tahapan, kemudian menunjukan tahapan terdapat dalam bagian apa, seperti Tabel 3.2 dibawah ini.

Tabel 3.2 Identifikasi Tahapan SNI 27037:2014

No	Detail Proses	Penjelasan Proses	Terdapat dalam bagian
A	**Identifikasi**		
1	Tahapan		
2	Tahapan		
B	**Pengumpulan**		
1	Tahapan		
2	Tahapan		
C	**Akuisisi**		
1	Tahapan		
2	Tahapan		
D	**Preservasi**		
1	Tahapan		
2	Tahapan		

3.4. Menyusun Daftar Ketentuan dan Proses SWGIT

Pada bagian ini adalah untuk mengidentifikasikan tahapanan yang diterapakan oleh SWGIT, yang mana pada dokumen yang dibahas dalam peneliitian ini adalah SWGIT *Retrieval of Digital Video.* Dokumen ini membahas mengenai langkah-lagkah yang sesuai untuk mendapatkan bukti video dari sistem rekaman *Digital Closed Circuit Television* (CCTV). Pada dokumen SWGIT yang digunakan ini adalah buku petunjuk dan memberi rekomendasi dalam penanganan kasus hukum secara perorangan, bisa digunakan sebagai refensi dalam penanganan kasus hukum.

Pada dokumen ini tidak ada disebutkan secara terinci mengenai pembagian tahapannya seperti pada dokumen SNI 27037:2014, oleh karena hal tersebut maka perlu untuk memahami terlebih dahulu tahapan penting apa saja yang dilakukan sehingga bisa diolah sebagai dasar untuk mengevaluasi *framework* sebelumnya sehingga mampu mengembangkan langkah-langkah yang tepat untuk menginvestigasi peralatan CCTV. Fokus dari dokumen ini yaitu untuk memastikan *playback* sambil tetap mempertahankan bukti terbaik dari video hasil ektraksi. Pada dokumen SWGIT tahapannya akan dipetakan mengikuti matrik logik yang seperti ditunjukan pada Tabel 3.2 dimana juga menampilkan mengenai detail proses, penjelasaan proses, dan komponen tercantum yang menjelaskan

tahapan berada di bagian apa. Berikut tabel identifikasi pedoman SWGIT ditampilkan pada Tabel 3.3 dibawah ini.

Tabel 3.3 Identifikasi Pedoman SWGIT

No	Detail Proses	Penjelasan Proses
A	**Recognizing DCCTV Evidence**	
1	Tahapan	
2	Tahapan	
B	**Steps to Take Upon Scene Arival**	
1	Tahapan	
2	Tahapan	
C	**Assessing the Recording System for Output**	
1	Tahapan	
2	Tahapan	
D	**Evidence Handling Procedures**	
1	Tahapan	
2	Tahapan	

3.5. Kolaborasi Dokumen Berdasarkan Tahapan

Setiap dokumen yang telah di ekstraksi terhadap masing-masing tahapan yang diklasifikasikan menurut detail proses atau penjelasaan terminologi, jika terdapat kesamaan tindakan yang diterapkan tetapi memiliki perbedaan dalam penamaan maka akan digabungkan menjadi satu. Pada tahapan ini seluruh tahapan yang awalnya telah diidentifikasi akan dikolaborasikan menjadi tahapan-tahapan utama yang nanti akan digunakan untuk menyusun *framework.* Tabel kolaborasi ditampilkan pada Tabel 3.4

Tabel 3.4 Kolaborasi

No	Detai Proses Pada SNI 27037:2014	Terdapat pada pedoman SWGIT bagian :		
		Tahapan	Terdapat Dibagian	Penandaan
A	**Identifikasi**			
1	Tahapan			
2	Tahapan			
B	**Pengumpulan**			
1	Tahapan			
2	Tahapan			

Tabel 3. 5 Kolaborasi Lanjutan

No	Detai Proses Pada SNI 27037:2014	Terdapat pada pedoman SWGIT bagian :		
		Tahapan	Terdapat Dibagian	Penandaan
C	**Akuisisi**			
1	Tahapan			
2	Tahapan			
B	**Preservasi**			
1	Tahapan			
2	Tahapan			

3.6. Hasil Kolaborasi

Pada bagian ini tidak membangun membangun sebuah *framework* baru mulai dari awal, tetapi melakukan perbaikan dengan melengkapai kekurangan-kekurangan yang ada didalam *framework* tersebut berdasarkan dari dokumen standar investigasi yang sebelumnya dipersiapkan. Sehingga diharapkan dapat terbentuknya sebuah *framework* forensik kamera pengawas CCTV yang memenuhi kriteria SNI 27037:2014, dan nantinya dapat dipergunakan sebagai pedomaan investigasi kamera pengawas CCTV untuk semua pihak.

3.7. Evaluasi Hasil Kolaborasi

Pada tahap ini dilakukan pembahasan dan evaluasi dari instrument tahapan yang dihasilkan. Setelah framework hasil perbaikan yang berbasiskan SNI 27037:2014 selesai dibangun, tahapan berikutnya yaitu menganalisis framework hasil perbaikan ini untuk melihat apakah framework hasil perbaikan telah memenuhi kegiatan investigasi forensik untuk CCTV berdasarkan standar yang berlaku. Evaluasi dilakukan dengan cara membandingkan dengan instrument tahapan yang telah diidentifikasikan terhadap ketentuan-ketentuan dan instrument tahapan proses penting yang terdapat dalam standar yang berlaku yang telah disusun pada penelitian sebelumnya. Berikut tabel Evaluasi instrumen ditampilkan Tabel 3.6.

Tabel 3.6 Evaluasi Instrumen

Terdapat pada penelitian	Tahapan dalam instrumen pembanding
Tahapan	Tahapan Pembanding
Tahapan	Tahapan Pembanding
Tahapan	Tahapan Pembanding

3.8. Uji Kelayakan Framework

Pada tahap selanjutnya di evaluasi menurut pendapat praktisi melalui kuesioner yang bertujuan untuk mengetahui apakah *framework* hasil penelitian mampu diterapkan bila digunakan pada kasus CCTV serta juga bertujuan untuk memperoleh saran dan masukan dari praktisi. Analisis yang direncanakan adalah dengan melakukan wawancara tentang kelayakan dan penggunaan framework ini ke beberapa praktisi forensika digital untuk melihat tanggapan dan komentar mereka tentang framework baru ini. Dari hasil wawancara yang dilakukan nantinya akan dianalisis apakah framework ini dapat diterima dikalangan praktisi dan layak untuk digunakan dalam investigasi kasus-kasus forensika digital serta untuk melihat sejauh mana kekurangannya sehingga kemudian dapat dilakukan perbaikan akhir.

3.9. Ilustrasi Penggunaan Framework

Pada tahap ini akan dijelakan ilustrasi penggunaan *framework* secara sederhana unuk membantu dalam memahami penggunaan *First Respond Framework* untuk CCTV. Alur yang ditampilkan untuk ilustrasi simulasi penggunan *First Respond Framework* untuk Forensik CCTV digunakan untuk mengakuisisi perangkat kamera pengawas CCTV sehingga dapat dipahami bagaimana penggunaan *framework* tersebut.

3.10. Simulasi

Pada tahap ini akan dilakukan kegiatan simulasi penggunan *First Respond Framework* untuk Forensik CCTV digunakan untuk mengakuisisi perangkat kamera pengawas CCTV sehingga dapat dipahami bagaimana penggunaan *framework* tersebut.

3.11. Kesimpulan

Pada tahap akhir ini akan didapat kesimpulan tentang bagaimana *framework investigasi digital* yang dikembangkan mengikuti standar SNI 27037:2014 ini dapat digunakan dalam penyelesaian kasus investigasi forensik digital khusunya pada perangkat CCTV. Penggunanan standar dalam penyusuanan *framework* mampu mendukung investigasi menjadi lebih baik dan pelaksanaanya tidak lagi diragukan karena telah mengikuti standar yang berlaku.

BAB IV
Pembahasaan

Bab ini, akan membahas tentang hasil analisis yang dilakukan terhadap apa yang diperoleh, ditinjau secara kualitatif. Berdasarkan data yang diperoleh melalui studi pustaka diolah menggunakan *Logical Framework Approach* sehingga bisa memperoleh *framework* investigasi yang telah memenuhi ketentuan pada standar yang tercantum pada SNI 27037:2014 untuk forensik kamera CCTV.

Berdasarkan hasil analisis dari proses identifikasi pada penelitian ini melalui matriks kegiatan atau *logframe matrix* pada *logical framework approach* untuk mengetahui aktivitas dari setiap tahapan SNI melalui terminologinya, maka kemudian dilanjutkan dengan mengkolabarasikan hasil proses identifikasi dokumen SWGIT untuk saling melengkapi sehingga mampu digunakan untuk mempermudah memahami langkah-langkah yang diambil untuk melakukan penangan awal bukti digital khususnya peralatan CCTV. Setelah itu dilakukan evaluasi pada tahapannya berdasarkan instrument evaluasi SNI 27037:2014 yang telah disusun pada penelitian sebelumnya untuk mengetahui perbedaanya mengenai ketentuan yang tidak harus dipenuhi. Kemudian dilakukan uji perbandingan pada langkah mekanisme pengangkatan video yang ada pada tahapan pengumpulan dan akuisisi dengan standar penangan lainya yang telah dipublis oleh ACPO sebagai pembandingnya sehingga diketahui jika ada perbedaan perlakuan untuk tiap peralatan elektronik dan memberikan rujukan *framework* yang sesuai untuk forensik CCTV.

4.1 Analisis Matriks Logical Framework Approach

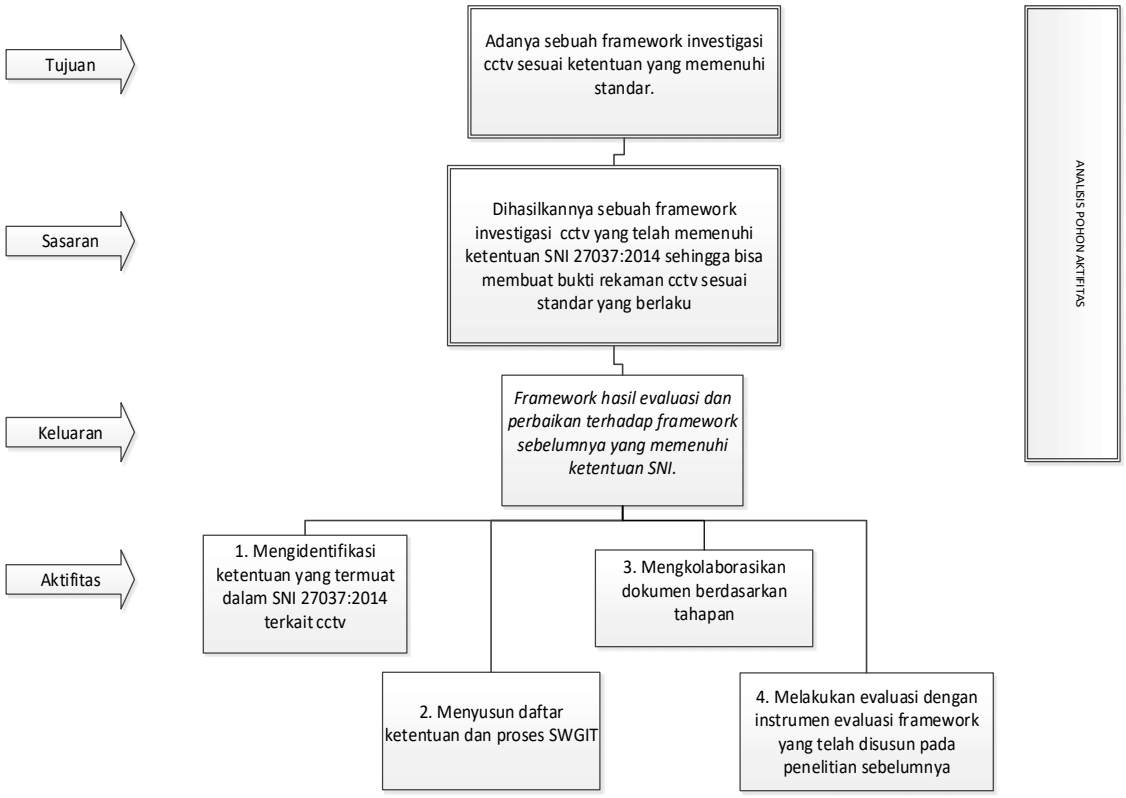
Pada tahapan analisis *Logical Framework Approach* dilakukan kegiatan untuk menyusun evaluasi yang dilakukan sebagai perencanan kegiatan dengan menggunakan matriks *logframe.* Dimana nantinya pada *logframe* tersebut dilakukan perincian untuk membagi ke beberapa bagian sehingga memperoleh alur evaluasi yang terstruktur untuk mencapai tujuan yang telah ditetapkan.

Pada matrik tersebut mampu menjelaskan mengenai keseluruhan kegiatan evaluasi yang dilakukan. Matrik ini tersusun dari empat elemen dasar yaitu tujuan (*goals*), sasaran (*purpose*), keluaran (*outputs*), dan kegiatan (*activities*). Sehingga mampu digunakan untuk menjadi landasan mengenai kegiatan apa saja yang dilakukan untuk dapat menghasilkan *framework* investigasi CCTV yang memenuhi ketentuan yang berlaku.

Tabel 4. 1 *Logframe* Kegiatan

Deskripsi Kegiatan	**Indikator**	**Cara Verifikasi**	**Asumsi**
Tujuan/*Goal* 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/*Purpose* Dihasilkannya sebuah *framework* investigasi CCTV yang telah memenuhi ketentuan SNI 27037:2014	*Framework* telah memenuhi ketentuan yang berlaku	Memenuhi instrument evaluasi untuk forensik CCTV	Mengikuti standar yang diakui untuk digunakan dalam penyelidikan forensik digital.
Keluaran/*Outputs* *Framework* hasil kolaborasi	*Framework* hasil perbaikan dan evaluasi	• Memenuhi instrument evaluasi • Memenuhi kebutuhan penyelidik	Ketika aktivitas dilakukan maka keluaran diperoleh
Aktifitas/*Activities* Mengidentifikasi ketentuan yang termuat dalam SNI/ISO 27037:2014 terkait CCTV	Proses penting terkait investigasi CCTV yang diatur SNI	SNI/ISO 27037:2014	Ketika data atau input tersedia maka aktivitas bisa dilakukan
Menyusun daftar ketentuan dan proses SWGIT	Metode praktis investigasi CCTV mengikuti SWGIT	SWGIT v1.0 2013.09.27	
Mengkolaborasikan hasil identifikasi	*framework* penangan awal untuk investigasi CCTV	Tahapan Mekanisme dan Dokumentasi pengambilan rekaman video dari CCTV	Tidak ada
Melakukan perbaikan terhadap *framework* sesuai ketentuan yang telah tertera	*Framework* perbaikan telah memenuhi ketentuan standar yang ada	Instrument evaluasi SNI/ISO 27037:2014 *List of Action* dari ACPO	Menambahkan tahapan bila ditemukan adanya tahapan yang tidak terpenuhi.
Melakukan uji *framework* melalui wawancara pendapat praktisi	*Framework* mudah dipahami dan bisa digunakan bila diterapkan	Pendapat praktisi, akademisi dan penyidik	Menyesesuaikan tahapan terhadap pendapat yang diberikan

Dari keterangan yang diperoleh dari rencana evaluasi berdasarkan tabel diatas, maka dapat digambarkan pohon kegiatan evaluasi yang mana pohon paling atas merupakan tujuan akhir yang mau dicapai., kemudian sasaran, keluaran, dan terakhir aktifitas yang dilakukan untuk mendapatkan keluaran yang hasilnya menjadi sasaran dari tujuan.



Gambar 4.1 Analisis Pohon Aktifitas

4.2 Identifikasi Ketentuan SNI 27037:2014

Pada dokumen SNI 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 motede penangan bukti elektronik.

Terdapat 4 tahapan kegiatan penyelidikan secara berurutan yang dibahas pada klausul terakhir yaitu identifikasi, pengumpulan, akuisisi dan preservasi. Dimana dalam penelitian ini proses identifkasi ketentuan standar berkaitan forensik CCTV dengan melakukan penelitian menyeluruh terhadap isi dokumen SNI 27037:2014 dimana hasil temuan nantinya akan di tampilkan kedalam Table 4.2 untuk mempermudah dalam mengamati hasil identifikasi.

Tabel 4. 2 Hasil Identifikasi Tahapan dalam SNI 27037:2014

No	Detail proses	Penjelsaan Proses	Bagian
A	**Identifikasi**		
1	Pengarahan	Sesi pengarahan mengenai perkara/kejadian, lokasi, peran dan tanggung jawab. Mandat/surat perintah investigasi.	6.3 dan 6.7.1
2	Persiapaan dan perencanan	Menpersiapakan rencana investigasi, alat khusus, peralatan dan manual terkait bukti digital yang menjadi focus.	6.7.2
3	Tindak Pencegahan	Melakukan pengamanan dan melindungi potensi bukti digital TKP.	6.2.1
4	Penliaian resiko	Melakukan penilaian resiko mengenai keamanan personel sebelum memulai proses. Contoh apakah terdapat bahaya fisik bagi personel.	6.2.2
5	Pencarian bukti	Mencari peralatan elektronik yang berkemungkinan menyimpan bukti digital potensial	5.4.2
6	Dokumentasi	Mencatat temuan yang diperoleh selama proses pencarian barang bukti	6.6
7	Chain of custody	Mencatat dokumen investigasi terkait kronologi dari penangan dan perpindaham bukti digital	6.1
B	**Mengumpulkan**		
1	Memastikan isi	Menetukan sistem mendokumetasikan potongan video terkait,waktu kejadian dalam alat rekam.	7.3
2	Memastikan kamera	Memastikan posisi peletakan dan kondisi kamera aktif merekam kejadian.	7.3
3	Jadwal overwrite	Memastikan atau meperkirakan jadwal	7.3
4	Dokumentasi	Mencatat model perangkat, *time frame*, perbedaan waktu di sistem dan waktu nyata.	7.3

Tabel 4. 3 Hasil Identifikasi Tahapan dalam SNI 27037:2014 Lanjutan

No	Detail Proses	Penjelasaan Proses	Bagian
C	**Akuisisi**		
1	Penetuan media akuisisi	Memilih cara memperoleh video digital,terdapat beberapa pilihan yaitu: DVD, *flash disk, network connection, export feature.*	7.3
2	Live akuisisi	Lakukan logikal akusisi menggunakan sistem pada peralatan CCTV. Karena tidak menyita dan tidak mengambil keseluruhan data Dan bisa disimpan dalam format data ZIP.	5.4.4
3	Pemeriksaan akusisi	Memeriksa potongan video hasil akuisis sesuai dengan kejadian video nyata, player media untuk menjalakan file.	7.3
4	Label bukti	Media penyimpanan hasil akuisisi ditandai sebagai *master digital evidence copy.*	7.3
5	Dokumentasi	Mencatat semua temuan dan tindakan yang dilakukan.	6.1
D	**Preservasi**		
1	Verifikasi akusisi	Menggunakan fungsi verifikasi sebagai segel keaslian pada *master evidence* seperti *digital signature* berupa nilai *hash* dari alogoritma md5	7.1.4
2	Memberikan segel barang bukti	Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.	6.9.2
3	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.	6.9.3
4	Dokumen perjalanan	Menyiapakan dokumen atau surat perjalan untuk perpindahan bukti digital dari penyidik kepada labortorium atau ruang penyimpanan.untuk memastikan keamanannya maka juga harus diterangkan pada *Chain of Cutody.*	6.9.4
5	Pemindahan barang bukti	Selama proses pemindahan barang bukti, petugas harus berhati-hati dan selalu memperhatikan keamanan barang bukti.	6.9.4
6	Penyimpanan barang bukti	Menyiapakan dokumen atau surat perjalanan untuk perpindahan bukti digital dari ruang penyimpanan.	6.9.4

Dari hasil identifikasi proses penting dari dokumen SNI 27037:2014 diperoleh 4 tahapan utama terkait dengan forensik CCTV yang mana nantinya akan dijadikan acuan untuk melakukan pengembangan terhadap *framework* yang akan dibangun. Tahapan Identifikasi

terdiri dari 7 proses, Tahapan Pengumpulan terdiri dari 5 Proses, Tahapan Akusisi terdiri dari 5 proses, Tahapan Preservasi terdiri dari 6 proses. Kegiatan penelitian selanjutnya adalah menyusun proses penting pada dokumen SWGIT *v1.0 2013.09.27.*

4.3 Menyusun Daftar Ketentuan dan Proses SWGIT

Pada dokumen SWGIT yang digunakan langsung membahas mengenai pedoman untuk setiap kondisi yang ada ditiap tindakan yang akan diambil saat melakukan forensik CCTV secara penulisanya dokumen ini berbeda dengan dokumen SNI yang secara jelas langsung menyampaikan tindakan yang diambil untuk mengekstrak video dari sistem CCTV dengan membagi tindakan yang diambil kedalam 4 tahapan. Untuk mempermudah dalam melihat proses pentingnya maka akan diidentifikasi dan menampilkannya kedalam Tabel 4.4.

Tabel 4.4 Tabel Identifikasi Tahapan dalam SWGIT

No	Detail Proses	Penjelasaan Proses
A	**Recognizing CCTV Evidence**	
1	Mengamati	Melihat keadaan sekitar TKP untuk mencari posisi perangkat CCTV
2	Type CCTV	Mengetahui jenis dvr yang digunakan *stand alone* atau *pc based* dan mengetahui *playback software.serial number,*
3	Feature CCTV	fitur yang terpasang pada dvr, seperti *multiplexer, transactional data, network capabilitis*
B	**Steps to Take Upon Scene Arival**	
1	Catatan	Catatan, harus selalu Menjaga/merangkum metode yang dipakai atau tindakan yang diambil
2	Melihat rekaman	Memastikan bahwa peristiwa /kejadian terkait dalam video relevan telah terekam dan dilakukan oleh yang paham alat *recording* saat melakukan *playback.*
3	Jadwal maintance	Menentukan tanggal rekaman paling awal untuk memperkirakan waktu tersisa sebelum *overwrite.*
4	Operator assist	Keberadaan operator terlatih mendampingi pengambilan video digital
5	Time display	Membandingkan waktu yang ditampilkan oleh sistem dengan waktu nyata,bila berbeda maka disamakan ke dalam zona waktu setempat.
6	Metadata	Mencatat metadata *image quality,fps, frame size, firmware version, event log,password*
7	Native file	Mencari tahu format file yang dipergunakan oleh sistem
8	Kontak lokasi	Mengumpulkan info alamat kejadian, jam operasi, kontak/telepon pemilik dan kontak *intaslle*r
9	Foto sistem	Foto sistem bagian depan dan belakang

Tabel 4. 5 Identifikasi Tahapan dalam SWGIT Lanjutan

No	Detail Proses	Penjelsaan Proses
B	**Steps to Take Upon Scene Arival**	
10	Sketsa posisi kamera	Membuat sketsa dari posisi kamera diruang lokasi kejadian
11	Operator pendamping	Mencari tahu siapa yang menjadi operator pada sistem CCTV tersebut. Hanya bila investigator tidak mampu atau tidak memahami sistem maka diperlukan ada nya operator atau admin dari kamera pengaswas yang mendampingi proses pengambilan file video.
C	**Assesing the Recording System for Output**	
1	Evaluasi output	Menentukan seberapa besar data dan tipe data yang akan diambil, sehingga diketahui media penyimpanan yang sesuai serta mengamati sistem *output* yang tersedia. Misalnya *Optical Disc*, *Flash media*, *usb*, VGA/HDMI, *removable /replacing hard drive.*
2	Waktu tersedia	Cara / pilihan metode untuk *output* terbaik berdasarkan dari waktu dan penyimpanan yang dibutuhkan.
3	Tes ambil	Melakukan tes pengambilan apakah peralatan menyediakan opsi untuk bisa mengambil *native file* beserta *playback software* nya.
4	Output tersedia	CD/DVD writer opsi ini dipilih bila video digital berdurasi beberapa menit yang tidak memerlukan ruang yang luas.
		Flash media opsi ini dipilih bila durasi video berkisar 24 jam
		Mass storage device opsi ini dipilih bila permintaan dari video yang diambil berkisar selama 30 hari, dimana menggunakan metode clone or removing the recording unit
		Network connection opsi ini jika network viewer melakukan recover dari rekaman native video file
5	Legal output	Metode output yang dipakai harus mampu mengangkat data video asli dari unit perekaman digital dan dapat di putar ulang/ *playback*
D	**Evidence Handling Procedure**	
1	Audit trail	Memastikan mencatat secara detail setiap tindakan pada tiap tahapan
2	Chain of Custody	Mencatat barang bukti dalam form CoC sesuai dengan aturan tiap instansi
3	Pemindahan	Memastikan pengemasaan dan menyegel bukti sesuai dengan dengan kebutuhan, jika *hard drive* gunakan *individual foam insert boxes* serta jauhkan dari kondisi yang bisa merusaknya.
4	Menyimpan bukti	Menjauhkan bukti digital dari magnet dan lingkungan yang bisa merusak

Dari hasil identifikasi proses penting dari dokumen SWGIT diperoleh proses penting terkait dengan pengangkatan video digital untuk forensik CCTV yang mana nantinya akan dijadikan bahan acuan untuk melakukan kolaborasi terhadap *framework* yang akan dibangun. Pada hasil idetifikasi diatas terdapat 4 tahapan utama, dimulai dari tahapan *Recognizing CCTV evidence* terdiri dari 3 proses penanganan, tahapan *Steps to take upon scene arrival* terdiri dari 4 proses penanganan, tahapan *Assesing the recording system for output* terdiri dari 6 proses penanganan, tahapan *Evidence Handling Procedure* terdiri dari 4 proses penanganan. Setelah mengidenifikasi proses penting untuk investigasi CCTV dari kedua dokumen tersebut, langkah selanjutnya adalah melakukan kolaborasi untuk saling melengkapi tahapan investigasinya.

4.4 Kolaborasi Tahapan Antar Dokumen

Pada tahapan ini seluruh tahapan yang awalnya telah diidentifikasi akan dikolaborasikan menjadi tahapan-tahapan utama yang nantinya akan digunakan untuk membangun sebuah instrument *framework* investigasi perangkat kamera pengawas CCTV. Proses pengkolaborasian dilakukan dengan mengadaptasi pemodelan pendekatan logika dan kesamaan terminologi.

4.4.1 Pengklasifikasian Menggunakan Pemodelan *Logic*

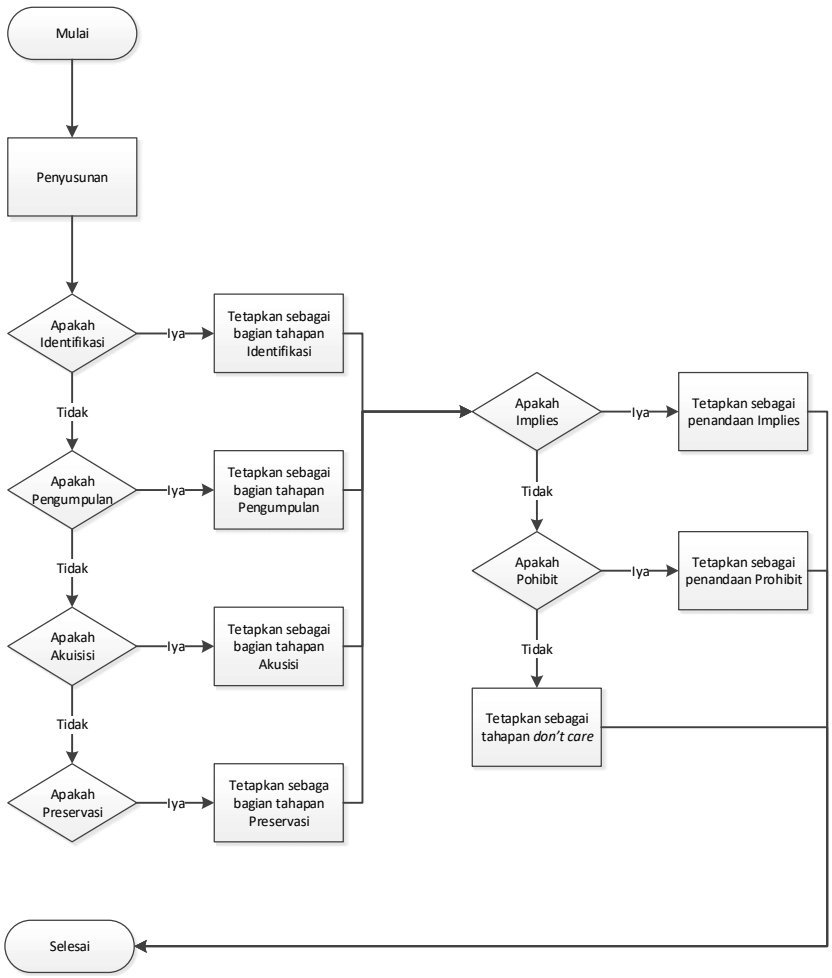
Setelah melakukan ekstraksi terhadap dokumen yang digunakan maka tindakan yang selanjutnya dilakukan adalah melakukan kolaborasi atau penggabungan antar dokumen tersebut kedalam beberapa tahapan menurut variable yang terbagi menjadi identifikasi, pengumpulan, akuisisi dan preservasi berdasarkan dari penjelasaan terminologi. Dimana tahapan hasil ekstraksi dari dokumen SWGIT akan diberikan indikator *role model* berdasarkan penjelasaan pada prosesnya atau terminologi dengan mengadaptasi dari pendekatan logika agar mempermudah penyusunannya saat dilakukan kolaborasi. Bila terdapat kesamaan terminologi maka tahapan tersebut dikatakan "*implies".* Kemudian bila tahapan tersebut merupakan tahapan yang dianggap penting dan tidak ada pada dokumen SNI maka dikatakan sebagai "*prohibit".* Sedangkan yang terakhir dikatakan sebagai "*don't care"* jika tahapan tersebut tetap berada pada tahapan semula karena tidak dapat dikolaborasikan dan tidak memiliki termnologi yang sama dengan tahapan pada dokumen SNI.

Table kolaborasi dari tabel 3.4, disertakan dengan kolom bernama penandaan sehingga diketahui *role* model dari tahapan hasil ektraksi SWGIT. Setiap tahapan yang telah

diektraksi dari masing-masing klausul akan diklasifikasikan menurut variable *ouput* (identifikasi, pengumpulan, koleksi, preservasi) dan kemudian pada tahapan yang telah diklasifikasi di kumpulkan berdasarkan *role* model yaitu *implies, prohibit, don't care* untuk selanjutnya di proses sesuai dengan tindakan yang sesuai berdasarkan kebutuhannya dalam penyusunannya.

Pengklasifikasian berdasarkan variable *output* dilakukan untuk membantu penyusunan saat melakukan kolaborasi antar dokumen nantinya, karena variable *output* merupakan tahapan utama dari tahapan – tahapan yang diekstraksi sehingga ditetapkan sebagai kerangka awal dalam penyususnan instrument *framework*. Sedangkan pengklasifikasian indikator sifat *role* model dibuat untuk mempermudah dalam melakukan kolaborasi pada tahapan selanjutnya, karena tahapan yang akan dikolaborasikan hanyalah tahapan yang bersifat "*implies"* dikarenakan memiliki kesamaan terminologi terhadap tahapan pada dokumen SNI 27037:2014.

Tindakan yang akan dilakukan untuk pengklasifikasiannya mengikuti *flowchart* yang telah dibuat pada Gambar 4.2 dibawah ini, kemudian melakukan penulisan kedalam tabel.



Gambar 4. 2 *Flowchart* Proses Pengklasifikasian

Pada alur proses tersebut menerangkan proses pengkalsifikasian yang digunakan untuk tahapan hasil identifikasi dari SWGIT, dimana untuk variable *output* berdasakan dari hasil kegiatan dari setiap tahapan yang menjadi aktifitas. Selanjunya untuk sifat *role* model ditentukan berdasarkan dari terminologi dan asumsi didalam tahapan yang berhubungan. Hasil ekstraksi yang telah dilakukan proses klasifikasi terhadap masing-masing tahapannya maka selanjutanya dapat menghasilkan sebuah tabel klasifikasi dengan penggambaran tabel yang menampilkan variable *output* dan sifat *role* modelnya. Dimaksudkan agar pembaca dapat dengan mudah untuk mengamati dan membedakan manakah tahapan yang bersifat *implies, prohibit, don't care.* Berikut dibawah ini Tabel 4.6 yang merupakan tabel klasifikasi hasil ektraksi dokumen SWGIT terkait forensik CCTV.

Tabel 4. 6 Klasifikasi Tahapan SWGIT

No	Detail Proses	Indikator Output	Asumsi	Role Model	Tanda SNI
	Recognizing DCCTV				
1	Mengamati	Indentifikasi	Kesamaan terminologi	Prohibit	A-5
2	Type CCTV	Indentifikasi	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	A-5
3	Feature CCTV	Indentifikasi	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	A-5
	Steps To Take Upon Scene Arival				
1	Catatan	Pengumpulan	Kesamaan terminologi	Implies	B-4
2	Melihat rekaman	Pengumpulan	Kesamaan terminologi	Implies	B-1
3	Jadwal maintance	Pengumpulan	Kesamaan terminologi	Implies	B-3
4	Operator assist	Pengumpulan	Tidak ada kesamaan dengan yang lainnya	Don't care	
5	Time display	Pengumpulan	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	B-4
6	Metadata dokumentasi	Pengumpulan	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	B-4
7	Native file	Pengumpulan	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	B-4
8	Secene Contact	Pengumpulan	Tidak ada kesamaan dengan yang lainnya	Don't Care	
9	Photograph system	Pengumpulan	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	B-5
10	Sketsa posisi kamera	Pengumpulan	Memiliki terminologi umum dan belum dimiliki oleh SNI	Prohibit	B-5
11	Operator pendamping	Pengumpulan	Tidak ada kesamaan dengan yang lainnya	Don't care	

Tabel 4. 7 Klasifikasi Hasil Klasifikasi SWGIT

No	Detail Proses	Indikator Output	Asumsi	Role Model	Tanda SNI
	Assessing the Recording System for Output				
1	Evaluasi output	Akuisisi	Kesamaan terminologi	Implies	C-1
2	Waktu tersedia	Akusisi	Tidak ada kesamaan dengan yang lainnya	Don't care	
3	Tes ambil	Akuisisi	Tidak ada kesamaan dengan yang lainnya	Don't care	
4	Output tersedia	Akuisisi	Terdapat kesamaan terminologi	Prohibit	C-1
5	Legal output	Akuisisi	Kesamaan terminologi	Implies	C-3
	Evidence Handling Procedure				
1	Audit trail	Preservasi	Tidak ada kesamaan dengan yang lainnya	Don'tcare	
2	Chain of Custody	Preservasi	Kesamaan terminologi	Implies	D-7
3	Pemindahan	Preservasi	Kesamaan terminologi	Implies	D-4
4	Menyimpan bukti	preservasi	Kesamaan terminologi	Implies	D-5

Setelah melakukan klasifikasi terhadap hasil ektraksi dari dokumen SWGIT maka telah diketahui setiap indikator dan sifat *role* model dari setiap tahapannya. Terdapat beberapa klausul yang tidak bisa dijadikan tahapan utama dikarenakan tidak menjelaskan mengenai proses penanganan awal forensik CCTV. Berdasarkan tabel klasifikasi tersebut maka bisa dilakukan tahapan selanjutnya yaitu mengelompokan setiap tahapan berdasarkan dari *role* modelnya, dimana terbagi menajdi tiga yaitu: 8 tahapan yang bersifat *implies,* 7 tahapan yang bersifat *prohibit*, dan 7 tahapan yang bersifat *don't care.* Semua tahapan tersebut terbagi dalam 4 tahapan utama berdasarkan penjelasaan terminologi, yaitu: Identifikasi, Pengumpulan, Koleksi, Preservasi. Berikut dibawah ini Tabel 4.8 yang merupakan tabel hasil klasifikasi SWGIT.

Tabel 4.8 Hasil Ektraksi SWGIT

NO	Identifikasi	Pengumpulan	Akuisis	Preservasi
1	Mengamati	Catatan	Tes ambil	Audit trail
2	Type CCTV	Melihat rekaman	Output tersedia	Chain of Custody
3	Feature CCTV	Jadwal maintance	Waktu tersedia	Pemindahan
4		Time display	Evaluasi output	Menyimpan bukti
5		Metadata	Legal output	
6		Native file		
7		Operator pendamping		
8		Kontak lokasi		
9		Foto sistem		
10		Sketsa posisi kamera		

Keterangan warna Tahapan:

: Tahapan dengan role model "*Implies*"

: Tahapan dengan role model "*Prohibit"*

: Tahapan dengan role model "*Don't Care"*

Dari tabel diatas telah disusun proses penting hasil ektraksi dari dokunen SWGIT berdasarkan pengklasifikasianya agar dapat mudah diamati oleh pembaca. Pada tabel tersebut divisualisasikan indikator role model dengan warna biru untuk indikator bersifat *implies,* coklat untuk indikator bersifat *prohibit,* dan warna hijau untuk indikator bersifat *don't care.* Dimana terdapat 3 tahapan untuk proses identifikasi, 10 tahapan untuk proses pengumpulan, 5 tahapan untuk proses akuisisi, dan 4 tahapan untuk proses preservasi.

4.4.2 Kolaborasi Dengan Indikator Role Model

Dari tabel sebelumnya yang merupakan tabel klasifikasi hasil ektraksi dokumen SWGIT, maka selanjutnya disusun untuk dikolaborasikan dengan hasil ekstraksi dokumen SNI 27037:2014 yang telah disusun sebelumnya pada tabel 4.11 dimaksudkan agar bisa diperoleh tahapan-tahapan utama yang nantinya akan digunakan untuk menyusun *framework* investigasi penanganan awal pada forensik CCTV sehingga mampu dipergunakan sebagai pedoman investigasi kamera pengawas CCTV. Pada proses kolaborasi ini terdapat variable *outcomes* yang merupakan pengaruh dari variable asumsi. Berikut tabel kolaborasi tahapan dengan *role* model yang ditampilkan pada Tabel 4.9.

Tabel 4.9 Kolaborasi Berdasarkan Role Model

No	Detai Proses Pada SNI 27037:2014	Terdapat pada pedoman SWGIT bagian :		
		Tahapan	Outcomes	Role Model
A	**Identifikasi**			
1	Pengarahan			
2	Persiapan dan perencanaan			
3	Tindak pencegahan dilokasi kejadian			
4	Penliaian resiko			
5	Pencarian bukti	• Mengamati • Tipe CCTV • Fitur CCTV	Penambahan tahapan ini menjadi tahapan utama	Prohibit
6	Dokumentasi			
7	Chain of custody			
B	**Pengumpulan**			
1	Memastikan isi	• Meilhat rekaman	Pengkolaborasian dan penamaan baru yang lebih mewakili	Implies
2	Memastikan kamera			
3	Jadwal overwrite			
4	Dokumentasi	• Catatan • Time display • Metadata • Native file	Penambahan tahapan ini menjadi tahapan utama	Prohibit
5	Keterangan verbal	• Maintain schedule • Scene contact • Photograph system • Operator assist	Penambahan tahapan ini menjadi tahapan utama	Prohibit
C	**Akuisisi**			
1	Penetuan media akuisisi	• Evaluasi output	Pengkolaborasian dan penamaan baru yang lebih mewakili	Implies
	Live akuisisi	• Output tersedia	Penambahan tahapan ini menjadi tahapan utama	Prohibit
2	Pemeriksaan akusisi			
3	Label bukti	• Legal output	Pengkolaborasian dan penamaan baru	Implies
4	Dokumentasi	• Catatan	Pengkolaborasian dan penamaan baru	Implies

Tabel 4. 10 Kolaborasi Berdasarkan Role Model

No	Detail Proses SNI	Terdapat pada pedoman SWGIT bagian :		
		Tahapan	**Outcomes**	**Role Model**
C	**Akuisisi**			
5	Penetuan media akuisisi	• Tes ambil	Tetap mempertahankan tahapan ini	Don't care
		• Waktu tersedia	Tetap mempertahankan tahapan ini	Don't care
D	**Preservasi**			
1	Verifikasi akusisi			
2	Memberikan segel barang bukti			
3	Pemeriksaan aspek keamanan pemindahan barang bukti			
4	Pemindahan barang bukti	• Pemindahan	Pengkolaborasian dan penamaan baru	Implies
5	Penyimpanan barang bukti	• Menyimpan bukti	Pengkolaborasian dan penamaan baru	Implies
6	Dokumen perjalanan			
		• Audit trail	Tetap mempertahankan tahapan ini	Don't care

Dari tabel 4.9 diatas yang merupakan rancangan awal dari kolaborasi, terlihat bahwa beberapa tahapan memiliki terminologi yang sama dengan hirarki *flowchart* yang sama juga. Maka pada tahapan ini setiap tahapan dengan indikator *implies* akan dikolaborasikan dengan menggabungkan menjadi sebuah tahapan dengan penamaan sesuai dengan literatur, buku maupun dokumen resmi forensik digital yang ada berikut ini adalah proses kolaborasi yang dilakukan:

a. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Pencarian baranag bukti.
   - Pencarian bukti merupakan proses pencarian barang bukti di sekitar lokasi kejadian yang bisa menjadi bukti potensial.
   - Mengamati merupakan proses memantau keadaan sekitar tkp untuk menyadari benda yang bisa menjadi bukti digital potensial.
b. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Memastikan isi.

- Memastikan isi berasal dari dokumen sni memiliki terminologi sebagai sebuah tahapan dimana melakukan pengamatan untuk menentukan sistem mendokumentasikan potongan video terkait waktu kejadian dalam alat rekam.
- Melihat rekaman berasal dari dokumen swgit memiliki terminologi sebagai sebuah tahapan dimana memastikan bahwa peristiwa /kejadian terkait dalam video relevan telah terekam dan dilakukan oleh yang paham alat *recording* saat melakukan *playback.*

Dari tahapan yang dijabarkan diatas, ternyata tahapan dari dokumen SWGIT memiliki terminologi yang sama dengan definisi pengumpulan untuk memastikan isi menurut dokumen SNI 27037:2014 pada klausul 7.3 CCTV *collection* yaitu suatu proses untuk memastikan isi pada konten video sesuai dengan informasi yang diinginkan dengan melakukan pengamatan visual. Secara objektif penulis memilih Memastikan Isi sebagai nama pada tahapan ini karena lebih mudah memahami maksud kegiatannya dari penyebutan tersebut.

c. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Jadwal *Overwrite*.
   - Jadwal *overwrite* menurut dokumen sni yaitu suatu tahapan untuk memastikan ukuran penyimpanan video terkait pada sistem sehingga diketahui jadwal *overwrite* saat data di media penyimpanan tertimpa data baru.
   - Jadwal *Maintance* adalah tahapan untuk menentukan tanggal rekaman paling awal untuk memperkirakan waktu tersisa sebelum *overwrite* pada media penyimpanan yang digunakan.

Dari tahapan berbeda istilah diatas, memiliki terminologi yang sama dengan definisi kegiatan memastikan waktu *overwrite* pada media penyimpanan yang digunakan oleh alat perekam. Dari tahapan berbeda isitilah diatas memiliki terminologi yang sama sehingga tahapan jadwal *overwrite* mencangkupi definisi tahapan lainnya. Oleh karena itu kolaborasi tahapan ini dinamakan sebagai tahapan Jadwal *Overwrirte*.

d. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Dokumentasi.
   - Dokumen adalah tahapan dari dokumen sni yang melakukan tindakan untuk mencatat semua temuan dan tindakan yang dilakukan saat investigasi.
   - Note adalah tahapan dari dokumen swgit dimana kegiatanya untuk merangkum temuan dan metode yang atau tindakan yang diambil selama investigasi.

Dari tahapan berbeda istilah diatas, memiliki terminologi yang sama namun tahapan dokumentasi telah mencangkupi definisi dari tahapan lainnya. Sehingga kolaborasi tahapan ini dinamakan sebagai tahapan Dokumentasi.

e. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Evaluasi *output*

- Penetuan Media akuisisi menurut dokumen sni yaitu suatu tahapan untuk memilih cara memperoleh video digital, terdapat beberapa pilihan yaitu: DVD, *flash disk, network connection, export feature.*
- Evaluasi *output* adalah tahapan dari dokumen swgit dimana kegiatanya menentukan seberapa besar data dan tipe data yang akan diambil, sehingga diketahui media penyimpanan yang sesuai serta mengamati sistem *output* yang tersedia. Misalnya *Optical Disc*, *Flash media*, *usb*, VGA/HDMI, *removable /replacing hard drive.*

Dari tahapan berbeda istilah diatas, memiliki terminologi yang sama namun tahapan Evaluasi *output* telah mencangkupi definisi dari tahapan lainnya. Sehingga kolaborasi tahapan ini dinamakan sebagai tahapan Evaluasi *output.*

f. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi Pemeriksaan akuisisi.

- Pemeriksaan akuisisi adalah tahapan dimana investigator memeriksa potongan video hasil akuisis sesuai dengan kejadian. Video nyata, dan *player* media untuk menjalakan file video tersebut juga bisa dijalankan disitem lainya untuk diputar ulang.
- *Legal output* adalah tahapan dari dokumen swgit untuk memastikan metode output yang dipakai harus mampu mengangkat data video asli dari unit perekaman digital dan dapat di putar ulang/ *playback.*

Dari tahapan berbeda istilah diatas, memiliki terminologi yang sama namun tahapan pemeriksaan akuisisi telah mencangkupi definisi dari tahapan lainnya. Sehingga kolaborasi tahapan ini dinamakan sebagai tahapan pemeriksaan akuisisi.

g. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi *Chain of Costudy*.

- CoC dari dokumen sni yaitu memastikan mencatat dokumen investigasi terkait kronologi dari penangan dan perpindaham bukti digital.
- CoC dari dokumen swgit mencatat dokumen mencatat barang bukti dalam form CoC sesuai dengan aturan tiap instansi.

Dari kedua dokumen tersebut memiliki nama tahapan yang sama dan terminologi yang juga sama. Oleh karena itu tahapan ini disebut dengan *Chain of Costudy*.

h. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi pemindahan barang bukti.
   - Pemindahan barang bukti menurut dokumen sni adalah 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*.
   - *Transfer* adalah tahapan dari dokumen swgit untuk memastikan pengemasaan dan menyegel bukti saat memindahkan sesuai dengan dengan kebutuhan, jika *hard drive* gunakan *individual foam insert boxes* serta jauhkan dari kondisi yang bisa merusaknya.

Dari kedua dokumen tersebut memiliki nama tahapan yang sama dan terminologi yang juga sama. Oleh karena itu tahapan ini disebut dengan Pemindahan barang bukti.

i. Kolaborasi tahapan yang memiliki indikator "implies" dengan terminologi penyimpanan barang bukti.
   - Penyimpanan barang bukti menurut dokumen sni adalah tahapan untuk mengamankan barang bukti ditempat aman, barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang baik.
   - Penyimpanan barang bukti menurut dokumen swgit adalah proses mengamankan barang bukti dengan menjauhkan dari magnet dan lingkungan yang bisa merusak.

Dari kedua dokumen tersebut memiliki nama tahapan yang sama dan terminologi yang juga sama. Oleh karena itu tahapan ini disebut dengan Penyimpanan barang bukti.

Selain tahapan berindikator *implies* juga terdapat tahapan yang bersifat *prohibit* yang memiliki istilah tahapan yang bersifat subjektif dan belum ter-generalisasi. Bila ditinjau dari sifat *role model prohibits* yang artinya tahapan tersebut memiliki terminologi umum dan belum dimiliki oleh *framework* lainya. Tahapan tersebut dapat diasumsian sebagai tahapan utama dalam penyusunan *framework* yang akan disusun. Dibawah ini tabel 4.11 merupakan tabel hasil klaborasi dengan menggunakan *role* model yang dirunut berdasarkan hasil dari proses pengklasifikasian.

Tabel 4. 11 Hasil Kolaborasi

No	Identifikasi	Pengumpulan	Akuisisi	Preservasi
1	Pengarahan	Melihat rekaman	Tes ambil	Verifikasi akusisi
2	Persiapaan dan perencanan	Memastikan kamera	Output tersedia	Memberikan segel barang bukti
3	Tindak pencegahan dilokasi kejadian	Jadwal overwrite	Waktu tersedia	Dokumen perjalanan
4	Penliaian resiko	Dokumentasi	Evaluasi output	Pemindahan barang bukti
5	Pencarian bukti	Time display	logikal akuisisi	Penyimpanan barang bukti
6	Tipe CCTV	Metadata	Pemeriksaan akusisi	Pemeriksaan aspek keamanan pemindahan barang bukti
7	Fitur CCTV	Native file	Label bukti	Audit trail
8	Dokumentasi	Keterangan verbal	Chain of Costudy	
9		Jadwal Maintain		
10		Kontak lokasi		
11		Foto sistem		
12		Operator pendamping		
		Sketsa posisi kamera		

Dari tabel diatas diperoleh hasil kolaborasi dari identifikasi proses penting dalam SNI 27037:2014 dan SWGIT *Retrieval of Digital Video*, didapatkan proses penting yang kemudian akan dijadikan acuan untuk menyusunnya kedalam diagram alur proses untuk proses forensik perangkat kamera pengawas CCTV.

4.5 Hasil Kolaborasi

Pada bagian ini menampilkan hasil kolaborasi tahapan yang telah dilakukan sebelumnya yang telah dipersiapkan pada tabel 4.11 ditunjukan untuk menyusun *first respond framework* untuk forensik CCTV.

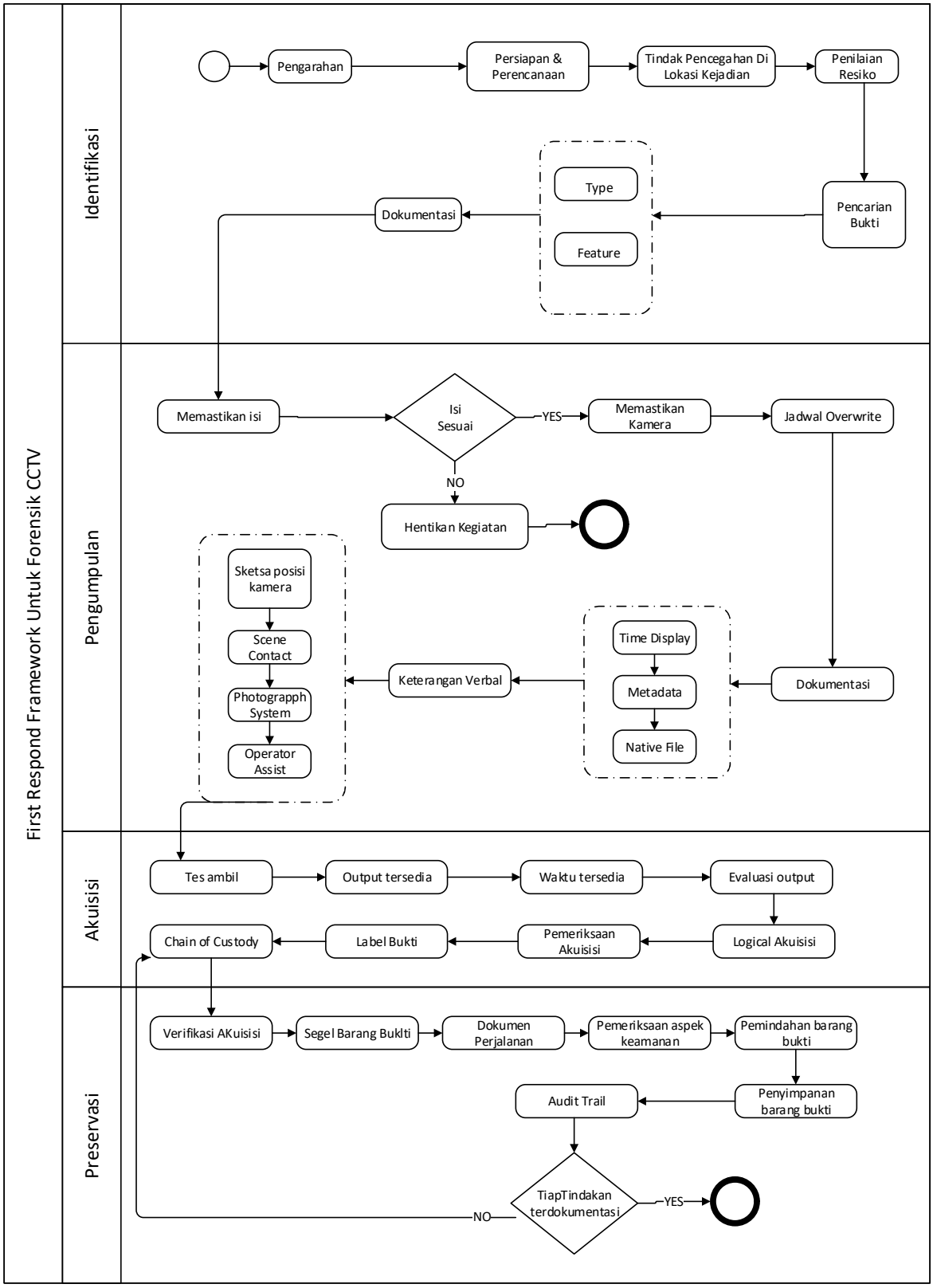
Penyusunan *framework* ini mengikuti ketentuan sebagai berikut:

1. Tahapan yang diidentifikasikan pada *output* di tabel hasil klasifikasi tahapan SWGIT akan ditetapkan sebagai tahapan utama dari *framework* karena diindekasikan sebagai tahapan tujuan dari kegiatan yang dideskripsikan dalam bentuk aktivitas.

2. Tahapan hasil kolaborasi yang ditampilkan pada tabel 4.15 telah berurut dan memiliki hirarki yang tetap dikarenakan pengaruh penerapan *role* model terhadap tahapan yang diperoleh dari identifikasi proses penting melalui dokumen yang dijadikan sebagai bahan rujukan.
3. *Framework* rancangan yang disusun ini akan dikritisi merujuk pada hasil evaluasi yang bersumber dari jurnal penelitian sebelumnya yang membahas instrumen penting di dokumen SNI 27037:2014 dan dokumen *best practice* yang telah diterbitkan oleh ACPO

4.5.1 Framework Rancangan Hasil Kolaborasi

Dengan memenuhi ketentuan dalam pembangunan *framework* diatas, maka peneliti merancang sebuah *framework* hasil kolaborasi yang telah didapat dengan menggunakan metode *logical framework approach.* Metode ini membantu proses pengkolaborasian *framework* berbeda dengan melalui kesamaan tujuan berdasarkan pemodelan *logic* dan kesamaan terminologi dari setiap tahapan, karena pengkolaborasian diarahkan pada kesamaan tujuan maka tidak merubah struktur hirarki dari model yang dikolaborasikan. Adapun *framework* rancangan hasil kolaborasi dapat dilihat pada gambar 4.3 dibawah ini.



Gambar 4. 3 Rancangan First Respond Framework Untuk Forensik CCTV

Pada diagram diatas menggambarkan mengenai alur proses tahapan pada *First Respond Framework* untuk forensik CCTV secara terurut. Pada diagram tersebut terdapat 4 bagian tahapan utama investigasi yang menjadi penyusunnya, yaitu Identifikasi,

Pengumpulan, Akuisisi dan Preservasi. Setiap tahapan utama tersusun dari beberapa tahapan yang mendukung proses tahapan utama.

Pada tahapan utama Identifikasi tersusun dari 6 tahapan dan 3 sub tahapan yang mendukung proses persiapan investigasi dan pencarian untuk mengenali serta mendokumentasikan bukti digital potensial. Mengidentifikasikan media penyimpanan digital dan perangkat pengolahan di lokasi TKP yang mungkin mengandung bukti digital potensial.

Selanjutnya tahapan utama Pengumpulan tersusun dari 5 tahapan dan 7 sub tahapan kemudian ada nya proses *decision* setelah tahapan *review record* untuk membantu pengguna dalam mengambil langkah selanjutnya bila rekaman video tidak berisi konten terkait dengan peristiwa yang diselidiki. Tahapan ini adalah kelanjutan dari tahapan utama Identifikasi, untuk mengumpulkan informasi mengenai bukti digital potensial setelah peralatan digital potensial teridentifikasi. Penyidik harus menentukan untuk melanjutkan atau tidak ke proses selanjutnya.

Tahapan utama Akuisisi tersusun dari 8 tahapan yang mendukung proses membuat salinan atau *copy* dari sistem peralatan CCTV yang kemudian menandainya sebagai *master evidence* dan mendokumentasikan tindakan yang diambil melalui *form Chain of Custody* dan berita acara pengambilan barang bukti.

Bagian terakhir *framework* adalah tahapan utama Preservasi tersusun dari 7 tahapan dan 1 proses *decision* untuk membantu dalam meng-audit kembali tindakan yang diambil telah terdokumentasi dan mengamankan serta memindahkan hasil akuisisi ke tempat penyimpanan.

Adapun penjelasan dari setiap tahapannya tentang aktivitas apa saja yang dilakukan dalam tahapan-tahapan *framework* tersebut berdasasrkan sumber dari gambar 4.3 dapat dilihat pada tabel di halaman lampiran.

4.6 Evaluasi Framaework Hasil Rancangan

Pada bagian ini dilakukan evaluasi terhadap *framework* yang dihasilkan. Evaluasi yang akan dilakukan adalah dengan menggunakan Instrumen Evaluasi *Framewrok* Investigasi Digital dan Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0 (ACPO, 2008). Perbandingan ini ditujukan untuk membuktikan bahwa *First Respond Framework* hasil ranganan peneliti dapat mengakomodir investigasi forensik untuk mengangkat video dari kamera CCTV.

4.6.1 Instumen Evaluasi Framework Investigasi Forensik Digital

Evaluasi dilakukan dengan membandingan tahapan-tahapan yang ada didalam *framework* yang telah dijabarkan sebelumnya dengan Instrumen Evaluasi *Framework* Investigasi Forensika Digital yang dirancang pada penelitian sebelumnya oleh (Sudyana et al., 2016) dimana pada penelitiannya berfokus untuk menyusun ketentuan dan proses penting dari standar yang berlaku dalam penelitiannya menggunakan SNI 27037:2014 sebagai dasar untuk membuat instrument evaluasi *framework*. Melalui instrument evaluasi untuk *framework* investigasi tersebut maka diharapkan dapat disesuaikan kembali *framework* hasil rancangan sehingga tidak melewatkan ketentuan yang telah diatur dalam standar nasional yang berlaku. Berikut penjelasan dari 38 proses penting yang dijadikan bahan acuan untuk melakukan evaluasi.

a. Identifikasi
    1. Perencanan investigasi

       Perencanaan dilakukan untuk menyusun strategi terkait investigasi yang akan dilakukan.
    2. Persiapan dan pengarahan tim

       Persiapan dilakukan dengan mempersiapkan seluruh kebutuhan baik itu hal administrasi maupun hal teknis untuk proses investigasi.
    3. Penilaian resiko keamanan TKP

       Penilaian resiko dilakukan untuk menjaga keamanan tim investigasi dan barang bukti.
    4. Pengamanan TKP

       Pengamanan TKP dilakukan untuk melindungi barang bukti. Pengamanan juga dilakukan untuk membatasi tidak semua orang bisa masuk ke TKP.
    5. Pencarian barang bukti

       Pencarian barang bukti merupakan proses dimulainya melihat keseluruh TKP dan mencari apa saja yang berpotensi sebagai barang bukti.
    6. Identifikasi barang bukti

       Melakukan identifikasi baik itu dari sisi jenis, bentuk, dan fungsinya terhadap barang bukti yang ditemukan dari hasil pencarian apakah bisa menjadi barang bukti yang berpotensi.
    7. Menentukan prioritas barang bukti

Memberikan prioritas terhadap barang bukti yang ditemukan terhadap aspek kerentanan data tersebut. Barang bukti yang mudah hilang seperti data dalam RAM harus diberikan prioritas.

8. Dokumentasi

   Segala aktivitias terkait penemuan barang bukti harus didokumentasikan. Dan dokumentasi disini juga mencakup keseluruhan aspek proses yang dilakukan mulai tahapan identifikasi sampai tahapan akhir investigasi yang harus selalu didokumentasikan.

9. Pencatatan barang bukti (Chain of custody)

   Chain of custody merupakan catatan rantai perjalanan barang bukti. Jadi ketika barang bukti ditemukan, harus dicatat informasinya dan selanjutnya kemana saja barang bukti tersebut berpindah atau apa saja yang dilakukan terhadap barang bukti harus dicatat di form chain of custody.

b. Pengumpulan

1. Menentukan barang bukti disita atau diakuisisi di TKP

   Dari hasil pemberian prioritas barang bukti, akan ditentukan apakah barang bukti yang ditemukan dapat langsung disita atau harus diakuisisi di TKP terkait datanya yang mudah hilang.

2. Melakukan penyitaan barang bukti

   Penyitaan barang bukti dibagi menjadi dua tahapan yaitu prosedur penyitaan perangkat dalam keadaan menyala dan dalam keadaan mati.

   (a) Barang bukti dalam keadaan menyala

   - Menganalisis apakah membutuhkan data *volatile* dari perangkat

     Analisis dilakukan untuk menentukan apakah dari perangkat yang menyala tersebut membutuhkan data *volatile* yang akan hilang apabila perangkat dimatikan.

   - Jika butuh lakukan prosedur *Live* akuisisi

     Jika hasil analisis menyimpulkan dibutuhkan data *volatile*, maka lakukan prosedur live akuisisi terhadap perangkat.

   - Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik

     Jika tidak butuh data *volatile*, atau proses *live* akuisisi telah selesai, lakukan pemeriksaan aspek keamanan data apakah data akan rusak apabila perangkat langsung dimatikan. Jika ternyata data akan rusak jika

perangkat langsung dimatikan, lakukan prosedur shutdown secara sistem normal.

- Melakukan prosedur shutdown perangkat

  Jika data stabil atau tidak bermasalah apabila perangkat langsung dimatikan, cabut secara langsung kabel power untuk mematikan perangkat.

(b) Barang bukti dalam keadaan tidak menyala

- Cabut semua kabel yang terkoneksi dan baterai

  Cabut semua kabel dan amankan kabel tersebut, lalu label seluruh port yang terkoneksi dengan kabel untuk memudahkan proses rekonstruksi.

3. Memberikan label barang bukti

   Label seluruh barang bukti untuk memudahkan proses rekonstruksi dan memudahkan mengenali barang bukti tersebut.

4. Mempacking barang bukti

   Packing atau lakukan proses pengemasan barang bukti dengan memasukkan barang bukti ke dalam alat pembungkus barang bukti. Perhatikan aspek keamanan barang bukti ketika akan dikemas.

5. Mengumpulkan keterangan verbal dari saksi-saksi

   Hal ini dilakukan untuk mendapatkan petunjuk lebih dan mencari informasi terkait barang bukti yang ditemukan.

c. Akuisisi

1. Pemeriksaan aspek keamanan barang bukti

   Pemeriksaan aspek keamanan untuk memastikan bahwa proses akuisisi yang dilakukan tidak akan merusak barang bukti.

2. Penentuan model akuisisi yang dilakukan

   Proses akuisisi terbagi menjadi 3 jenis yaitu akuisisi pada perangkat menyala, akuisisi pada perangkat yang tidak menyala dan partial akuisisi.

   (a) Akuisisi pada perangkat yang menyala

   - Lakukan prosedur *live* akuisisi untuk mendapatkan data volatile

     live akuisisi dilakukan ketika perangkat masih dalam keadaan menyala. Petugas harus berkompetensi dan menggunakan *tools* yang valid untuk melakukan prosesdur ini.

   - Jika data *non volatile* juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data *non volatile*

Lakukan juga prosedur live akuisisi jika data *non volatile* seperti data yang tersimpan di *logical* juga dibutuhkan.

- Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti
  Jika setelah proses akuisisi pada data *volatile* selesai dan perangkat dapat disita lakukan prosedur pengumpulan barang bukti.

(b) Akuisisi pada perangkat yang tidak menyala

- Lakukan prosedur static akuisisi dengan melakukan imaging terhadap media penyimpanan data
  Proses static akuisisi dijalankan dengan melakukan bitstream copy.

(c) Partial akuisisi

- Dapat dilakukan dengan menggunakan perpaduan prosedur live dan static akuisisi
  Partial akuisisi dilakukan untuk perangkat yang krusial dan tidak dimungkinkannya melakukan akuisisi terhadap keseluruhan data seperti dikarenakan jumlah data yang sangat besar.

3. Pelaksanaan akuisisi
   Setelah proses penentuan metode akuisisi dipilih, berikutnya adalah dilaksanakan proses akuisisi sesuai dengan metode akuisisi yang telah ditentukan sebelumnya.
4. Verifikasi hasil akuisisi
   Verifikasi dilakukan untuk memastikan data hasil akuisisi identik dengan data aslinya. Verifikasi dapat dilakukan dengan menggunakan fungsi hash.

d. Preservasi

1. Memberikan segel barang bukti
   Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya.
2. Pemeriksaan aspek keamanan pemindahan barang bukti
   Pemeriksaan aspek keamanan dilakukan untuk memastikan barang bukti aman selama proses pemindahan barang bukti dari TKP ke laboratorium.
3. Pemindahan barang bukti
   Selama proses pemindahan barang bukti, petugas harus memperhatikan keamanan barang bukti. Selain itu juga harus melakukan update di form chain of custody.
4. Penyimpanan barang bukti
   Barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang baik.

4.6.2 Evaluasi Framaework Dengan Instrumen Evaluasi Framework Investigasi

Pada evaluasi ini akan menggunakan tabel instrument evaluasi *framework* yang telah dibuat pada penelitian sebelumnya sebagai media untuk melihat perbandingan. Sehingga dapat diamati tahapan investigasi yang telah terpenuhi sebagaimana diatur sesuai Standar Nasional Indonesia untuk investigator dengan peran tugas sebagai penangan awal atau *Digital Evidence First Responder* yang bertanggung jawab untuk *inditification, collection, acquisition and preservation* dari bukti digital potensial bertujuan untuk menjaga integritas bukti digital. Berikut tabel 4.12 dibawah ini menampilkan hasil evaluasi *framework*.

Tabel 4.12 Hasil Evaluasi Framework

Proses Penting SNI 27037:2014	**Kelengkapan dalam *Framework* / SOP**	
	Ada	**Tidak**
Identifikasi		
Perencanaan investigasi	✓	
Persiapan peralatan & pengarahan team	✓	
Penilaian resiko keamanan TKP	✓	
Pengamanan TKP	✓	
Pencarian barang bukti	✓	
Identifikasi barang bukti	✓	
Menentukan prioritas barang bukti		✓
Dokumentasi	✓	
Pencatatan barang bukti (Chain of custody)	✓	
Pengumpulan		
Menentukan barang bukti disita atau diakuisisi di TKP		✓
Melakukan penyitaan barang bukti		✓
• Barang bukti dalam keadaan menyala	✓	
- Menganalisis apakah membutuhkan data volatile dari Perangkat		✓
- Jika butuh lakukan prosedur Live akuisisi		✓
- Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik		✓
- Melakukan prosedur shutdown perangkat		✓
• Barang bukti dalam keadaan tidak menyala		✓
- Cabut semua kabel yang terkoneksi dan baterai (jika ada baterai)		✓
- Lakukan prosedur pengumpulan berikutnya		✓
Memberikan label barang bukti	✓	
Mempacking barang bukti	✓	
Mengumpulkan keterangan verbal dari saksi-saksi	✓	

Tabel 4. 13 Hasil Evaluasi Framework Lanjutan

Proses Penting SNI 27037:2014	Kelengkapan dalam *Framework* / SOP	
	Ada	Tidak
Pengumpulan		
Akuisisi		
Pemeriksaan aspek keamanan data barang bukti		✓
Penentuan model akuisisi yang dilakukan	✓	
• Akuisisi pada perangkat yang menyala	✓	
- Lakukan prosedur live akuisisi untuk mendapatkan data Volatile		✓
- Jika data non volatile juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data non volatile tersebut		✓
- Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti		✓
• Akuisisi pada perangkat yang tidak menyala		✓
- Lakukan prosedur static akuisisi dengan melakukan imaging terhadap media penyimpanan data		✓
• Partial Akuisisi		✓
- Dapat dilakukan dengan menggunakan perpaduan prosedur live dan statik akuisisi		✓
Pelaksanaan akuisisi	✓	
Verifikasi hasil akuisisi	✓	
Preservasi		
Memberikan segel barang bukti	✓	
Pemeriksaan aspek keamanan pemindahan barang bukti	✓	
Pemindahan barang bukti	✓	
Penyimpanan barang bukti	✓	

Berdasarkan hasil evaluasi *framework* rancangan untuk forensik CCTV terhadap instrumen evaluasi untuk investigasi forensik digital oleh penelitian sebelumnya, walaupun saling memakai SNI 27037:2014 yang sama tetapi terdapat perbedaan tahapan yang dilakukan saat berada diproses pegumpulan dan akuisisi. Terlihat jika ada nya aktivitas yang berbeda saat proses ekstraksi datanya untuk memperoleh bukti digital.

Hasil evaluasi yang bias diamati yaitu terdapat 19 tahapan investigasi menurut instrument evaluasi yang tidak diterapkan oleh First Respond Framework untuk CCTV. Pada tahapan Identifikasi terdapat 1 proses forensik yang tidak dilakukan, kemudian pada tahapan Pengumpulan terdapat 9 proses forensik yang tidak lakukan, selanjutnya untuk tahapan Akuisisi terdapat 8 proses forensik yang tidak lakukan

Hal ini disebabkan karena *framework* rancangan pada penelitian ini berfokus untuk penangaan investigasi kamera pengawas CCTV, dimana setiap peralatan elektronik digital

memiliki karakteristiknya tersendiri. Langkah pendekatan untuk mengekstrak potongan video dari *Computer Based Digital Video Recorder* atau *Stand-Alone Embedded DVR CCTV system* berbeda dari ektraksi konvensional bukti digital di komputer. Peralatan sistem kamera pengawas CCTV adalah peralatan yang sifatnya kritis dan ukuran total data di media penyimpan keseluruhannya jauh lebih besar dari pada data yang diperlukan. Dikarenakan hal tersebut sistem pada CCTV memiliki menu untuk penyalinan data nya sehingga tidak perlu mematikan peralatan untuk pengambilan data nya. Oleh karena itu diperkenankan untuk dilakukannya proses akuisisi logikal yang hanya menyalin durasi video tertentu yang diperlukan saja dan artefak lainnya semisal *playback software* untuk *native file* nya.

4.6.3 Retrieval of Video Evidence from Digital CCTV Systems v2.0

Evaluasi selanjutnya dilakukan karena tidak adanya persamaan metode yang diambil untuk mengekstrak data dari perangkat elektronik digital pada tahapan pengumpulan dan akuisisi, oleh karena itu peneliti mengajukan Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0 (ACPO, 2008).

Dokumen ini berisi prosedur langkah tindakan yang diperuntukan bagi pihak investigator yang ingin memahami metode penangan yang sesuai untuk pengambilan video dari perangkat *Digital CCTV System.* Pada dokumen ini diterangkan bagaimana metode untuk mengambil *native file format* dari *digital CCTV system* yang nantinya akan dilabel sebagai *master evidence.* Metode yang diterapkan melalui *checklist of action* suatu langkah kerja yang pengerjaannya harus diikuti secara terurut sehingga data yang diambil nantinya relevan dengan kebutuhan dan integritas barang bukti terjaga. Berikut penjelasan dari *checklist of action.*

a. *Contemporaneous notes*

   Selalau mencatat setiap tindakan yang diambil, untuk mempermudah *audit trail.*

b. *Note the make and model of the CCTV system*

   Mencatat seri model dari sistem peralatan CCTV, jumlah kamera terpasang. Serta juga lakukan fotografi dilokasi tkp.

c. Note the basic system settings

   Hal ini hanya untuk sebagai persiapan bila nanti seting pada sistem CCTV harus dirubah untuk memfasilitasi pengambilan data, sehingga bisa dikembalikan kondisi ny semula.

d. *Time check*

Membandingkan waktu yang ditampilkan oleh CCTV dengan waktu nyata untuk memastikan kesesuain data pada saat di salin, dan bila ada error pada perbedaan waktu di sistem dan waktu nyata harus di catat pada *audit trail*.

e. *Determine time period required*

Memastikan waktu tersedia untuk dilokasi tkp.

f. *Determine which camera views are required*

Memastikan posisi kamera yang merekam dalam gedung dan dalam sistem, kemudian tentukan apakah hasil rekaman dari kamera terebut bisa diambil terpisah bukan hasil rekaman seluruh kamera yang terpasang. Pastikan untuk membuat sketsa posisi kamera untuk membantu pengambilan keputusan.

g. *Replay data*

Memeriksa jika sistem CCTV merekam video kejadian yang dimaksudkan.

h. *Overwrite time*

Memastikan jangka waktu yang tersedia untuk potongan video yang dimaksud tersimpan didalam sistem sebelum data menghilang.

i. *Obtain system password*

Jika perlukan, password admin berkemungkinan diperlukan untuk mengaktifkan akses pengambilan data.

j. *The recording should not be stop during the retrieval process*

Selama proses pengambilan data sistem CCTV tidak harus dimatikan terkecuali fitur yang tersedia didalam sistem mengharuskan.

k. *Protect data*

Hanya bila tersedia oleh sistem CCTV, mengaktifkan fitur *wrire-protecting* terhadap potongan video yang dipilih sebagai upaya perlindungan dari *overwrite*.

l. *Confirm that the data can be retrieved in its native file format*

Mengekstrak potongan file video didalam *native format* atau format *default* yang digunakan oleh sistem CCTV. Untuk menjaga kualitas gambar.

m. *Replay software*

Bila berhasil mengambil *native file* maka diperlukan juga untuk mengambil *replay software* ny, karena *native file* memerlukan player tersendiri.

n. *Confirm success of retrieval*

Melakukan pemeriksaan hasil ekstraksi semua data yang diperlukan telah terpenuhi dan potongan video tersebut bisa diputat di sistem yang berbeda.

o. Restart the CCTV system

Memeriksa potongan video hasil ekstraksi sesuai dengan yang ada ditampilkan oleh monitor sistem CCTV.

p. Complete evidence sheet

Beberapa informasi harus disertakan didalam laporan bukti digital, untuk mempermudah investigator bagian laboratorium saat menganlisis dan memutar video.

q. *Media handling*

Mengkemas media penyimpanan berisi ekstraksi data sesuai dengan kebutuhannya agar tidak rusak saat disimpan.

4.6.4 Evaluasi Framework dengan Dokumen ACPO

Evaluasi yang dilakukan setelah memahami terminologi tahapan yang digunakan didalam ACPO tersebut. ACPO membuat *Checkhlist of Actions* dalam penangannya untuk mengekstrak potongan video yang dinginkan. Maka proses evaluasi yang akan diterapkan ke *framework* hasil rancangan peneliti akan menerepakan *checklist* tersebut untuk memeriksa apakah tahapan yang disebut oleh ACPO telah dipenuhi. Berikut ditampilkan melalui Tabel 4.14 *checklist of action*.

Tabel 4.14 *Checklist of Action*

No	Checklist of action	Terpenuhi	
		Iya	Tidak
1	Contemporaneous notes	✓	
2	Note the make and model	✓	
3	Note the basic system settings	✓	
4	Time check	✓	
5	Determine time period required	✓	
6	Determine which camera views are required	✓	
7	Replay Data	✓	
8	Overwrite time	✓	
9	Obtain system password	✓	
10	The recording should not be stopped during the retrieval process	✓	
11	Protect data		✓
12	Confirm that the data can be retrieved in its native file format	✓	
13	Replay software	✓	
14	Confirm success of retrieval	✓	
15	Restart the CCTV system		✓
16	Complete evidence sheet	✓	
	- Make and model - Error in display time and date - Time period covered by download - Map of camera locations and coverage - Include replay software if available	✓	
17	Media handling	✓	

Pada dokumen ACPO tersebut sama sekali tidak membahas mengenai tahapan Identifikasi dan Preservasi yang diperlukan selama proses investigasi forensik sehingga terdapat banyak perbedaan yang dilakukan dalam mendokumentasikan dan mengamankan data rekaman video CCTV hasil akuisisi.

Berdasarkan *checklist of action* yang telah dilakukan dapat diamati bahwa *First Respond Framwork* untuk Forensik CCTV pada tahapan pengumpulan dan akuisisi untuk mengangkat video tidak ada tahapan krusialnya yang terlewati. Pada tabel diatas terdapat dua kegiatan yang tidak dimiliki oleh *framework* rancangan peneliti, yaitu *Protect data* dan *Restart the CCTV system*.

Hal ini terjadi karena kedua kegiatan tersebut adalah tindakan yang berupa kondisonal yang tidak harus dilakukan terhadap seluruh model *digital CCTV system*. *Restart the CCTV system*. tindakan tersebut tidak dilakukan oleh invstigator karena itu adalah seting dari sistem *digital CCTV system* yang mengharuskan me-*restart* sistem bila ada tindakan pengambilan potongan video. Sedangkan untuk *Protect data* adalah suatu tindakan yang memanfaatkan fitur yang tersedia pada sistem untuk membuat *write-protecting* pada potongan video yang dipilih agar terhindar dari *overwriteen*. Dikarenakan tidak semua *digital CCTV system* memiliki fitur tersebut maka peneliti tidak menambahkan tindakan tersebut kedalam tahapan yang dilakukan.

4.6.5 Hasil Evaluasi Framework

Pada bagian ini akan membahas mengenai hasil evaluasi *framework* untuk mengamati perbandingan yang ada tahapannya bila ditinjau dari *First Respond Framework* untuk Forensic CCTV guna mempermudah proses analisa. *Framework* yang telah dijabarkan akan diberikan kode atau singkatan nama. kode tersebut dapat dilihat pada Tabel 4.15.

Tabel 4. 15 Kode Framework

No	Nama Framework	Kode Framework
1	Insrumen Evaluasi Framework Investigasi Forensik Digital	IEFIFD
2	Retrieval of Video Evidence from Digital CCTV System	RVE-ACPO

Setelah pemberian nama kode *framework,* tahapan berikutnya yaitu melakukan analisa kelayakan *framework*. Pada Tabel Perbandingan dibawah ini akan menampilkan tahapan yang tidak dilakukan oleh *framework* pembanding berdasarkan terminologi. Berikut perbandingan tahapan ditampilkan pada Tabel 4.16.

Tabel 4. 16 Perbandingan Framework

First Respond Framework untuk Forensik CCTV				IEFIFD	RVE-ACPO
1	**Identifikasi**			✓	
	1.1	Pengarahan		✓	
	1.2	Persiapaan dan perencanan		✓	
	1.3	Tindak pencegahan dilokasi kejadian		✓	
	1.4	Penliaian resiko		✓	
	1.5	Pencarian bukti		✓	
		1.5.1	Tipe CCTV		✓
		1.5.2	Fitur CCTV		✓
	1.6	Dokumentasi		✓	✓
2	Pengumpulan			✓	✓
	2.1	Memastikan isi		✓	✓
	2.2	Memastikan kamera		✓	✓
	2.3	Jadwal overwrite		✓	✓
	2.4	Dokumentasi			✓
		2.4.1	Time display		✓
		2.4.2	Metadata		✓
		2.4.3	Native file		✓
	2.5	Keterangan verbal			✓
		2.5.1	Jadwal Maintaince		
		2.5.2	Kontak lokasi	✓	
		2.5.3	Foto sistem		
		2.5.4	Operator pendamping		
3	Akuisisi			✓	✓
	3.1	Tes ambil			
	3.2	Output tersedia			
	3.3	Waktu tersedia			✓
	3.4	Evaluasi output			
	3.5	Live akuisisi		✓	✓
	3.6	Pemeriksaan akusisi		✓	✓
	3.7	Label bukti		✓	
	3.8	Chain of Costudy		✓	✓

Tabel 4. 17 Perbandingan Framework

First Respond Framework untuk Forensik CCTV			IEFIFD	RVE-ACPO
4	Preservasi		✓	✓
	4.1	Verifikasi akusisi	✓	
	4.2	Memberikan segel barang bukti	✓	
	4.3	Dokumen perjalanan	✓	
	4.4	Pemindahan barang bukti	✓	
	4.5	Penyimpanan barang bukti	✓	✓
	4.6	Pemeriksaan aspek keamanan pemindahan barang bukti	✓	
	4.7	Audit trail	✓	✓

Berdasarkan keseluruhan hasil evaluasi yang telah dilakukan, diperoleh bahwa tidak ada proses penting tahapan pada *framework* penelitian yang terlewati berdasarkan standar keperluan untuk investigasi forensik CCTV. Oleh karena itu *framework* ini tidak diperlukan adanya perubahan pada tahapannya.

4.7 Uji Kelayakan Framework

Pada bagian ini, setelah *framework* selesai di evaluasi tahapan berikutnya untuk megetahui apakah hasil penelitian ini mampu memenuhi keperluan penyidik dalam mengangkat barang bukti digital berupa video dari peralatan kamera pengawas CCTV. Dalam melakukan uji ini, dilakukan melalui wawancara yang mengajukan pertanyaan mengenai, pendapat, saran dan masukan dari pihak kepolisian mengenai hasil penelitian dari sudut pandang penydidik, akademisi dan praktisi. Hasil penelitian berupa *First Respond Framework* untuk Forensik CCTV. Apakah telah memenuhi kebutuhan bila dipergunakan pada kasus nyata.

Hasil wawancara ini dipergunakan untuk sebagai evaluasi dalam menyesesuaikan kembali *framework* hasil penelitian terhadap pendapat penyidik untuk menangani kasus CCTV. Wawancara dilakukan dengan terlebih dahulu menyerahkan hasil penelitian kepada pihak kepolisian POLDA D.I.Y untuk dipelajari dulu oleh responden yang berada pada unit Reserse Kriminal Khusus.

Ujicoba untuk melihat kelayakan *framework* hasil penelitian kepada Aparat Penegak Hukum dilakukan oleh Kompol Donny Zuliyanto. Beliau merupakan Kepala Unit I Sub

Direktorat II *Cybercrime* dan Perbankan Direktorat Reserse Kriminal Khusus Kepolisian Daerah D.I.Y.

Adapun hasil validasi terkait kelayakan *First Respond Framework* untuk Forensik CCTV yang didapatkan dari Kompol Donny Zuliyanto menggunakan wawancara bahwa semua tahapan dalam *framework* dapat dilakukan dalam proses penyelidikan secara *scientific* dan hal tersebut dianggap terlalu bertele-tele atau bisa disebut juga terlalu berlarut-larut. Berdasarkan hal tersebut beliau memberikan saran untuk memodifikasi *framework* tersebut menjadi lebih ringkas untuk digunakan dalam pengambilan video dari perangkat sistem kamera pengawas. Adapun hasil wawancara tersebut antara lain:

a. Dalam tahapan utama Identifikasi, mengkolaborasikan beberapa tahapannya menjadi satu tahapan. Tahapan yang dimaksudkan adalah Pengarahan, Persiapan dan Perencanan, tindak pencegahan dilokasi kejadian, penilian resiko. Keseluhan tahapan tersebut menjadi satu tahapan yaitu, Pengarahan. Hal ini dikarenakan pada kasus CCTV tidak berada dalam situasi TKP yang berbahaya dan tidak memerlukan persiapan khusus dan pemilik CCTV bukanlah pelaku kejahatan.
b. Pada tahapan utama Akuisisi, adanya perubahan tahapan yang diambil yaitu tahapan *possible output, amount of time, evaluation of output*, tahapan tersebut tidak diperlukan karena pada penyilidikan yang dilakukan oleh POLRI tidak terpengaruh oleh biaya dan waktu durasi di TKP. Sehingga tahapan ini diubah untuk mendukung keaslian hasil akuisisi yang diambil nantinya, tahapan tersebut adalah merekam monitor dan saksi akuisisi. Kemudian pada proses yang *logical* akusisi diubah namanya menjadi *live* akusisi.
c. Pada tahapan dokumentasi ditambahkan keterangan untuk mencatat tindakan yang diambil selama penyelidikan. Hal ini dimaksudkan agar tindankan yang diambil oleh penyidik dapat diamati secara kronologis.

Adapun hasil validasi terkait kelayakan *First Respond Framework* untuk Forensik CCTV yang didapatkan dari Mukhlis Prasetyo beliau adalah seorang dosen dari Universitas Muhammadiyah Purwokerto dan juga seorang praktisi forensik digital *Private Investigator* menggunakan kuesioner memberikan pendapat bahwa semua tahapan dalam *framework* cukup panjang tetapi mudah untuk diikuti. Berdasarkan hal tersebut beliau memberikan saran untuk menyederhanakan proses sehingga langkahnya lebih cepat.

Pendapat ahli berikutnya adalah dari Josua Sinambela beliau adalah seorang praktisi dari rootbrain.com yang bergerak dibidang keamanan dan forensik digital. Melalui kuesioner

yang diserahkan kepada beliau diperoleh pendapat, masukan dan saran terkait uji kelayakan *framework* penelitian. Beliau menjawab bila bisa memahami alur proses *framework* dan bisa diterapkan bila digunakan pada kasus yang melibatkan CCTV. Akan tetapi beliau menyarankan untuk menyederhanakan kembali alur tahapan yang digunakan.

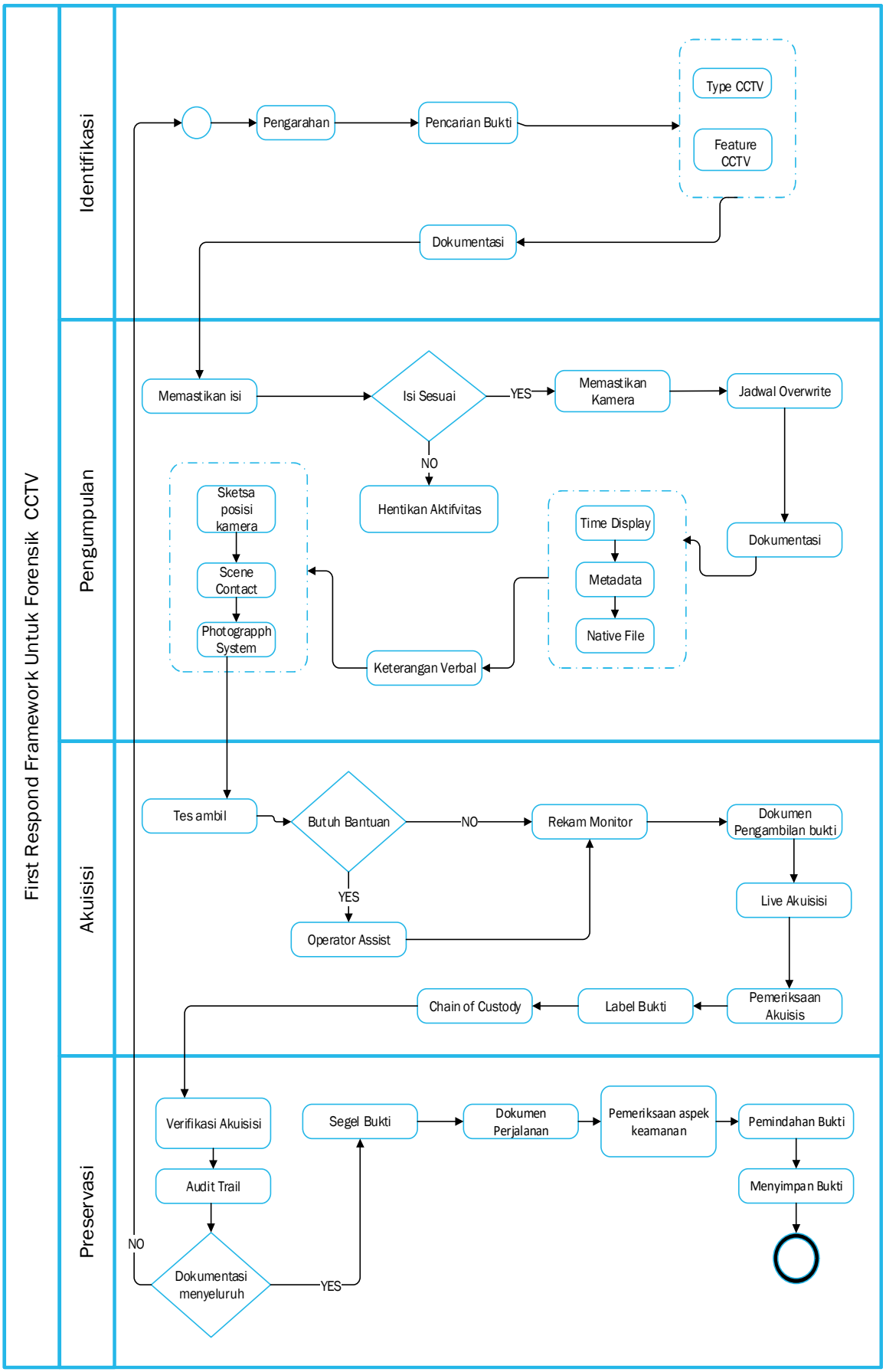
4.7.1 Perbaikan Framework Berdasarkan Hasil Wawancara

Melalui hasil wawancara terkait ujicoba *framework* menurut pendapat ahli bila digunakan pada kasus nyata, dirangkum beberapa perubahan yang dilakukan terhadap *framework*. Perbaikan akan ditampilkan kedalam tabel agar mudah dalam mengamati, berikut ditampilkan rangkuman perbaikan dalam Tabel 4.18.

Tabel 4. 18 Rangkuman Perbaikan

No	Jenis Perbaikan	Tahapan Diperbaiki	Keterangan
1	Perubahan tahapan Identifikasi	Pengarahan	Keseluruhan tahapan tersebut menjadi 1 tahapan "Pengarahan"
		Persiapan dan Perencanaan	
		Tindak pencegahan dilokasi kejadian	
		Penilaian resiko	
2	Perubahan tahapan Akusisi	• *Output* tersedia • Waktu tersedia	Keseluruhan tahapan tersebut diubah menjadi tahapan rekam monitor
		Evaluasi output	Menjadi tahapan dokumen pengambilan bukti dan ada nya saksi yang menyaksikan proses pengambilan video.
3	Perbaikan penjelasaan tahapan	Dokumentasi	Mencatat tindakan yang dilakukan selama di TKP.

Berdasarkan tabel rangkuman tersebut, maka dilakukan perbaikan *framework* menyesesuaikan dengan kebutuhan penyelidik dalam melalukan pengambilan bukti digital berupa rekaman video dari perlatan CCTV. Hasil perbaikan dapat dilihat pada gambar dibawah ini.



Gambar 4. 4 First Respond Framework Untuk Forensik CCTV Hasil Perbaikan

Adapun penjelasaan dari alur tahapan yang terdapat dalam diagram diatas hasil perbaikan *framework* penelitian ini antara lain:

a. 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:

1 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.

2 Pencarian bukti: Merupakan proses pencarian barang bukti di sekitar lokasi kejadian yang bisa menjadi bukti potensial.

3 Type CCTV: Mengetahui jenis dvr yang digunakan *stand alone* atau *pc based* dan mengetahui *serial number.*

4 Feature CCTV: Fitur yang terpasang pada dvr, seperti *multiplexer, transactional data, network capabilitis*

5 Dokumentasi: Mencatat temuan yang diperoleh selama proses pencarian. Mencatat/dokumentasi dari jenis peralatan dan seting waktu yang tertera *uniquei identifier,* siapa yang mengkases, siapa yang memeriksa. Megumpulkan informasi terkait kondisi *system setting* peralatan CCTV, seperti model dan *serial number, multiplexer model, playback software name password and version.*

b. Pengumpulan

Setelah peralatan digital yang berkemungkinan berisi bukti digital potensial teridentifikasi. Investigator harus menentukan untuk melanjutkan atau tidak ke proses selanjutnya.

a. Memastikan isi: Memeriksa hasil rekaman untuk memastikan bahwa peristiwa /kejadian 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,fps, 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. Scene Contact: 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. Photograph system: Foto sistem bagian depan dan belakang.

c. Akuisisi

Suatu proses yang membuat *copy* atau salinan dari bukti digital 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* nya.
b. Operator assist: Mencari tahu siapa yang menjadi operator pada sistem CCTV tersebut. Hanya bila investigator tidak mampu atau tidak memahami sistem maka diperlukan ada nya operator atau admin dari kamera pengaswas yang mendampingi proses pengambilan file video.
c. Rekam Monitor: merekam layar monitor untuk meperoleh video mengenai kronologis tindakan yang dilakukan saat pengambilan video.
d. Dokumen pengambilan bukti: membuat surat berita acara pengambilan rekaman video kepada pemilik atau operator CCTV dan meminta mereka menjadi saksi saat pengambilan video.

e. Live akuisisi: melalukan metode *live* akuisis untuk mengambil rekaman video dari CCTV dikarenakan peralatan tidak perlu dimatikan 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 custdy: Mencatat kedalam dokumen investigasi terkait kronologi dari penangan untuk pengangkatan barang bukti. Disertakan pula dengan berita acara pengambilan barang bukti.

d. 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 modifikasi sejak diperoleh.

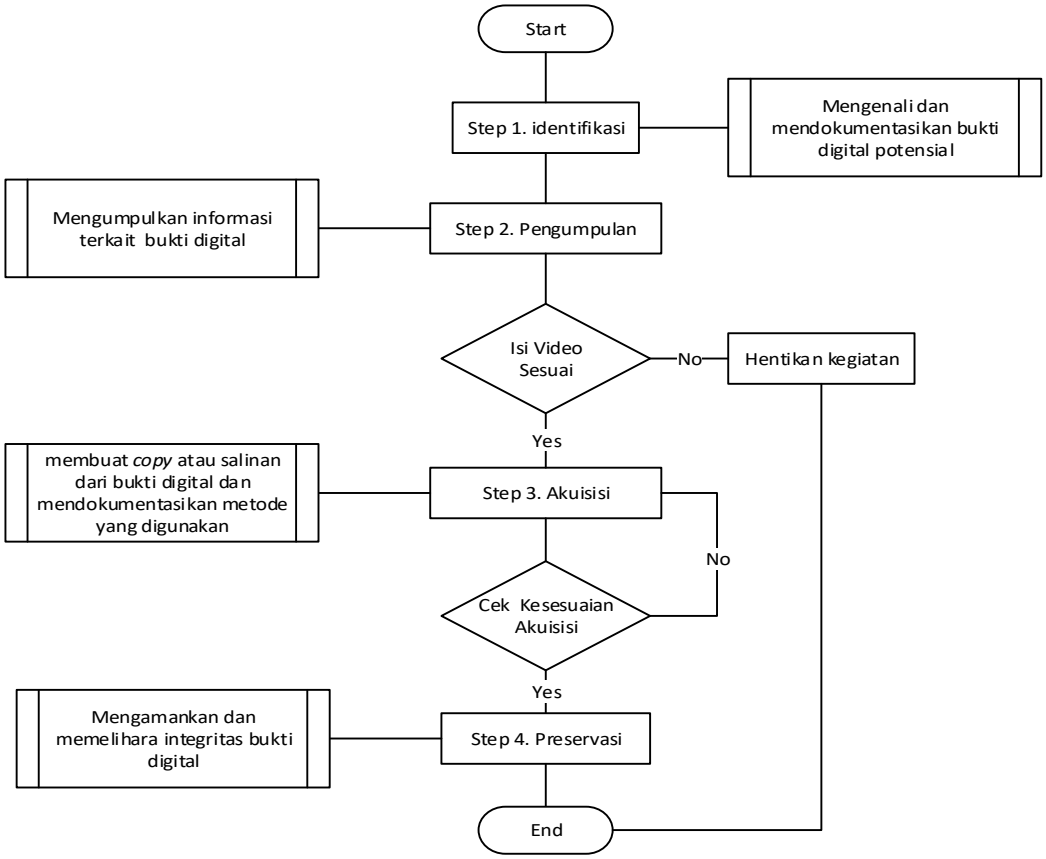
a. Verifikasi akusisisi: Menggunakan fungsi verifikasi sebagai segel keaslian pada *master evidence* seperti *digital signature* berupa nilai *hash* dari alogoritma md5. Serta juga mengatifkan fungsi *write protector* untuk menghasilkan preservasi yang menjamin kerahasian, keutuhan dan ketersedian.
b. Audit Trail: Memeriksa kembali dokumen apakah telah mencatat detail tindakan yang dilakukan. Hal ini bertujuan untuk mempermudah bila adanya permintaan investigasi ulang oleh investigator yang berbeda.
c. Segel barang bukti: Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.
d. Dokumen perjalanan: Menyiapakan dokumen atau surat perjalan untuk perpindahan bukti digital dari penyidik kepada labortorium atau ruang penyimpanan untuk mematikan keamanannya maka juga harus diterangkan pada *Chain of Cutody.*
e. 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.

f. Pemindahan barang bukti: Selama 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.
g. 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.

Setelah dilakukannya perbaikann penyesesuaian berdasarkan saran yang diperoleh terhadap *framework* pada penelitian ini. Maka penelitian yang dilakukan untuk menghasilkan *First Respond framework* untuk Forensik CCTV yang telah memenuhi seluruh ketentuan terhadap SNI/ISO 27037:2014 selesai dilakukan. Sebagai penutup, dengan adanya *framework* ini diharapkan dapat digunakan sebagai acuan ketika terkait kasus CCTV.

4.8 Ilustrasi Penggunaan Framework

Pada bagian ini, untuk mempermudah dalam memahami penggunan *framework* maka akan dijelaskan secera sederhana mengenai alur penggunan *first respond framework* untuk forensik CCTV melalui sebuah alur *flowchart* yang dapat diamati pada Gambar 4.5 dibawah ini.



Gambar 4.5 Ilustrasi Penggunaan Framework

Melalui gambar *flowchart* diatas maka dapat dilakukan penjelaskan ilustrasi pengggunaan *framework* yang telah dibangun 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 dibawah ini penjelasan *flowchart* dari gambar 4.4.

Step 1. Idenifikasi

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.

Step 2. Pengumpulan

Setelah peralatan digital yang berkemungkinan berisi bukti digital potensial teridentifikasi. Investigator menggali informasi yang terkandung didalam *digital CCTV system* untuk menemukan keterkaitan nya dengan perkara yang terjadi, dalam hal ini investigator 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.

Step 3. Akuisisi

Suatu proses yang membuat copy atau salinan dari bukti digital dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan. Investigator harus mengaplikasikan metode akuisisi berdasarkan situasi, biaya dan waktu, dan tools yang tersedia.

Step 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 modifikasi sejak diperoleh.

4.9 Simulasi Penggunaan Framework

Pada bagian ini akan dilakukan simulasi penggunaan *First Respond Framework* untuk forensik CCTV guna membantu dalam menjelaskan bagaimana alur tahapan forensik untuk mengangkat rekaman video dari peralatan kamera pengawas CCTV. Simulasi dilakukan digedung kantor milik Pondok Pesantren As'ad yang telah terpasang peralatan CCTV yang tidak menggunakan fitur *motion detection* sehingga selalu aktif merekam. Pada simulasi ini tidak menggunakan skenario karena aktifitas yang dilakukan berfokus untuk mengakusisi rekaman video dengan menerapkan tahapan yang telah disusun pada *framework* penelitian.

Sebagaimana yang telah dijabarkan sebelumnya pada bagian ilustrasi penggunaan *framework* bahwa terdapat 4 bagian tahapan utama yang dilakukan secara berurutan dimulai dari Identifikasi, Pengumpulan, Akuisisi dan Preservasi. Oleh karena itu simulasi yang dilakukan juga akan mengikuti alur forensik tersebut. Tahapan yang dilakukan meliputi hal berikut ini.

4.9.1 Pelaksanaan Simulasi Tahapan Identifikasi

Langkah awal yang dilakukan untuk pelaksaan simulasi dimulai dari tahapan utama Identifikasi yang bertujuan untuk mengenali dan mendokumentasikan bukti digital potensial yang mungkin megandung bukti digital potensial yang relevan dengan kasus yang dihadapi. Berikut proses penting yang dilakukan untuk tahapan Identifikasi.

a. Pengarahan

Proses penting yang dilakukan terlebih dahulu adalah pengarahan. Dimana bertujuan untuk menyampaikan atau memberikan arahan mengenai investgasi yang dilakukan. Skenario untuk simulasi pengarahan yang dilakukan yaitu memperoleh bukti keterlibatan oknum pada peristiwa pencurian yang dilakukan dilingkup area Ponpes As'ad dari perangkat kamera pengawas CCTV dan pihak penyidik yang diterjunkan kelapangan diminta mempersiakan peralatan kebutuhan yang diperlukan untuk akusisi rekaman video CCTV. Peralatan akusisi yang dibawa ke lokasi berupa Laptop, flashdisk, Hardisk eksternal dan Handycam atau kamera.

b. Pencarian Bukti

Setelah pengarahan telah disampaikan penyidik dilokasi segera melakukan proses pencarian posisi alat rekam CCTV berupa Digital Video Recorder (DVR) yang merupakan alat eletronik yang difungsikan untuk merekam dan menyimpan tangkapan gambar yang berasal dari kamera CCTV yang terpasang. Begitu diketahui posisinya proses selanjutnya yaitu mencari tahu perlatan yang digunakan.

1. **Tipe CCTV**

   Mengetahui jenis DVR yang digunakan *PC Based* atau *Stand Alone* dan *serial number.*

   Jenis : Stand Alone

   Merek : BXS-8216

   Serial Number : bxs002***

Gambar 4. 6 Tipe DVR

2. **Fitur CCTV**

   Mengetahui fitur yang terpasang pada DVR seperti *multiplexer, network capabilities,* dan fitur atau alat lainya yang disandingkan dengan peralatan DVR.

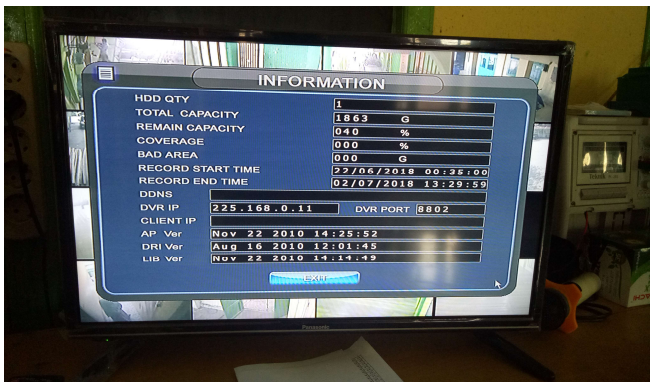
   Multiplexer : 16 Channel

Network terhubung : iya,ip 225.168.0.11 port 8.8.0.2

Transactional data : USB

Penyimpanan : HDD 2 TB

Gambar 4. 7 Fitur multiplexer 16 channel



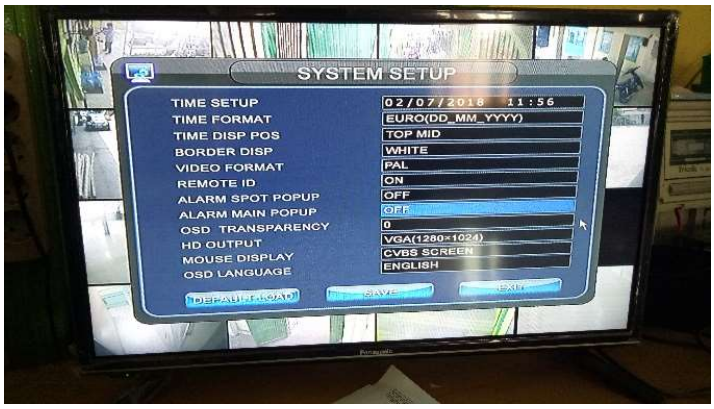
Gambar 4. 8 Informasi DVR

c. Dokumentasi

Mencatat temuan dan informasi semua yang terkait selama proses pencarian bukti seperti kondisi seting sistem dan penyidik yang mengakses. Berikut dokuemtasi yang diperlukan.

Siapa yang mengakses : Danang Mulyadipa

Seting sistem terpasang : Telah didokuemntasikan



Gambar 4. 9 Seting Sistem

4.9.2 Pelaksanaan Simulasi Tahapan Pengumpulan

Peralatan digital yang berkemungkinan berisi bukti digital potensial selesai diidentifikasi. Penyidik harus menetukan untuk melanjutkan atau tidak ke proses selanjutnya.

a. Memastikan Isi

Memeriksa rekaman DVR untuk memastikan bahwa peristiwa relevan terkait kasus yang ditangani telah terekam pada tanggal berapa serta lama durasi. Bila penyidik tidak memahami bagaimana mengoperasikan alat DVR maka disarankan untuk meminta bantuan operator.

Kronologi isi video : Terlihat ciri-ciri atau kegiatan oknum terduga pelaku

Gambar 4. 10 Video menerangkan peristiwa terjadi

b. Memastikan Kamera

Bila rekaman video tersebut berisi peristiwa yang dimaksudkan maka lanjutkan tahapan forensik. Setelah memeriksa video lanjutkan dengan memastikan kamera yang merekam dan posisi kamera tersebut berada.

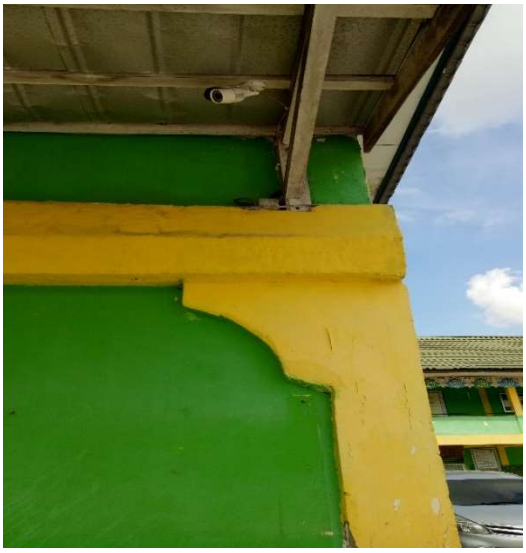
Video relevan : Channel 8

Nomor Kamera : Kamera 8

Posisi Kamera : Gerbang masuk

Gambar 4. 11 Channel di monitor DVR

Foto Channel di monitor DVR



Gambar 4. 12 Posisi kamera

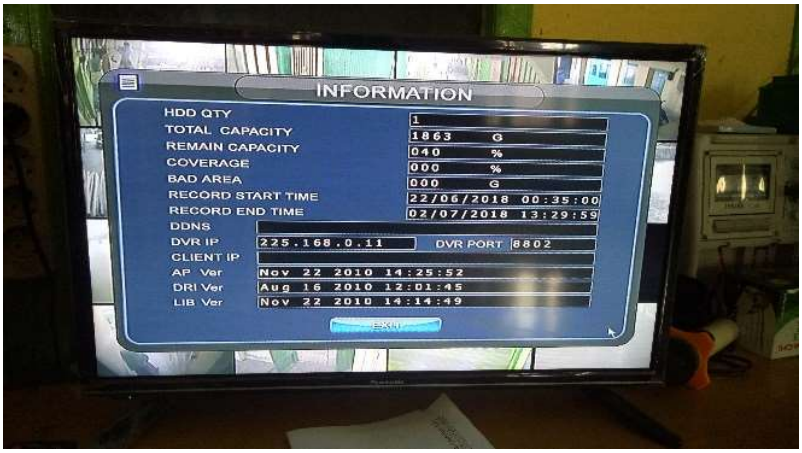
c. Jadwal *Overwrite*

Memastikan waktu tersedia sebelum rekaman video terhapus dengan mengetahui tanggal waktu rekaman terakhir dan tanggal rekaman terbaru. Hal ini dimaksudkan apabila pihak yang berada dilokasi tidak ada yang bisa melakukan akuisisi nantinya bisa mengambil keputusan untuk meminta bantuan dari pihak yang melakukan instalasi peralatan CCTV atau menyita DVR.

Record Start : Tanggal 22/06/2018 Pukul 00:35:00

Record End : Tangal 02/07/2018 Pukul 13:29:59

Estimimasi : Tersisa 20 hari menjelang rekaman video terhapus



Gambar 4. 13 Kumpulan Rekaman

d. Dokumentasi

Mencatat temuan yang diperoleh selama proses berinteraksi dengan DVR.

1. Time Display

Mencatat waktu tertampil dalam rekaman untuk memastikan waktu kejadian yang sesungguhnya.

Waktu kejadian : 29 Juli 2018 Pukul 15:00 WIB

2. Metadata

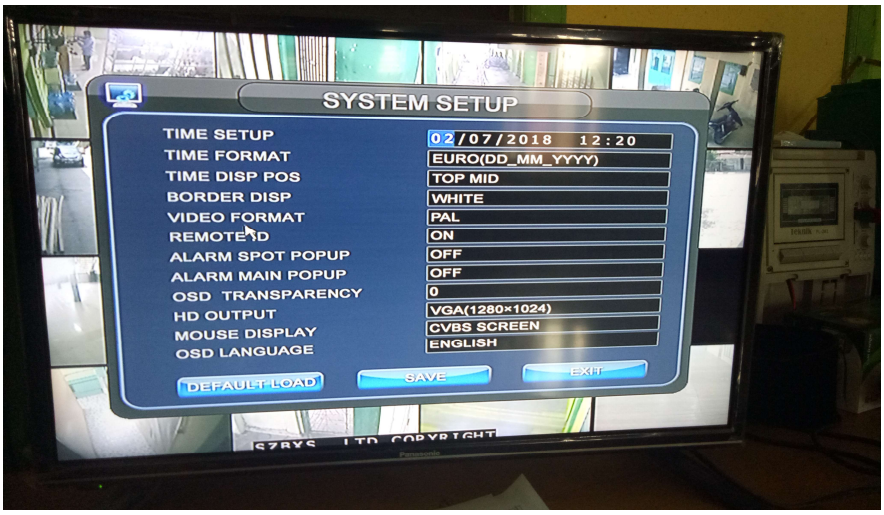
Mencatat informasi tersedia terkait dengan rekaman tersebut.

Video Format : PAL

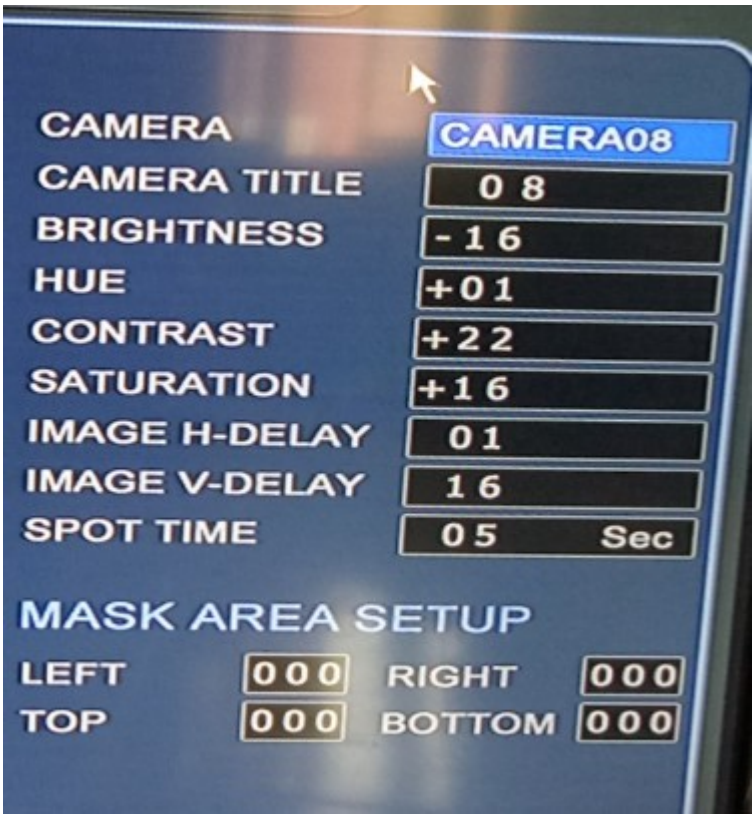
Resolusi dimonitor : VGA

Resolusi video : 1280x1024

Password DVR : Tidak diketahui



Gambar 4. 14 Sistem Setup



Gambar 4. 15 Seting Kamera

3. **Native File:**

   Mencari tahu format file yang digunakan oleh DVR. Hal ini dimaksudkan untuk membantu pihak labortorium nantinya saat menganalisis rekaman lebih jauh.

   Native File : tersedia format .avh

   Format lainnya : tidak tersedia

   Playback software : tersedia

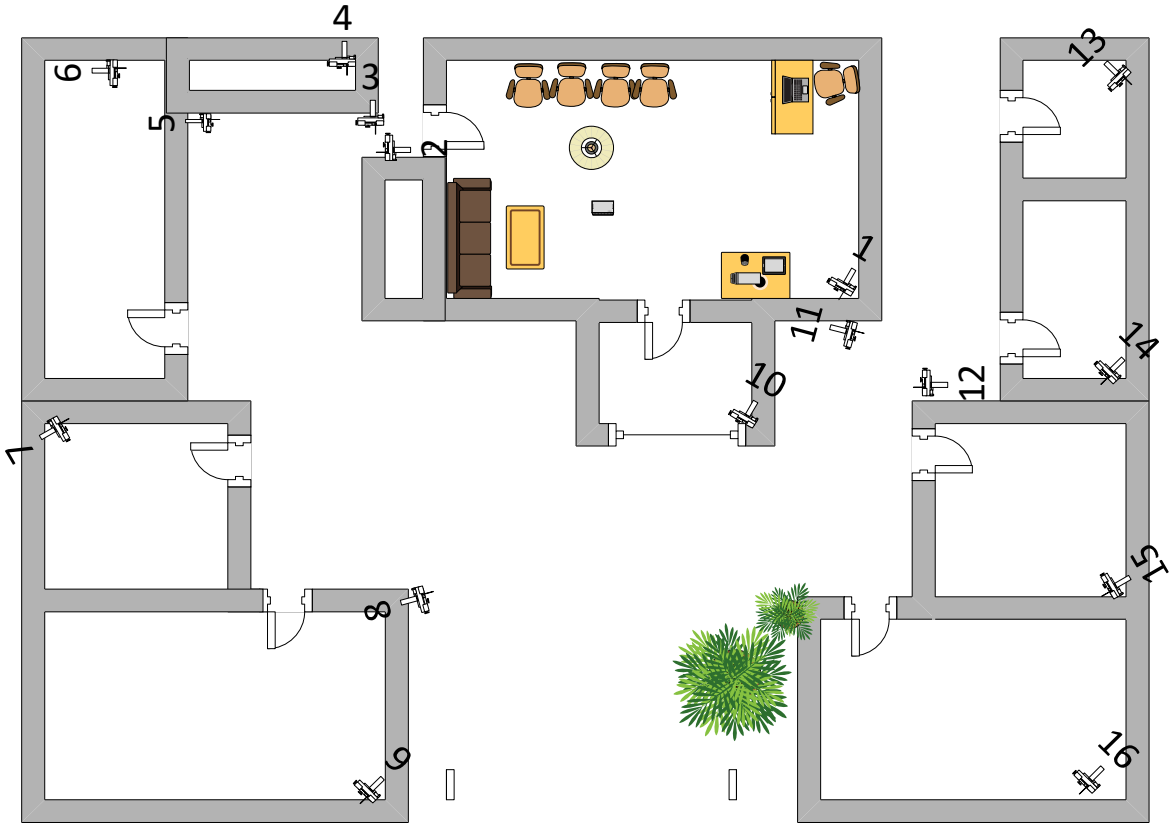
e. Keterangan Verbal

Keterangan verbal dimaksudkan untuk mengetahui informasi lebih terperinci untuk diserahkan kepihak labor nantinya bila dibutuhkan.

1. **Sketsa Posisi Kamera**

   Memastikan posisi kamera terpasang sesuai dengan rekaman.

   Posisi kamera: seluruh kamera berada pada sudut lorong bangunan



Gambar 4. 16 Sketsa posisi kamera

2. **Kontak Lokasi**

   Memperoleh kontak operator yang bertanggung jawab atas peralatan CCTV bila nantinya diperlukan.

   Nama operator: Ust. Umar

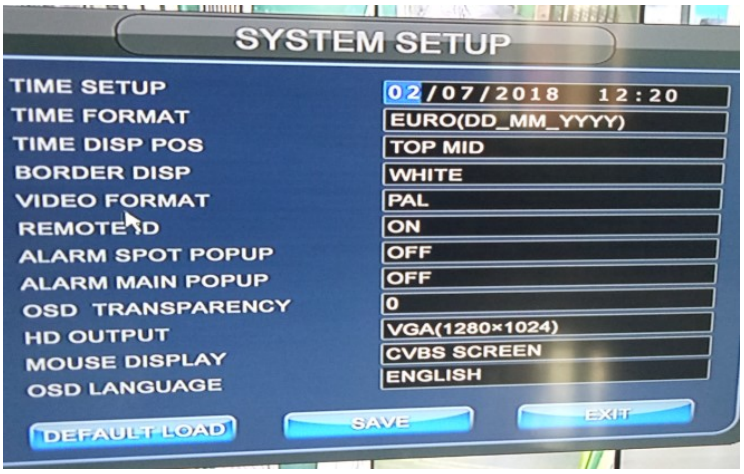
   Nomor HP: 0853****2000

3. **Foto Sistem**

   Memfoto atau merekam untuk mencatat sebagai pegangan bila nantinya harus merubah seting konfigurasi DVR saat mengambil rekaman video.

   Seting Sistem DVR : Default

   Seting Kamera : brightness -16, Hue +01, Contrast +22, Saturation +16



Gambar 4. 17 Seting Setup

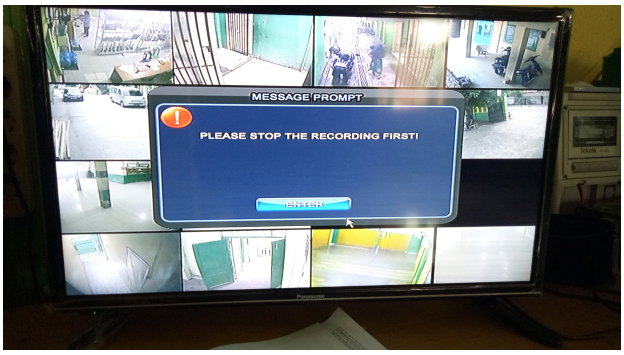
Gambar 4. 18 Seting Kamera

4.9.3 Pelaksanaan Simulasi Tahapan Akuisisi

Pada tahapan ini penyidik membuat salinan dari bukti digital dan mendokumentasikan tindakan yang dilakukan.

a. Tes Ambil

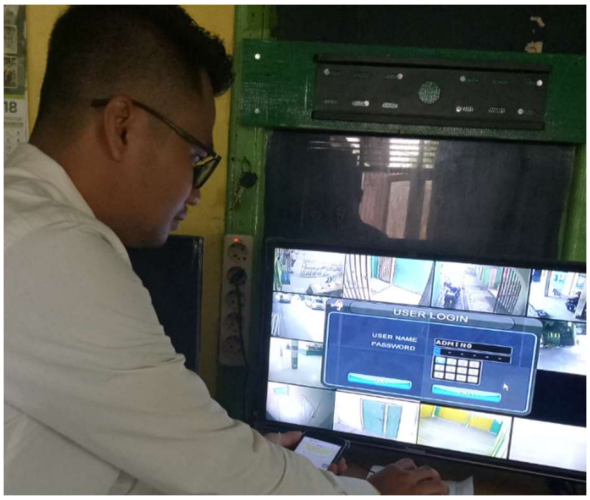
Melakukan uji pengambilan rekaman apakah penyidik mampu mengoperasikan DVR untuk melakukan pengambilan video. Bila mampu maka lakukan akuisisi. Pada saat akan mengakses menu back up terjadi kendali tidak biaa diakses atau sisem tidak merespon maka diperlukan pendampingan dari operator.



Gambar 4. 19 Tes Ambil

b. Operator Pendamping

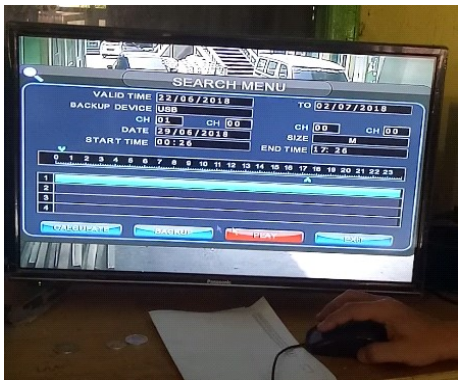
Bila penyidik tidak mampu atau adanya larangan pihak luar untuk mengoperasikan maka diperlukan bantuan operator untuk melakukan akuisisi.



Gambar 4. 20 Dampingan Operator

c. Rekam Monitor

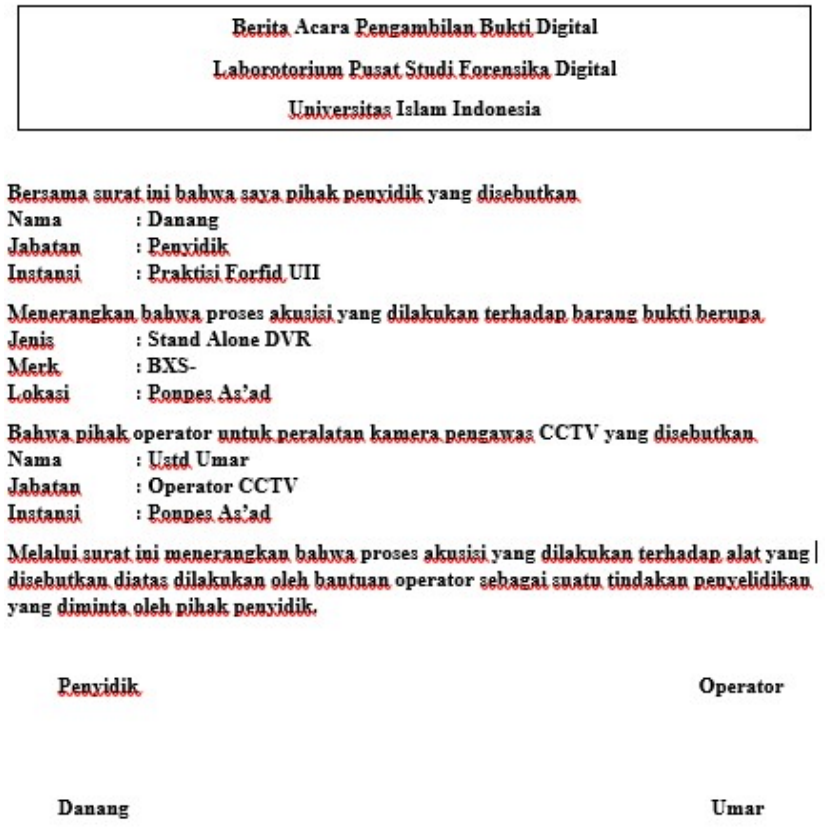
Merekam kegiatan yang dilakukan selama proses akuisisi untuk mempermudah proses *audit trail* memahami kronologi tindakan yang diterapkan bila nantinya diperlukan.



Gambar 4. 21 Merekam aktifitas yang dilakukan

d. Dokumen Pengambilan Bukti

Membuat surat berita acara yang menerangkan pengambilan rekaman video dan meminta pemilik atau operator untuk menjadi saksi pengambilan. Hal ini bersifat kondisonal, dilakukan bila berkemungkinan dibutuhkan karena proses akusisi dilakukan oleh pihak operator.



Berita Acara Pengambilan Bukti Digital

Laborotorium Pusat Studi Forensika Digital

Universitas Islam Indonesia

Bersama surat ini bahwa saya pihak penyidik yang disebutkan
Nama : Danang
Jabatan : Penyidik
Instansi : Praktisi Forfid UII

Menerangkan bahwa proses akusisi yang dilakukan terhadap barang bukti berupa
Jenis : Stand Alone DVR
Merk : BXS-
Lokasi : Ponpes As'ad

Bahwa pihak operator untuk peralatan kamera pengawas CCTV yang disebutkan
Nama : Ustd Umar
Jabatan : Operator CCTV
Instansi : Ponpes As'ad

Melalui surat ini menerangkan bahwa proses akusisi yang dilakukan terhadap alat yang disebutkan diatas dilakukan oleh bantuan operator sebagai suatu tindakan penyelidikan yang diminta oleh pihak penyidik.

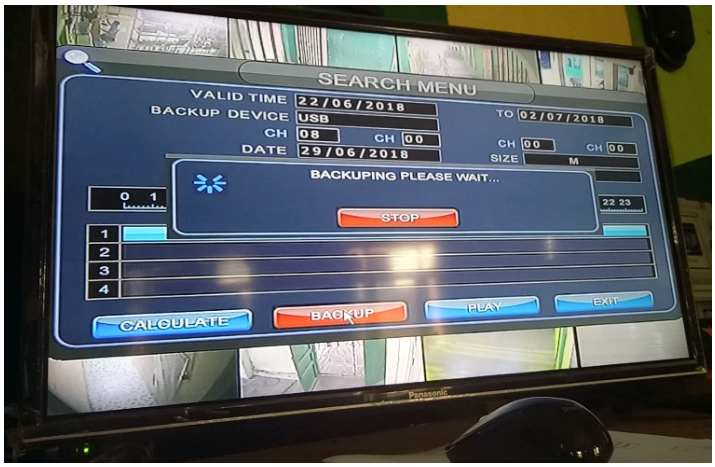
Penyidik **Operator**

Danang **Umar**

Gambar 4. 22 Contoh Surat Pengambilan Bukti

e. Live Akuisisi

Melakukan live akusisi terhadap DVR dikarenakan peralatan tidak perlu dimatikan dan tidak mengambil keselurahan data. Bila memungkinkan maka lakukan tindakan perekaman proses akusisi sebagai tindakan untuk mempermudah *audit trail*.



Gambar 4. 23 Rekam Pengambilan Potongan Video

f. Pemeriksaan Akuisisi

Memeriksa hasil akusisi sesuai dengan yang diinginkan.

Nama folder : AnaVideo

Format file : .avh dan .avd

Playback Software : tersedia

Jumlah file : 5 file berformat .avh dan 5 file berformat .avd

File akses date/time : 2018:07:25 09:37:51+07:00

File creation date/time: 2018:07:25 09:37:51+07:00

Name	Date modified	Type	Size
playback	02/07/2018 13:01	File folder	
20180629_140200.avd	02/07/2018 13:04	AVD File	137.550 KB
20180629_140200.avh	02/07/2018 13:04	AVH File	342 KB
20180629_142902.avd	02/07/2018 13:06	AVD File	137.791 KB
20180629_142902.avh	02/07/2018 13:06	AVH File	341 KB
20180629_145606.avd	02/07/2018 13:09	AVD File	135.619 KB
20180629_145606.avh	02/07/2018 13:09	AVH File	339 KB
20180629_152256.avd	02/07/2018 13:11	AVD File	134.343 KB
20180629_152256.avh	02/07/2018 13:11	AVH File	342 KB
20180629_154958.avd	02/07/2018 13:12	AVD File	48.887 KB
20180629_154958.avh	02/07/2018 13:12	AVH File	127 KB

Gambar 4. 24 Hasil Akusisi

g. Label Bukti

Memberikan label bukti terhdap media penyimpanan hasil akusisi sebagai *master digital evidence copy*.

h. Chain of Custody

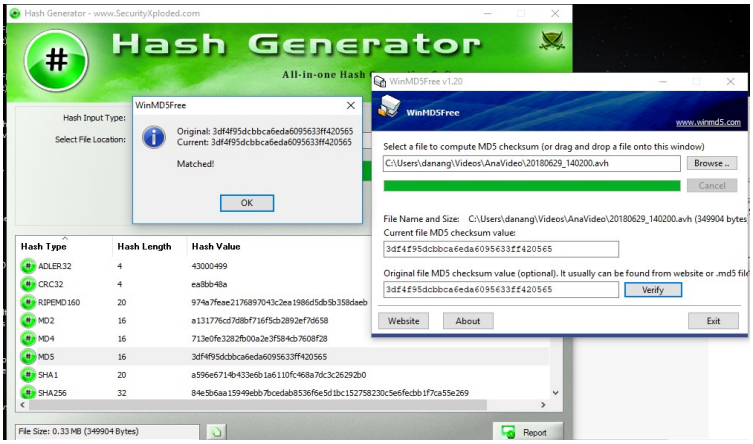
Catatan dokumentasi barang bukti, sejak barang bukti ditemukan ditempat kejadian perkara sampai proses duplikasi, dan penyimpanan.

4.9.4 Pelaksanaan Simulasi Tahapan Presrvasi

Setelah akusisi dilakukan maka selanjtnya dilakukan tahapan preservasi atau pemiliharaan untuk menjaga kondisinya tetap utuh sehingga mampu menunjuka bahwa tetap utuh semenjak diperoleh.

a. Verifikasi Akusisi

Mengunanakan fungsi verifikasi seperti *hash* pada data hasil akuisisi dan fungsi *write blocker* untuk menjamin keutuhan, ketersedian dan keasliannya.



Gambar 4. 25 Pemasangan Fungsi Hash

Gambar 4. 26 Pemasangan Fungsi Writeblocker

b. Audit Trail

Memeriksa kembali tindakan yang telah dilakukan apakah terdapat bagian yang terlewati.

.

c. Segel Bukti

Memberikan atau membungkus *master evidence* dalam suatu kemasan untuk menjaga integritasnya.

Gambar 4. 27 Kemasaan Flashdisk

d. Dokumen Perjalanan

Menyiapkan dokumen perjalanan atau bisa melakukan *update* pada form CoC yang berisi informasi mengenai pemberi dan penerima bukti.

e. Pemeriksaan Aspek Keamanan

Memeriksa aspek keamanan barang bukti tetap dalam kondisi aman selama proses pemindahaan. Karena media penyimpanan hasil akuisisi berupa flashdisk sehingga tidak memerlukan keamanan khusus untuk menjaganya dari kerusakan karena factor eksternal.

f. Pemindahaan Bukti

Pastikan Memindahkan bukti dari lokasi ke labortorium atau ruang penyimpanan atau ke pihak yang telah ditentukan sebelumnya. Lakukan update di form CoC

g. Menyimpan Bukti

Barang bukti berupa *master evidence* yang diperoleh disimpan diruang khusus untuk menjaga integritasnya bila dipertanyakan. Lakukan update di form CoC

4.9.5 Pelaksanaan Simulasi Tahap Chain of Custody

Ketika telah melaksanakan investigasi dilokasi maka diperlukan upaya dokumentasi barang bukti sejak ditemukan sampai proses duplikasi dan penyimpanan barang bukti tersebut. *Chain of Custody* menjadi hal yang penting bagi penyidik karena untuk menjaga keaslian barang bukti digital sehingga pada saat dipersidangan bukti yang diajukan tidak akan diragukan karena terdokumentasi dan tidak ada unsur manipulasi terhadap barang bukti.

Simulasi menggunakan *framework* hasil penelitian ini telah bisa menjawab kebutuhan dari karakteristik CoC yang diperlukan yaitu keaslian, kelengkapan, dan dapat dipercaya. Oleh karena itu akan dibuat form CoC untuk menyesesuaikan dengan hasil investigasi. Pada penulisan untuk dokumen *Chain of Custody* tidak ada standar baku yang harus diikuti oleh karena itu bisa menggunakan bentuk form CoC yang berbeda. Walaupun tidak ada standar baku untuk diikuti akan tetapi tidak bebas membuatnya karena CoC harus mampu menjelaskan siapa saja pihak yang terlibat saat investigasi, tindakan yang dilakukan, temuan yang diperoleh dan bagaimana memperlakukan temuan tersebut, siapa yang betanggung jawab atas investigasi, kepada siapa di serahkan. Adapun contoh *Chain of Custody* yang dapat digunakan untuk keperluan investigasi seperti gambar dibawah ini.

Formulir Chain of Custody
Laborotorium Pusat Studi Forensika Digital
Universitas Islam Indonesia

Informasi Kasus			
Nomor Kasus	14***	**Tanggal**	10 Juli 2018

Pengambilan Barang bukti			
Nomor barang bukti	1	**Tangal**	10 Juli 2018
Lokasi	Ponpes As'ad	**Jam**	14:00 WIB

Petugas Penanggung Jawab Barang Bukti			
Nama	Danang	**Jabatan**	Penyidik
Lembaga	Pusfid	**No Telepon**	0853***

Deskripsi Barang Bukti			
Jenis Barang Bukti	Flashdisk	**Model**	----------
Nomor serial	----------	**Merek**	Toshiba
Kondisi	Write protected	**Keterangan lain**	Master Evidence

Perpindahan Barang Bukti			
Tanggal	10 Juli 2018	**Lokasi**	**Labortorium Pusfid**
Diserahkan Oleh		**Diterima Oleh**	
Nama	Danang	**Nama**	Fulan
Jabatan	Penyidik	**Jabatan**	Laboran Pusfid
Tanda tangan	----------	**Tanda tangan**	----------
Keterangan	Master evidence yang berisi 10 rekaman video dan 1 *playback software* hasil akusisi perangkat CCTV berformat .avh		
	Nomor hash : 3df4f95dcbbca6eda6095633ff420565 7afe53ad98dc55134ba98672f8fa719f 8f60147db4fa2e01656483e66ba049b5 a126eb144eaee33c4466501b757ce5b1 75f071ea84e6f98a31848e48cc8b6e0e		

Gambar 4. 28 Chain of Custody

Berdasarkan isi dokumen *Chain of Custody* yang diperoleh dari dokuemntasi yang dilakukan selama proses forensik menggunakan *First Respond Framework* untuk CCTV tersebut dapat diamati bahwa proses penting untuk forensik CCTV telah memenuhi standar yang berlaku dan kebutuhan penyidik bila digunakan untuk menyelsaikan kasus nyata. Dimana dapat membimbing investigator untuk melakukan kegiatan forensik untuk memperoleh bukti digital berupa rekaman CCTV yang dapat menunjukan proses forensik yang dilakukan dan bukti keaslian dari rekaman CCTV tersebut sebagai bukti digital dihadapan pengadilan.

BAB V
Kesimpulan

5.1 Kesimpulan

Kesimpulan yang dapat disimpulkan dari penelitian yang dilakukan adalah:

a. Berdasarkan hasil penelitian diperoleh kesimpulan bahwa metode *Logical Framework Approach* dapat diterapkan dalam menyusun sebuah *framework* forensik untuk penanganan bukti digital berupa kamera pengawas CCTV, dengan cara menggunakan *Logframe* matrik untuk melakukan perincian perencanaan dan evaluasi sehingga diperoleh alur penelitian yang terstruktur untuk memperoleh First Respond Framework untuk Forensik CCTV yang sesuai dengan ketentuan standar yang berlaku.
b. Berdasarkan hasil kolaborasi yang dilakukan terhadap dokumen SNI dan SWGIT diperoleh tahapan proses penting yang menjadi alur investigasi forensik yang menjadi *First Respond Framework* untuk forensik CCTV. Kolaborasi yang dilakukan adalah menggabungkan proses penting investigasi forensik terhadap CCTV dari dokumen SNI dan SWGIT. Setiap framework memiliki penamaan dan urutan tahapan forensik yang berbeda oleh karena itu perlu untuk diidentifikasikan terlebih dahulu proses penting terkait forensik CCTV untuk first responder yang terdapat pada masing-masing dokumen berdasarkan dari penjelsaan terminologi nya. Dimana pada proses penggabungan tersebut, sebelumnya mengklasifikasikan proses penting yang ada pada pada tiap tahapan dari dokumen SWGIT menggunakan *role mode implies, prohibit* dan *don't care* berdasarkan terminologinya. Pada proses ini, tahapan yang memiliki penjelasan terminologi yang sama dinyatakan sebagai *implies* sehingga tahapan tersebut dijadikan satu agar tak membuat bingung pengguna dan tahapan dengan *role model* lainya dianggap proses penting yang dijadikan sebagai tahapan investigasi.
c. Perbaikan yang dilakukan *First Respond Framework* untuk Forensik *CCTV* dengan cara membandingkan tahapannya dengan dokumen best practice ACPO dan dokumen instrument evaluasi *framework* kemudian mevalidasinya kepada akademisi, praktisi dan penyidik. Hasil evaluasi menunjukan bahwa *framework* ini telah mengakomodir semua tahapan yang terdapat pada instrument evaluasi terkait

forensik *CCTV* yang dijadikan bahan kajian dalam penelitian ini. Serta mampu memenuhi kebutuhan penyidik bila digunakan pada kasus nyata.

5.2 Saran

Sebagai pengembangan penelitian selanjutnya, perlu memperhatikan beberapa faktor berikut:

a. Mengkolaborasikan *framework* tersebut dengan *framework* investigatisi forensik video, sehingga nantinya dapat diperoleh *framework* yang lebih fleksibel untuk digunakan sehingga tidak perlu menganti *framework* saat akan menganalisis konten video.
b. Menggunakan pendekatan metode lain untuk melalukan evaluasi dan pengujian *framework.*

DAFTAR PUSTAKA

ACPO. (2008). Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0, 32.

ACPO. (2011). ACPO Good Practice Guide for Digital Evidence, (March), 41. Retrieved from http://www.acpo.police.uk/documents/crime/2014/Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011_Website.pdf

Al-azhar, M. N. (2012). *Digital Forensic*. Jakarta: Salemba Infotek.

Alshaikh, A., & Sedky, M. (2015). Post Incident Analysis Framework for Automated Video Forensic Investigation. *International Journal of Computer Applications*, *129*(17), 975–8887.

Badan Standarisasi Nasional. (2014). SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital.

Chowdhry, R. (n.d.). FORENSIC SCIENCE PAPER No . 7 : Criminalistics and Crime Scene Investigation MODULE No . 32 : Use of CCTV for Forensic Evidence FORENSIC SCIENCE PAPER No . 7 : Criminalistics and Crime Scene Investigation MODULE No . 32 : Use of CCTV for Forensic Evidence, (7).

EU Integration Office. (2011). *the Logical Framework Approach Framework*. Retrieved from http://www.evropa.gov.rs/Evropa/ShowDocument.aspx?Type=Home&Id=525

Hermaduanti, N., & Riadi, I. (2016). Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. *Journal of Theoretical and Applied Information Technology*, *93*(2), 287–296.

Ieong, R. S. C. (2006). FORZA - Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*(SUPPL.), 29–36. https://doi.org/10.1016/j.diin.2006.06.004

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, *38*(November), 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Kurniawan, E., & Riadi, I. (2018). SECURITY LEVEL ANALYSIS OF ACADEMIC INFORMATION SYSTEMS BASED ON STANDARD ISO 27002 : 2013 USING SSE-CMM, *16*(1), 1–9.

Kurniawan, E., & Riadi, I. (2018). Security Level Analysis of Academic Information Systems Based on Standard Iso 27002: 2013 Using Sse-Cmm. *International Journal of Computer Science and Information Security (IJCSIS)*, *16*(1), 139–147. https://doi.org/10.13140/RG.2.2.20925.15840

Lizarti, N., Sugiantoro, B., & Prayudi, Y. (2017). PENERAPAN COMPOSITE LOGIC DALAM MENGKOLABORASIKAN FRAMEWORK TERKAIT MULTIMEDIA FORENSIK, *2*(1), 26–33.

Palmer, G. (2001). the first Digital Forensic Research Workshop. *The First Digital Forensic Research Workshop (DFRWS)*, (1), 15–18. https://doi.org/10.1111/j.1365-2656.2005.01025.x

Riadi, I., Eko, J., Ashari, A., & -, S. (2013). Internet Forensics Framework Based-on Clustering. *International Journal of Advanced Computer Science and Applications*, *4*(12), 115–123. https://doi.org/10.14569/IJACSA.2013.041217

Sania, R. (2014). Pertemuan ke 6 & 7 - logical framework approach. Retrieved January 8, 2018, from https://www.slideshare.net/RuliInsaniA/pertemuan-ke-6-7-logical-framework-approach

Satti, R. S., & Jafari, F. (2015). Domain Specific Cyber Forensic Investigation Process Model. *Journal of Advances in Computer Networks*, *3*(1), 75–81. https://doi.org/10.7763/JACN.2015.V3.145

Sinambela, J. (2016). Digital Forensik dan Barang Bukti Rekaman CCTV kasus Jessica – Indonesia's Information Security Portal. Retrieved November 28, 2017, from https://infosec.id/2016/10/digital-forensik-dan-barang-bukti-rekaman-cctv-kasus-jessica/

Sudyana, D., Sugiantoro, B., & Luthfi, A. (2016). Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan Sni 27037 : 2014, (April 2017), 10. https://doi.org/10.13140/RG.2.2.16419.86560

SWGDE. (2014). SWGDE Best Practices for Computer Forensics, *1*(3.1), 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2014-09-05 SWGDE Best Practices for Computer Forensics V3-1

SWGIT. (2013). Section 24 Best Practice for Retrieval of Digital Video, *1.0 2013.0*.

LAMPIRAN A

Lampiran 1 : Penjelasan tahapan dan kegiatan dari *First Respond Framework* untuk Forensik CCTV hasil penelitian

Tabel 4.19 Penjelasaan Tahapan Framework Rancangan

No	Tahapan	Penjelasaan
	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.
1	Pengarahan	Sesi pengarahan mengenai perkara/kejadian, lokasi, peran dan tanggung jawab. Mandat/surat perintah investigasi.
2	Persiapaan dan perencanan	Menpersiapakan rencana investigasi, alat khusus, peralatan dan manual terkait bukti digital yang menjadi fokus.
3	Tindak pencegahan dilokasi kejadian	Melakukan pengamanan dan melindungi potensi bukti digital TKP.
4	Penliaian resiko	Melakukan penilaian resiko mengenai keamanan personel sebelum memulai proses. Contoh apakah terdapat bahaya fisik bagi personel
5	Pencarian bukti	Merupak proses pencarian barang bukti di sekitar lokasi kejadian yang bisa menjadi bukti potensial
6	Observe	Melihat keadaan sekitar TKP untuk mencari posisi perangkat CCTV
7	Type CCTV	Mengetahui jenis dvr yang digunakan *stand alone* atau *pc based* dan mengetahui *playback software.serial number,*
8	Feature CCTV	Fitur yang terpasang pada dvr, seperti *multiplexer, transactional data, network capabilitis*

9	Dokumentasi	Mencatat temuan yang diperoleh selama proses pencarian. Mencatat/dokumentasi dari jenis peralatan dan seting waktu yang tertera,*uniquei identifier,* siapa yang mengkases, siapa yang memeriksa. Megumpulkan informasi terkait kondisi *system setting* peralatan CCTV, seperti model dan *serial number, multiplexer model, playback software name password and version.*
	Pengumpulan	Setelah peralatan digital yang berkemungkinan berisi bukti digital potensial teridentifikasi. Investigator harus menentukan untuk melanjutkan atau tidak ke proses selanjtnya.
1	Memastikan isi	Memeriksa hasil rekaman untuk memastikan bahwa peristiwa /kejadian terkait dalam video relevan telah terekam dan pemeriksaan diupayakan dilakukan oleh yang paham alat *recording* saat melakukan *playback.*
2	Memastikan kamera	Memastikan posisi peletakan dan kondisi kamera aktif merekam kejadian.
3	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.*
4	Dokumentasi	Mencatat temuan yang diperoleh dari sistem kamera pengawas CCTV.
5	Time display	Mencari tahu durasi dan waktu kejadian saat di lokasi dan yang tercatat dalam sistem.
6	Metadata	Mencatat metadata dari file rekaman berupa *image quality,fps, frame size, firmware version, event log,password*
7	Native file	Mencari tahu format file yang dipergunakan oleh sistem.
8	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.
9	Sketsa posisi kamera	Membuat sketsa dari posisi kamera diruang lokasi kejadian.
10	Scene contact	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.
11	Photograph system	Foto sistem bagian depan dan belakang.
12	Operator assist	Mencari tahu siapa yang menjadi operator pada sistem CCTV tersebut. Hanya bila investigator tidak mampu atau tidak memahami sistem maka diperlukan ada nya operator atau admin dari kamera pengaswas yang mendampingi proses pengambilan file video.
	Akuisisi	Suatu proses yang membuat *copy* atau salinan dari bukti digital dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan. Investigator harus mengaplikasikan metode akuisisi berdasarkan situasi., biaya dan waktu, dan *tools* yang tersedia.
1	Dokumen akuisisi	Jika rekaman menunjukan petunuk terkait kasus. Maka penyidik dapat secara resmi meminta rekaman yang relavan dengan membuatkan berita acara pengambilan barang bukti
2	Tes ambil	Melakukan tes pengambilan apakah peralatan menyediakan opsi untuk bisa mengambil *native file* beserta *playback software* nya.
3	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. Berikut beberapa pilihan metode nya.
		CD/DVD writer opsi ini dipilih bila video digital berdurasi beberapa menit yang tidak memerlukan ruang yang luas.
		Flash media opsi ini dipilih bila durasi video berkisar 24 jam .
		Mass storage device opsi ini dipilih bila permintaan dari video yang diambil berkisar selama 30 hari, dimana menggunakan metode clone or removing the recording unit.
		Network connection opsi ini jika network viewer melakukan recover dari rekaman native video file.
		Replacing hardisk jika memerlukan waktu tercepat untuk mengakuisisi dengan menukar *hardisk* pada dvr.
		Drive duplication jika memerlukan keseluruhan data maka dilakukan duplikasi.
		Removal unit bila opsi lainya tidak memungkinkan untuk dilakukan
4	Waktu tersedia	Mencari tahu waktu atau durasi yang diperlukan untuk akusisi file video yang perlukan sehingga tidak memilih metode *output* yang memerlukan durasi panjang.
5	Evaluasi Output	memutuskan menggunakan metode *output* yang sesuai berdasarkan dari hasil tes pada *possible output* dan *amount of time*.
6	Live akuisisi	Melakukan tindakan logikal akusisi menggunakan sistem pada peralatan CCTV. Karena tidak menyita dan tidak mengambil keseluruhan data.
7	Pemeriksaan akuisisi	Memeriksa hasil akuisisi, apakah konten hasil akusisi sesuai dengan keperluan

8	Label bukti	Media penyimpanan hasil akuisisi dan ditandai sebagai *master digital evidence copy.* Kemudian membuat salinannya.
9	Chain of custdy	Mencatat kedalam dokumen investigasi terkait kronologi dari penangan untuk pengangkatan barang bukti. Disertakan pula dengan berita acara pengambilan barang bukti.
	Preservasi	Bukti digital potensial harus dalam kondisi preservasi atau dipelihara untuk memastikan kegunaannya dalam investigasi. Oleh karena itu mejadi hal yang pnting untuk menjaga integrititas atau keutuhan dari barang bukti, dengan mampu menunjukan jika bukti tersebut tidak modifikasi sejak diperoleh.
1	Verifikasi akuisisi	Menggunakan fungsi verifikasi sebagai segel keaslian pada *master evidence* seperti *digital signature* berupa nilai *hash* dari alogoritma md5. Untuk mengaplikasikan prinsip preservasi yang menjamin kerahasian, keutuhan dan ketersedian.
2	Memberikan segel barang bukti	Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.
3	Dokumen perjalanan	Menyiapakan dokumen atau surat perjalan untuk perpindahan bukti digital dari penyidik kepada labortorium atau ruang penyimpanan.untuk mematikan keamanannya maka juga harus diterangkan pada *Chain of Cutody.*
4	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.
5	Pemindahan barang bukti	Selama 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.
6	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.
7	Audit trail	Memeriksa kembali dokumen apakah telah mencatat detail tindakan yang dilakukan. Hal ini bertujuan untuk mempermudah bila adanya permintaan investigasi ulang oleh investigator yang berbeda.

Kemudian dilakukan pembuatan tabel matriks *logframe* hasil turunan dari matriks *logframe* yang utama di aktivitas identifikasi tahapan dan terminology dalam *framework* sehingga didapatkan indikator dan terminologi untuk setiap proses tahapan dalam *framework* tersebut. Berikut tabel 4.9 menampilkan matriks *logframe framework* rancangan.

Tabel 4.20 Matriks *Logframe Framework* Rancangan

Deskripsi Kegiatan	**Indikator**	**Verifikasi Indikator**	**Asumsi & Resiko**
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 Dihasilkannya sebuah *framework*	*Framework* telah memenuhi ketentuan yang berlaku	Memenuhi instrument evaluasi	Mengikuti standar yang diakui untuk digunakan dalam

investigasi CCTV yang telah memenuhi ketentuan SNI 27037:2014		untuk forensik CCTV	penyelidikan forensik digital.
Keluaran *Framework* hasil kolaborasi	*Framework* hasil perbaikan dan evaluasi	• Memenuhi instrument evaluasi • Memenuhi kebutuhan penyidik	Ketika aktivitas dilakukan maka keluaran diperoleh
Aktifitas 1. Pengarahan	- Pengarahan terkait perkara yang terjadi. - Pengarahan Peran dan tanggung jawab. - Persiapan mandat /surat perintah investigasi.	- Memahami perkara yang ditangani. - Memahami tugas yang harus dipenuhi di lokasi TKP. - Surat izin penyelidikan. - Surat izin pengeledahan.	- Dilakukan sebelum di lokasi TKP.
2. Persiapan dan perencanaan	- Perencanaan strategi investigasi. - Persiapan peralatan untuk dilokasi TKP dan mengambil barang bukti yang menjadi fokus.	- Strategi investigasi. - Peralatan untuk pengambilan barang bukti.	Tidak ada
3. Tindak pencegahan dilokasi kejadian	- Pengamanan TKP. - Membatasi akses ke area lingkup TKP.	- Petugas berwenang	Megikuti prosedur yang berlaku untuk mengamankan TKP.

		mejaga keamanan TKP. - Hanya pemilik hak akses yang bisa memasuki lingkup TKP.	
4. Penilaian resiko	- Keamanan tim investigasi di TKP.	- Terjaga keamanan tim investigasi forensik	Mengikuti prosedur yang berlaku.
5. Pencarian bukti	- Pencarian perlatan elektronik potensi barang bukti	- Barang bukti elektronik potensial	Memperkiran alat elektornik digital yang ada di TKP.
6. Type CCTV	- Mengetahui jenis alat perekam yang digunakan CCTV	- Barang bukti	Tidak ada.
7. Feature CCTV	- Mengindentifikasi fitur yang dimiliki sistem CCTV.	- Barang buki	Tidak ada.
8. Dokumentasi	- Dokumentasi TKP	- Catat temuan yang diperoleh.	Mendokumentasikan temuan pencarian di TKP.
9. Memastikan isi	- Memeriksa rekaman video	- Visual cek video dengan *playback*	Memastikan perkara yang dimaksud terekam kamera CCTV
10. Memastikan kamera	- Memeriksa posisi kamera yang merekam.	- Posisi kamera sesuai rekaman.	Memastikan kamera yang merekam TKP.
11. Jadwal overwrite	- Mengamati total kapasitas dari penyimpanan dan	- Jadwal overwrite selanjutnya.	Perkiraan waktu tersisa sebelum *overwrite*.

	tanggal rekaman paling awal.		
12. Dokumentasi	- Dokumentasi video rekaman CCTV	- Artefak digital.	Tidak ada
13. Time display	- Membandingan waktu tertera di rekaman dengan waktu nyata	- Error di *display time and date*. - Durasi peristiwa yang terekam.	Mencatat perbedaan waktu sistem dan nyata. Untuk audit trail.
14. Metadata	- Identifikasi metadata	- Metadata.	Mencatat temuan metadata.
15. Native file	- Identifikasi *native file format*	- *Native file video.* - *Playback software.*	Memastikan native file format tersedia
16. Keterangan verbal	- Wawancarai saksi	- Keterangan saksi di TKP.	Kondisi saat peristiwa terjadi.
17. Sketsa posisi kamera	- Posisi seluruh kamera CCTV	- Sketsa pemetaan TKP.	Tidak ada.
18. Scene contact	- Wawancarai pemilik gedung atau lokasi yang menjadi TKP	- Kontak pemilik bangunan	Bila ada nya audit trail dan kembali ke TKP.
19. Photograph system	- Dokumentasi barang bukti	- Fotografi barang bukti.	Tidak ada.
20. Operator assist	- Permintaan kepada admin CCTV untuk mendampingi saat proses akuisisi.	- Pendampingan oleh admin CCTV.	Bila investigator tidak mampu atau tidak memahami sistem maka diperlukan ada nya operator yang mendampingi.

21. Tes ambil	- Ketersedian opsi pengambilan file video	- Uji pengambilan file video	Memahami opsi akusisi yang tersedia oleh sistem CCTV.
22. Output tersedia	- Metode pengambilan video	- Output yang tersedia pada peralatan	Tidak ada.
23. Waktu tersedia	- Durasi tersedia untuk akuisisi	- Durasi akusisi tiap metode	Tidak ada.
24. Evaluasi Output	- Memutuskan memilih metode *output*	- Memilih metode *output*	Tidak ada.
25. Live akuisisi	- Prosedur partial akuisisi	- Barang bukti digital	Mengambil hanya sebagaian file yang diperlukan.
26. Pemeriksaan akuisisi	- Memeriksa hasil akuisisi	- konten akusisi sesuai kebutuhan. - Bisa diakses.	Memastikan akusisi menghasilkan *output* sesuai kebutuhan.
27. Label bukti	- Pelabelan barang bukti	- Label master evidence - Membuat salinan	Dimaksudkan untuk memudahkan mengenali barang bukti.
28. Chain of custody	- Catatan kronologi penangan terhadap barang bukti	- Form Chain of Costudy	Menjaga integritas barang bukti.
29. Verifikasi akusisi	- Melakukanan autentikasi data dengan *digital signature.*	- Nilai hash data barang bukti.	Menjaga integritas barang bukti.
30. Memberikan segel barang bukti	- Mengemas barang bukti - Menyegel barang bukti	- Pengemasan - Penyegelan	Memastikan barang bukti agar tidak tertukar dan terkontaminasi.

31. Dokumen perjalanan	- Menyiapkan surat pemindahan bukti digital dari	- Surat pemindahan barang bukti	Mengikuti prosedur yang berlaku untuk memindahkan barang bukti dari TKP ke ruang penyimpanan.
32. Pemeriksaan aspek keamanan pemindahan barang bukti	- Pengamanan barang bukti	- Mengemas barang bukti ke dalam wadah khusus	Menjaga agar tidak rusak.
33. Pemindahan barang bukti	- Memindahkan barang bukti ke pinyimpanan	- Investigator membawa ke tempat penyimpanan.	Update *chain of custody* ketika memindahkan.
34. Penyimpanan barang bukti	- Menyimpan barang bukti	- Ruang penyimpanan barang bukti	Ruang penyimpanan harus aman.
35. Audit trail	- Pemeriksaan kelengkapan dokumentasi tindakan dan temuan yang diperoleh	- *Chain of Custody*	mempermudah bila adanya permintaan investigasi ulang oleh investigator yang berbeda.

LAMPIRAN B

No	Deskripsi Kasus
1	Unit penyidik menangani kasus pencurian di areal Pesantren As'ad yang telah terpasang peralatan CCTV pada tanggal 10 Juni 2018 sekitar pukul 14:00 WIB. Memperoleh bukti digital rekaman video keterlibatan oknum pada peristiwa pencurian yang dilakukan dilingkup area Ponpes As'ad dari perangkat kamera pengawas CCTV.

TATA LANGKAH INVESTIGASI

Histori Tindakan Investigasi di Lokasi		
No	**Temuan Bukti**	**Keterangan**
1	Perangkat Digital DVR	Jenis: Stand Alone Merek: BXS-8216 Nomor Serial: bxs002*** Multiplexer: 16 Channel Transactional data: USB Penyimpanan: HDD 2 TB
2	Info File	Time Display 29-06-2018 Waktu kejadian 15:03:47 WIB Durasi 5 Menit 5 file Format .avh 5 file Format .avd *Playback software* tersedia
3	File hasil akuisisi berjumlah 10	Nama File: 20180629_140200.avh Hash:3df4f95dcbbca6eda6095633ff420565
		Nama file: 20180629_142902.avh hash:7afe53ad98dc55134ba98672f8fa719f
		Nama File: 20180629_145606.avh Hash: 8f60147db4fa2e01656483e66ba049b5
		Nama file: 20180629_152256.avh Hash: a126eb144eaee33c4466501b757ce5b1
		Nama file: 20180629_154958.avh Hash: 75f071ea84e6f98a31848e48cc8b6e0e
		Nama file: 20180629_140200.avd Hash: 599051eb3813c170f3b55d3e814fc386
		Nama file: 20180629_142902.avd Hash: 36c3968a054c2d816b3bcdabd575e2b0
		Nama file: 20180629_145606.avd Hash: 1df9bbbb7e6a5474e81159d47eac34f6
		Nama file: 20180629_152256.avd Hash: d32db9ad28ea09c2ad85768b90c9012c Nama fie: 20180629_154958.avd Hash: 5ff9caff3eb8b4b85cc70219c7787de4

Gambar 4. 29 Chain of Custody a

Tools yang digunakan

No	Tool	Keterangan
1	WinMD5	Untuk mengetahui nilai *hash*
2	USBWriteProtect	Untuk *WriteProtect* media penyimpanan *Master Evidence*

Peralatan untuk dilokasi

No	Peralatan	Keetrangan
1	Laptop	Untuk memeriksa hasil akuisisi
2	Flashdisk	Untuk media Penyimpanan hasil akuisisi
3	Kamera	Untuk dokumentasi forensik

Lampiran

Foto hasil akusisi

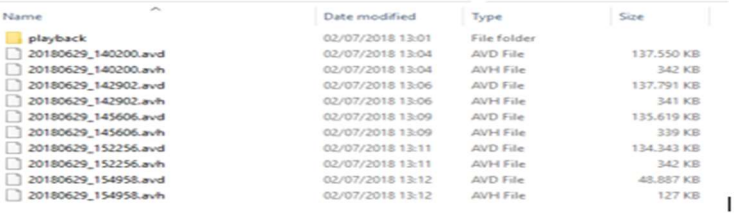
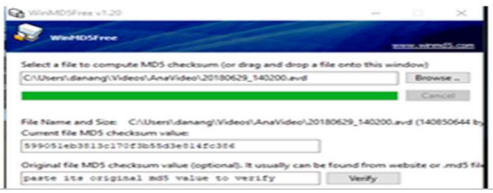


Foto nilai hash

Foto ke 1 hasil akuisisi file nama: 20180629_140200.avh

Memiliki nilai hash: 3df4f95dcbbca6eda6095633ff420565



Gambar 4. 30 Chain of Cutody b

Foto ke 2 hasil akuisisi file nama:
20180629_142902.avh
Memiliki nilai hash:
7afe53ad98dc55134ba98672f8fa719f

Foto ke 5 hasil akuisisi file nama:
20180629_154958.avh
Memiliki nilai hash:
75f071ea84e6f98a31848e48cc8b6e0e

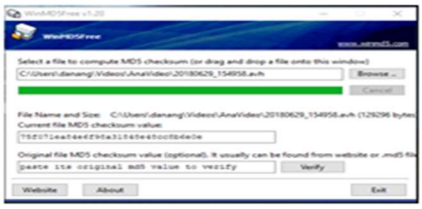


Foto ke 3 hasil akuisisi file nama:
20180629_145606.avh
Memiliki nilai hash:
8f60147db4fa2e01656483e66ba049b5

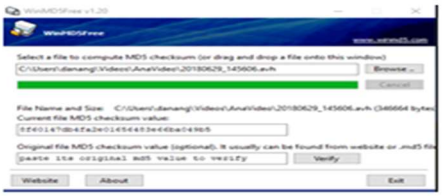


Foto ke 6 hasil akuisisi file nama:
20180629_140200.avd
Memiliki nilai hash:
599051eb3813c170f3b55d3e814fc386

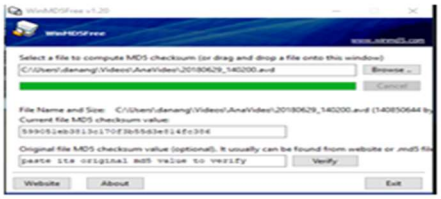


Foto ke 4 hasil akuisisi file nama:
20180629_152256.avh
Memiliki nilai hash:
a126eb144eaee33c4466501b757ce5b1

Foto ke 7 hasil akuisisi file nama:
20180629_142902.avd
Memiliki nilai hash:
36c3968a054c2d816b3bcdabd575e2b068a05

Gambar 4. 31 Chain of Cutody c

Foto ke 8 hasil akuisisi file nama:
20180629_145606.avd
Memiliki nilai hash:
1df9bbbb7e6a5474e81159d47eac34f6

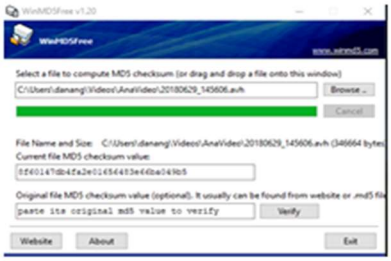


Foto ke 10 hasil akuisisi file nama:
20180629_154958.avd
Memiliki nilai hash:
5ff9caff3eb8b4b85cc70219c7787de4

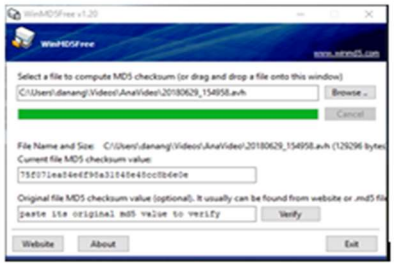
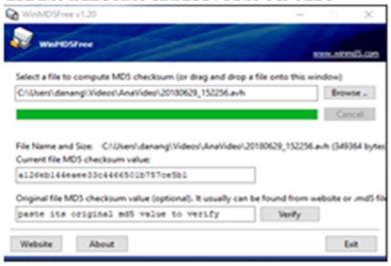
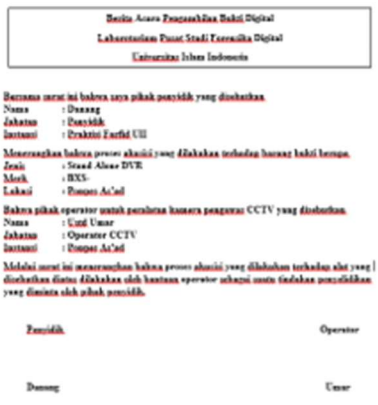


Foto ke 9 hasil akuisisi file nama:
20180629_152256.avd
Memiliki nilai hash:
d32db9ad28ea09c2ad85768b90c9012c



Berserta dilampirkan 1 keping CD rekaman proses akuisisi saat di lokasi dengan nilai hash mhkdb9a2376a09c2ad85768b90c9ff5

Lapiran surat pengambilan rekaman disaksikan saksi



Berita Acara Pengambilan Bukti Digital
Laboratorium Pusat Studi Forensika Digital
Universitas Islam Indonesia

Bersama surat ini bahwa saya pihak penyidik yang disebutkan
Nama : Danang
Jabatan : Penyidik
Instansi : Praktisi Fardid UII

Menerangkan bahwa proses akuisisi yang dilakukan terhadap barang bukti berupa
Jenis : Stand Alone DVR
Merk : HXS-
Lokasi : Pospam Ac'ad

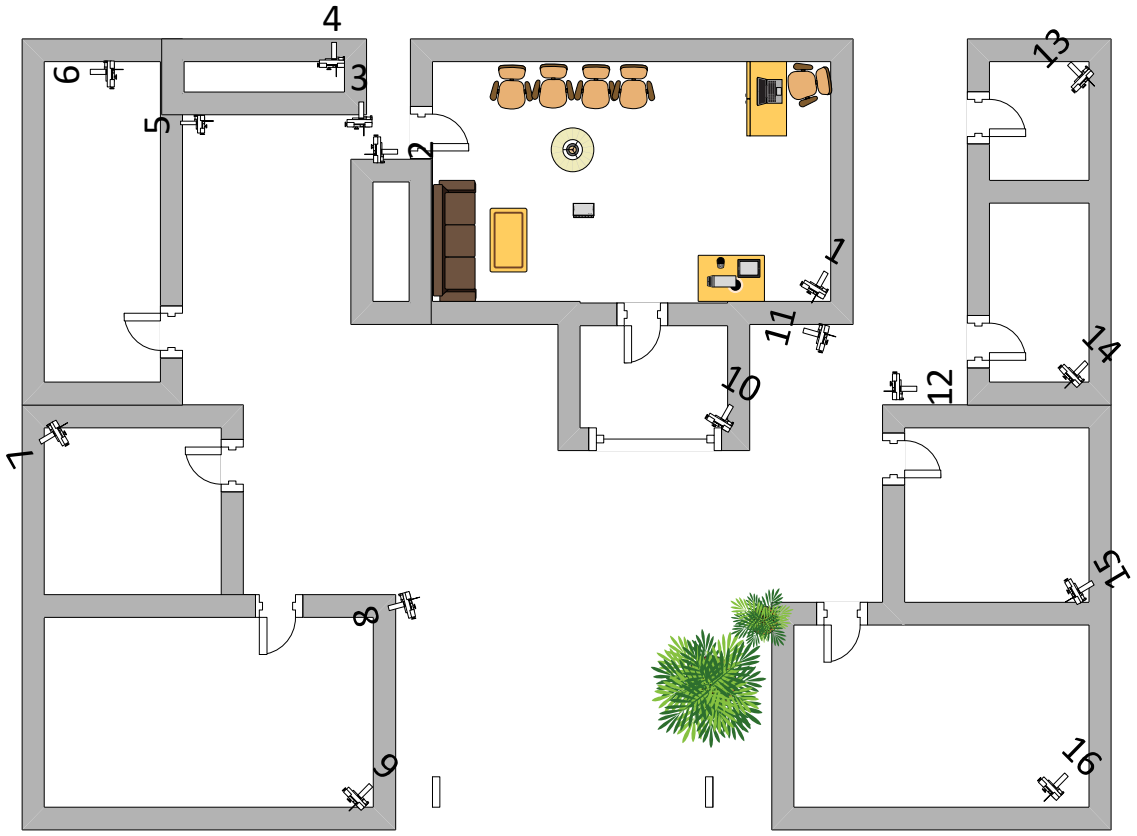
Bahwa pihak operator untuk perubatan kamera pengawas CCTV yang disebutkan
Nama : Umar Umar
Jabatan : Operator CCTV
Instansi : Pospam Ac'ad

Melalui surat ini menerangkan bahwa proses akuisisi yang dilakukan terhadap alat yang disebutkan diatas dilakukan oleh bantuan operator sebagai untuk tindakan penyidikan yang diminta oleh pihak penyidik.

Penyidik — Operator

Danang — Umar

Gambar 4. 32 Chain of Custody d



Gambar 4. 33 Sketsa Posisi Kamera

LAMPIRAN C

SURAT KETERANGAN
NOMOR: SKET/19/VII.LIT.2.1./2018/Ditreskrimsus

Kepala Kepolisian Daerah D.I. Yogyakarta menerangkan bahwa :

1. Nama : Danang Mulyadipa Suratno
2. NIM : 14917113
3. Jurusan/Prodi : Magister Teknik Informatika/Forensik Digital
4. Fakultas : Teknologi Industri
5. Akademi / Universitas : Universitas Islam Indonesia

Telah selesai mengadakan penelitian/pendataan/pengembangan/pengkajian dan studi lapangan di Direktorat Reserse Kriminal Khusus Polda D.I. Yogyakarta dengan cara Observasi wawancara dan pengambilan dokumentasi sebagai bahan penelitian yang berjudul :

"FIRST RESPOND FRAMEWORK UNTUK FORENSIK DIGITAL CCTV"

Demikian untuk menjadikan maklum dan agar dapat dipergunakan sebagai mana mestinya.

Yogyakarta, 18 Mei 2018

a.n. KEPALA KEPOLISIAN DAERAH D.I. YOGYAKARTA
DIREKTUR RESERSE KRIMINAL KHUSUS
u.b
KASUBBAGRENMIN

WIDANINGSIH, S.E.
KOMPOL NRP 15010876

Gambar 4. 34 Keterangan Polda DIY

LAMPIRAN D

Wawancara Uji First Respond Framework untuk Forensik CCTV

Identitas Responden

Nama :

Jabatan :

Instansi :

Tujuan Kuesioner

Mengajukan pertanyaan terbuka mengenai pendapat, saran dan masukan, bapak/ibu responden mengenai hasil penelitian dari sudut pandang ahli dan praktisi. Berupa First Respond Framework untuk Forensik CCTV. Apakah telah memenuhi kebutuhan bila digunakan pada kasus nyata.

Tujuan Pengumpulan Data

Hasil wawancara ini nantinya akan dipergunakan sebagai evaluasi untuk menyesesuaikan kembali framework hasil penelitian terhadap pendapat ahli dan praktis untuk menangani kasus-kasus CCTV.

Abstrak

Hasil dari peneiitian ini adalah First Respond Framework untuk forensik CCTV. Sebuah framework yang diperuntukan kepada mereka yang melakukan penganan awal terhadap bukti digital potensial berupa peralatan elektronik sistem DCCTV yang ditemukan di TKP. Fokus dari framework ini adalah sebagai petunjuk panduan atau disebut *guideline* yang memberikan **Standar** dan **Dokumentasi** tertentu untuk forensik CCTV sehingga dapat diajukan sebagai bukti hukum yang sah.

Standar

petunjuk mekanismes penangann dimana setiap aktivitas dalam kegiatan forensik dilakukan dengan cara yang tepat.

Dokumentasi

setiap aktivitas digital forensik dan temuannya haru didomentasikan. Sehigga jika diperlukan untuk disampaikan dipengadilan maka bisa menyampaikan mengenai proses menemukan dan mengambil serta menyimpan bukti digital tersebut

Daftar Pertanyaan

1. menurut bapak/ibu, alur pada framework ini cukup mudah diikuti.
2. Apakah bapak/ibu dapat mengaplikasikan framework tersebut pada kasus-kasus CCTV.
3. Bila diterapkan, apakah terdapat kendala.
4. Bila terdapat kendala, pada bagian apa.
5. Menurut bapak/ibu, saran dan masukan untuk First Respond Framework untuk forensik CCTV dari penelitian ini.