Pengembangan Framework Konseptual Terintegrasi Menggunakan Metode *Composite Logic* untuk *Cloud Forensic Readiness* pada Organisasi

Merisa Kurniasari Fadilla

17917113

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2021

Lembar Pengesahan Pembimbing

Pengembangan Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness pada Organisasi

Merisa Kurniasari Fadilla

17917113

Yogyakarta, Desember 2021

Pembimbing I	Pembimbing II
(Dr. Ir. Bambang Sugiantoro, S.SI., MT.)	(Dr. Yudi Prayudi, S.Si., M.Kom.)

Lembar Pengesahan Penguji

Pengembangan Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness pada Organisasi

Merisa Kurniasari Fadilla

17917113

Yogyakarta, Desember 2021

Tim Penguji,

Dr. Ir. Bambang Sugiantoro, S.SI., MT.
Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.
Anggota 1:

Dr. Imam Riadi, S.Pd., M.Kom.
Anggota II:

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

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

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli da ri 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, 31 Desember 2021

Merisa Kurniasari Fadilla, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari penulisan tesis ini.

Fadilla, M.K., Sugiantoro, B., & Prayudi, Y. (2022). Membangun Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness pada Organisasi. Jurnal Media Informatika Budidarma

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Merisa Kurniasari Fadilla	Mendesain eksperimen (70%) Menulis paper (100%)
Bambang Sugiantoro	Memberi ide dan Saran (30%) Telaah Artikel
Yudi Prayudi	Memberi ide dan Saran (30%) Telaah Artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari kontribusi dari berbagai pihak yang berbentuk saran maupun bimbingan, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Ir. Bambang Sugiantoro, S.Si., MT, Dr. Yudi Prayudi, S.Si., M.Kom, dan Dr. Imam Riadi, S.Pd., M.Kom.

Halaman Persembahan

Tesis ini saya persembahkan kepada orang tua, kakak dan adik saya yang telah mendukung dan menyemangati dalam menyelesaikan tugas akhir ini, tidak lupa juga saya ucapkan terima kasih kepada dosen pembimbing yang telah mengajar dan membimbing dengan sabar dan tidak lupa pula saya mengucapkan terima kasih kepada rekan-rekan dan adik tingkat yang banyak memberikan masukan dan saran dalam menyusun laporan tesis ini dan yang terakhir saya ucapkan terima kasih.

Kata Pengantar

Bismillahiwabihamdih

Assalamulaikum Wr. Wb.

Segala puji dan syukur saya panjatkan ke hadirat Tuhan yang Maha Esa karena berkat rahmat dan hidayah serta karunia-Nya, laporan tugas akhir ini dapat terlaksana sebagaimana mestinya. Proses penyusunan tugas akhir ini dapat saya laksanakan dengan bantuan serta bimbingan dari berbagai pihak. Oleh karena itu, pada saat ini saya bermaksud untuk menyampaikan ucapan terima kasih yang sebesar besarnya kepada:

1. Allah SWT yang telah memberikan rahmat, kesehatan dan kekuatan sehingga dapat menyelesaikan penyusunan laporan tesis ini.
2. Kedua Orang tua, bapak Munawar dan Ibu Wartini serta kakak dan adik. Terima kasih telah memberikan dukungan baik dari materi, kasih sayang, perhatian dan doa kepada penulis.
3. Bapak Dr. Ir. Bambang Sugiantoro, S.SI., MT., dan bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku Dosen Pembimbing tesis ini yang selalu membantu serta memberikan arahan dan masukan sehingga tesis ini dapat selesai.
4. Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D, selaku Ketua Program Studi Informatika – Program Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta
5. Seluruh Dosen Informatika UII yang telah membimbing dan mengajarkan hal-hal baru.
6. Semua sahabat-sahabat yang selalu memberikan dukungan dan bersemangat untuk menyelesaikan laporan ini.

Penulis menyadari terdapat banyak kekurangan dalam proses penyampaian dan penyusunan laporan tesis ini. Oleh karena itu, saya berharap kritik, saran, dan masukan yang bersifat membangun dari pembaca untuk memperbaiki diri kedepannya. Akhir kata semoga laporan ini dapat memberikan manfaat bagi semua pihak. Amin. Wassalaamu'alaikum Wr. Wb.

Bantaeng, 31 Desember 2021

Merisa Kurniasari Fadilla,

Daftar Isi

Cover i
Lembar Pengesahan Pembimbing ii
Lembar Pengesahan Penguji iii
Pernyataan Keaslian Tulisan iv
Daftar Publikasi v
Halaman Kontribusi vi
Halaman Persembahan vii
Kata Pengantar viii
Daftar Isi ix
Daftar Gambar xi
Daftar Tabel xii
Abstract xiii
Abstrak xiv
BAB I Pendahuluan 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Batasan Masalah 4
1.5 Manfaat Penelitian 5
1.6 Literatur Review 5
1.7 Metode Penelitian 6
1.8 Sistematika Penulisan 7
BAB II Tinjauan Pustaka 9
2.1 Digital Forensic Readiness 9
2.2 Cloud Forensics Readiness 10

2.3 Logic Model 12
2.4 Composite Logic Model 13
BAB III Metode Penelitian 15
3.1 Identifikasi Masalah 16
3.2 Studi Literatur 16
3.3 Analisis Karakteristik Framework *Cloud Forensic Readiness* Pada Organisasi 17
3.4 Pembuatan Framework Dengan Metode Composite Logic 17
3.5 Analisis Evaluasi Framework 17
3.6 Kesimpulan 18
BAB IV Hasil dan Pembahasan 19
4.1 Karakteristik Kesiapan Forensik Komputasi awan 19
4.2 Pembuatan Framework Dengan Metode Composite Logic 19
4.2.1 Identifikasi Framework *Cloud Forensic Readiness* 20
4.2.2 Proses Ekstraksi Menggunakan Pemodelan Logic, Terminologi, dan *Composite Role Model* 22
4.2.3 Klasifikasi Menggunakan Composite *Logic* Model 31
4.2.4 Kolaborasi Menggunakan *Composite Role Model* 34
4.2.5 Perancangan Framework 34
4.3 Implementasi *Cloud Forensic Readiness* Terintegrasi 38
4.4 Analisa Evaluasi *Framework* 39
4.4.1 Evaluasi Terhadap Framework yang ada 39
4.4.2 Evaluasi Terhadap Implementasi Framework 41
BAB V Kesimpulan dan Saran 45
5.1 Kesimpulan 45
5.2 Saran 45
Daftar Pustaka 47
Lampiran 49

Daftar Gambar

Gambar 1.1. Skema Alur Penelitian 7
Gambar 2.1. Template Logic Model 13
Gambar 3.1. Metodologi Penelitian..... 15
Gambar 4.1. Skema Penerapan Composite Logic 20
Gambar 4.2. Flowchart Proses Pengklasifikasian 32
Gambar 4.3. Alur *framework*..... 36
Gambar 4.4. Tampilan Muka Aplikasi SIPP 41

Daftar Tabel

Tabel 4.1. Hasil identifikasi *Cloud Forensic Readiness* 21
Tabel 4.2 Hasil identifikasi *Cloud Forensic Readiness* (Lanjutan)..... 22
Tabel 4.3. Hasil Ekstraksi "*A Digital Forensic Readiness Framework for South African SME's"* 24
Tabel 4.5 Hasil Ekstraksi "*Digital Forensic Readiness in the Cloud"* 25
Tabel 4.6. Hasil Ekstraksi "*Digital Forensic Readiness in the Cloud"*(Lanjutan) 26
Tabel 4.7. Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution"*..... 27
Tabel 4.8 Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution"* (Lanjutan)..... 28
Tabel 4.9 Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution" (lanjutan 2)*..... 29
Tabel 4.10. Hasil Ekstraksi "*Research on digital forensic readiness design in a cloud computing-based smart work environment"* 30
Tabel 4.11 Hasil Ekstraksi "*Research on digital forensic readiness design in a cloud computing-based smart work environment"*(Lanjutan) 31
Tabel 4.12. Hasil Klasifikasi Menggunakan *Composite Logic* 33
Tabel 4.13. Hasil Kolaborasi Menggunakan *Composite Role Model*..... 34
Tabel 4.14. Tahapan *Framework* awal 35
Tabel 4.15. Evaluasi *framework*..... 40
Tabel 4.16. Tabel evaluasi framework terhadap organisasi Pengadilan Agama Bantaeng. 42
Tabel 4.17. Tabel evaluasi framework terhadap organisasi Pengadilan Agama Bantaeng Lanjutan.. 43
Tabel 6.1. Tabel Hasil wawancara evaluasi penerapan *Integrated Cloud Forensic Readiness* pada organisasi Pengadilan Agama Bantaeng..... 50

Abstract

Building an Integrated Conceptual Framework Using the Composite Logic Method for Cloud Forensic Readiness in Organizations

In the Forensic Readiness approach, incident readiness is the goal of the company or organization in dealing with incidents that may occur. Forensic Readiness can consist of actions or steps, technical and non-technical, that supposedly maximize an organization's ability to use digital evidence. A well-built Cloud Forensic Readiness Framework can help speed up and simplify decision-making regarding an incident occurring in a cloud computing environment. This creates new opportunities for collaboration in the field of digital forensics and cloud computing or cloud computing, so that solutions can be studied and researched by analyzing various literature sources of cloud computing forensic readiness framework, extracting its steps and classifying them based on their etymology terms and building an Integrated Cloud Forensic Readiness framework on an institutional scale using the composite logic method. Therefore, Integrated Cloud Forensic Readiness is concluded in five major steps which, is (1) Resource Identification, (2) Policy and Procedure, (3) Technical Readiness, (4) Digital Forensic Response, (5) Evaluation and Report. The diversity in the complete steps of the readiness framework designed, is expected to result in easing the decision-making process for organizational stakeholders when an incident occurs.

Keyword: *Framework; Forensic Readiness; Cloud Forensic Readiness; Composite Logic; Incident Responses; Cloud Computin*

Abstrak

Membangun Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness pada Organisasi

Dalam pendekatan *Forensic Readiness*, kesiap-siagaan insiden menjadi tujuan perusahaan ataupun organisasi dalam menghadapi insiden yang swaktu-waktu terjadi. *Forensic Readiness* dapat terdiri dari tindakan atau langkah, teknis dan non-teknis, yang memaksimalkan kemampuan organisasi untuk menggunakan bukti digital. Sebuah *Cloud Forensic Readiness Framework* yang terangkai dengan baik dapat membantu mempercepat dan mempermudah dalam pengambilan keputusan yang berkenaan dengan sebuah insiden terjadi dalam lingkungan komputasi awan. Hal ini memunculkan kesempatan baru pada kolaborasi bidang digital forensic dan komputasi awan atau cloud computing, sehingga dapat ditelaah dan diteliti solusinya dengan menganalisis berbagai sumber *literature framework* kesiapan forensik komputasi awan, memecahnya dan mengelompokkannya sesuai *etymology* setiap katanya dan membangun *Integrated Cloud Forensic Readiness Framework* dalam skala institutional menggunakan metode composite logic. Oleh karena itu, Kesiapan Forensik Cloud Terintegrasi disimpulkan dalam lima langkah utama, yaitu (1) Identifikasi Sumber Daya, (2) Kebijakan dan Prosedur, (3) Kesiapan Teknis, (4) Tanggapan Forensik Digital, (5) Evaluasi dan Laporan. Dalam tahapan lengkap *readiness framework* yang dirancang, diharapkan dapat memudahkan proses pengambilan keputusan bagi pemangku kepentingan organisasi ketika terjadi insiden.

Kata Kunci: Framework; Kesiapan Forensik; *Composite Logic*; *Incident Responses*; Komputasi Awan.

BAB I
Pendahuluan

1.1 Latar Belakang

Mengacu pada seiringnya pertumbuhan kebutuhan teknologi modern kebutuhan masyarakat-pun turut meningkat dipicu oleh ketergantungan kemudahan teknis yang di berikannya. Hal ini membuat pertumbuhan teknologi terus menjadi tren yang sewaktu-waktu dapat mengubah dan mempengaruhi tidak hanya pola sosial dan bisnis, namun juga kriminalitas.

Salah satu diantaranya adalah *cybercrime* atau kejahatan dunia maya merupakan bentuk tindakan kejahatan menggunakan teknologi computer, jaringan computer, internet dan perangkat digital lainnya sebagai alat dan sasaran dalam melakukan aksi nya. Kejahatan dunia maya muncul seiring dengan semakin majunya perkembangan teknologi digital, informasi dan komunikasi. Perkembangan tersebut telah mengubah cara pandang sebagian pelaku ekonomi dan bisnis dalam beraktivitas, dimana dalam hal ini selain digunakan untukan meninkatkan efektivitas, efisiensi dan produktivitas namun juga dapat digunakan sebagai alat untuk mengambil keuntungan secara illegal. Beberapa istilah lain yang dapat setara dengan cybercrime adalah, computer abuse, computer fraud, computer related crime, dan computer misuse.

Internet merupakan salah satu faktor penyebab terus naiknya tren pemanfaatan teknologi yang sedang berkembang. Karena satu komputer terhubung dengan komputer lain membentuk sebuah jaringan, munculah tren kegiatan sosial dan bisnis yang terjadi secara virtual. Beberapa puluh tahun tak lama setelah jaringan antar komputer ditemukan dan dikembangkan, kini masyarakat yang mulai mengerti kebutuhan teknologi dan pentingnya terhubung dengan jaringan internet mulai menyasarkan perhatiannya pada fenomena komputasi terbaru, yaitu komputasi awan.

Komputasi awan menurut NIST (National Institute Science Technology) adalah sebuah model untuk kemudahan akses jaringan berdasarkan permintaan (on demand) dalam sumber komputasi publik yang bisa dikonfigurasi dan bisa dengan cepat di kondisikan serta dapat di rilis dengan usaha manajemen yang minimal untuk interaksi antar penyedia jasa. Komputasi awan menggunakan teknik virtual dalam membangun versi

maya dari sebuah komputer. Komputasi awan memiliki enam komponen utama, yaitu: clients, services, application, platform, storage, dan infrastructure (Mell, P.,et al, 2011).

Di Indonesia sendiri komputasi awan sudah mulai digalakkan seiring dengan adanya target pemerintah menuju revolusi industri ke-empat dunia, atau biasa disebut Making Indonesia 4.0. Dalam program kerja tersebut, pemerintah mulai mendorong Industri Kreatif Mandiri (IKM) dan berbagai perusahaan dalam negeri untuk menggunakan berbagai produk teknologi 4.0, yaitu diantaranya; IoT (Internet of Things), Komputasi Awan (Cloud Computing), hingga AI (Artificial Intelligence)[1].

Namun seiring teknologi yang berkembang, fenomena tersebut turut sejalan dengan modus operandi kriminal dunia maya yang semakin beragam. Sehingga kemudian menjadi tantangan baru bagi investigator *Digital Forensic*. Pada komputasi awan sering kali tidak dijumpai bentuk fisik langsung yang diperlukan dalam proses imaging saat mengamankan barang bukti digital di tempat kejadian perkara. Tantangan yang berbeda menyangkut lingkungan komputasi awan juga ditemukan pada saat penyelidikan menggunakan investigasi live forensic, dimana hanya gambar (screenshots) dari mesin berjalan saja yang dapat diselidiki. Sehingga tidak memungkinkan dilakukan reka ulang kejadian perkara seperti pada saat penyelidikan statik (George et al., 2012).

Komputasi awan memberikan kesempatan juga tantangan pada instansi pemerintah, khususnya dalam bidang ketahanan hukum dan keamanan nasional. Tantangan tersebut salah satunya disebabkan oleh keterbatasan jurisdiksi hukum suatu negara, ketika layanan komputasi awan itu sendiri bersifat internasional tak terbatas.(Martini & Choo, 2013)

Media penyimpanan dalam komputasi awan adalah milik vendor penyedia sepenuhnya, sehingga untuk mengamankan bukti fisik secara utuh akan memerlukan waktu, tidak begitu praktis dan menyulitkan DEFR (Digital evidence First Responder) dalam mengamankan barang bukti digital.(Grispos et al., 2013)

Konsep forensic readiness menurut Tan, 2002 mempunyai tujuan utamanya yaitu memaksimalkan kemampuan sebuah lingkungan dalam mengumpulkan barang bukti digital namun juga dapat meminimalisir biaya forensik yang dibutuhkan pada saat incident response. Hal ini dijelaskan lebih lanjut oleh Rowlingson (Rowlingson, 2004), dimana sebuah pendekatan forensic readiness dimaksud agar kesiapan terhadap sebuah kejadian perkara menjadi tujuan pada saat membahas aksi teknik dan non-teknis yang dapat memaksimalkan kemampuan sebuah organisasi dalam menggunakan bukti digital.

[1] kemenperin.go.id/artikel/18967/Making-Indonesia-4.0:-Strategi-RI-Masuki-Revolusi-Industri-Ke-4,2018

Moouhtaropolous, 2014 mengemukakan bahwa dalam pendekatan bisnis, tujuan utama sebuah organisasi adalah meminimalisir dampak akibat sebuah perkara pada proses bisnis yang sedang berjalan, sehingga sebuah organisasi diharapkan mampu mempersiapkan langkah antisipasi agar proses bisnis tidak terganggu dan investigasi forensik dapat terlaksana dengan baik.

Sebuah instansi yang tidak menyiapkan dengan baik untuk kejadian perkara kriminal akan kesulitan dalam menjaga posisinya, karena kurangnya bukti yang dibutuhkan, penanganan bukti yang tidak benar, dan kontaminasi bukti. Maka dari itu penting untuk menngantisipasi skenario terburuk, dan salah satu cara untuk menangani hal tersebut adalah menyiapkan model rencana yang dapat menghasilkan bukti digital yang reliable bahkan sebelum benar-benar diperlukan. (Barske et al., 2010)

Banyak peneliti yang mengusulkan model arsitektur cloud forensic readiness dengan membangun server forensik hingga usulan botnet (Kebande, 2014) sebagai media atau pihak ketiga yang meonitoring pergerakan data dan logs dalam komputasi awan, namun hingga saat ini masih sulit diwujudkan karena terlalu luasnya cakupan hukum dan kebijakan antar negara yang perlu ditempuh untuk mewujudkan hal tersebut.

Kebalikan dari model arsitektur cloud forensic readiness, jika menilik masalah dari segi aturan per regional (negara) dalam pendekatan *Forensic Readiness*, kesiap-siagaan insiden menjadi tujuan perusahaan dan terdiri dari tindakan atau langkah, teknis dan non-teknis, yang memaksimalkan kemampuan organisasi untuk menggunakan bukti digital. Sebuah *Integrated Cloud Forensic Readiness Framework* yang terangkai dengan baik dapat membantu mempercepat dan mempermudah dalam pengambilan keputusan yang berkenaan dengan sebuah insiden terjadi dalam lingkungan komputasi awan. Masih belum adanya yang meneliti dan menganalisis serta membangun konsep framework *Integrated cloud forensic readiness* pada skala institusi dan dengan beragam kelengkapan tahapan framework kesiapan yang ramah untuk pemula atau orang awam. Pemilihan sebuah model framework kesiapan forensika awan yang paling tepat sesuai dengan kondisi hukum dan aturan sebuah negara dalam tingkatan prosedural sebuah organisasi dibutuhkan untuk menjawab tantangan dalam menyiapkan lingkungan komputasi awan yang siap untuk dilakukan proses digital forensik di dalamnya.

1.2 Rumusan Masalah

Ketiadaan framework *Integrated Cloud Forensic Readiness* yang khusus menelaah kebutuhan sumber daya yang memfasilitasi kesiapan sebuah proses cloud forensic dalam sebuah organisasi, membuat banyak organisasi mengalami kerentanan terhadap insiden yang terjadi di sebuah lingkungan komputasi awan yang digunakan oleh organisasi.

Dengan adanya permasalahan ini perlu adanya sebuah framework kesiapan untuk mendukung pembangunan sebuah mekanisme digital forensic readiness dalam lingkungan komputasi awan pada organisasi. Oleh karena itu penelitian ini mengusulkan sebuah perancangan framework *Integrated Cloud Forensic Readiness* pada organisasi dengan menggunakan metode *Composite Logic.*

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini adalah sebagai berikut:

a. Untuk mengetahui karakteristik sebuah *Cloud Forensic Readiness Framework* dengan menggunakan model *logic.*
b. Untuk mengetahui bagaimana merancang sebuah *Cloud Forensic Readiness Framework* yang terintegrasi.
c. Untuk dapat menerapkan *Cloud Forensic Readiness Framework* yang telah dirancang dalam pelaksanaan kesiapan investigasi forensik digital di lingkungan awan pada Organisasi

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

a. Penelitian ini dilakukan untuk merancang sebuah *Cloud Forensic Readiness Framework* terintegrasi menggunakan metode composite logic pada organisasi.
b. Penelitian ini menganalisis beberapa model framework kesiapan forensika awan yang telah ada untuk mendapatkan faktor pembanding.
c. Penelitian ini berfokus untuk menganilisis sumber daya dan mekanisme kerja yang dibutuhkan dalam pembangunan framework.

1.5 Manfaat Penelitian

Peksanaan penelitian ini diharapkan dapat memberikan manfaat diantaranya sebagai berikut:

a. Dengan adanya penelitian ini, diharapkan dapat melakukan analisa terhadap karakteristik framework kesiapan *cloud forensic readiness* pada organisasi.
b. Menghasilkan sebuah *framework* konseptual terintegrasi untuk Cloud Forensic Readiness pada organisasi
c. Dengan adanya *framework* ini, diharapkan dapat memberikan kontribusi dan kemudahan untuk stake holder dalam membangun lingkungan awan yang siap (ready) dalam penyelidikan *digital* maupun *cloud forensic*.
d. Dengan adanya penelitian ini juga diharapkan dapat memberikan kontribusi bagi penelitian selanjutnya.

1.6 Literatur Review

Digital Forensic Readiness menurut Tan, 2002 merupakan upaya sebuah lingkungan dalam mengumpulkan bukti digital serta meminimalisir biaya forensik yang digunakan pada saat respon insiden. Kesiapan sebuah organisasi dalam menggunakan barang bukti digital inilah yang kemudian menjadi tujuan teknis dan non teknis organisasi terkait. (Rowlingson, 2004). Cloud Forensic Readiness (*Integrated Cloud Forensic Readiness*) merupakan perpaduan ilmu konsep antara digital forensic readiness dengan komputasi awan.

Penelitian yang dilakukan oleh Alenezi pada tahun 2019, mengemukakan perancangan framework Kesiapan Forensik Komputasi Awan (*Cloud Forensic Readiness*) yang didasarkan dari beberapa rancangan yang sudah ada ditelaah lebih lanjut dan membandingkannya dengan review atau wawancara dari pakar forensik (Alenezi et al., 2019).

Sedangkan pada penelitian (Park et al., 2018) dikembangkan framework kesiapan digital forensic hingga tingkat pencegahan insiden, dengan mempertimbangkan perubahan perubahan pada lingkungan kerja cerdas berbasis cloud computing. Untuk memverifikasi model yang dirancang, Park dan kawan-kawan membuat survei yang menargetkan profesional terkait bidang forensik digital, menganalisis validitasnya, dan menyimpulkan model kesiapan forensik digital dari lingkungan kerja cerdas berbasis komputasi awan yang terdiri dari tujuh area terperinci dan 44 komponen. Setelah dilakukan analisis mereka

kemudian menyimpulkan area yang harus ditekankan dan dibandingkan dengan lingkungan kerja yang ada untuk meningkatkan kesiapan forensik di lingkungan kerja cerdas berbasis komputasi awan.

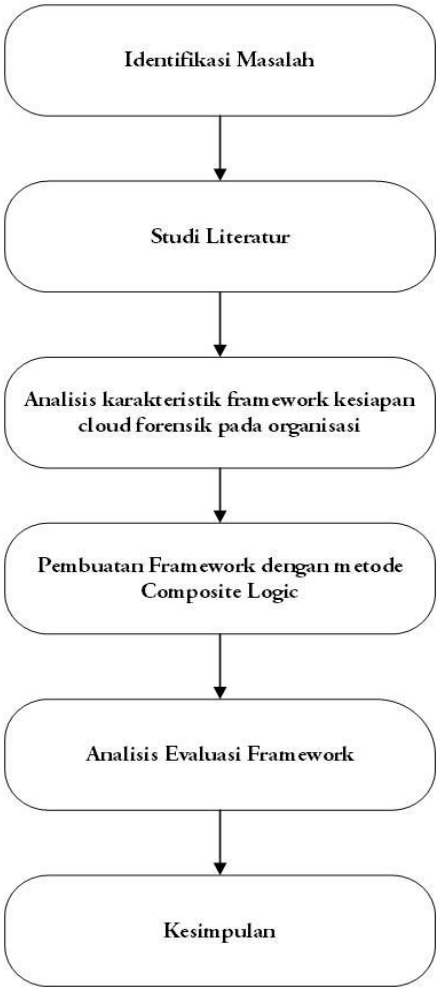
Penelitian yang dilakukan Karie dan Karume menyajikan berbagai masalah dan tantangan seputar penerapan kesiapan forensik digital (DFR) dalam organisasi. Area konsentrasi utama adalah: berbagai tindakan proaktif yang dapat dilakukan organisasi sebagai cara untuk meningkatkan kemampuan merespons insiden keamanan dan menciptakan lingkungan yang siap untuk forensik digital. Namun, penelitian tersebut juga melihat masalah dan tantangan yang berkaitan dengan penyimpanan dan disposisi data dalam organisasi yang mungkin juga memiliki beberapa efek pada penerapan kesiapan forensik digital (DFR). Hal ini didukung oleh fakta bahwa meskipun kebutuhan forensik digital dan bukti digital dalam organisasi telah dieksplorasi, seperti kebutuhan kesiapan forensik digital dalam organisasi, pengambil keputusan masih perlu pemahaman lebih lanjut tentang apa saja yang dibutuhkan dalam sebuah organisasi untuk memastikan implementasi yang efektif dari kesiapan forensik digital (Karie & Karume, 2017).

Penelitian mengenai perancangan konsep framework untuk cloud forensic readiness dilakukan oleh (Alenezi et al., 2017) yang membahas faktor organisasi, teknis dan legalitas yang mempengaruhi kesiapaan digital forensic dalam lingkungan komputasi awan, khususnya pasa Infrastructure as a Service (laaS). Alenezi membahas beberapa studi mengenai DFR sebelum mengusulkan sebuah konsep framework cloud forensic readiness dalam organisasi.

Penelitian selanjutnya dilakukan oleh (Alex & Kishore, 2017) tentang framework forensik untuk cloud computing. Penelitian ini dilakukan untuk menjawab tantangan yang dihadapi dalam forensik cloud dan menawarkan solusi untuk peneliti lainnya. Framework ini merupakan sebuah model baru untuk mengurangi tantangan dalam cloud forensik telah diusulkan dan divalidasi dengan serangan DDoS untuk melakukan pemeriksaan terhadap Forensic Monitoring Plane (FMP) dengan mengumpulkan semua informasi yang diperlukan terkait dengan kegiatan penipuan yang diperlukan untuk analisis forensik.

1.7 Metode Penelitian

Langkah-langkah yang ditempuh untuk melakukukan penelitian ini dapat digambarkan dalam *flowchart* sebagai berikut:



Gambar 1.1. Skema Alur Penelitian

1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tuuan penelitan, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II KAJIAN TEORI

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV PEMBAHASAN

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

BAB V PENUTUP

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB II
Tinjauan Pustaka

2.1 Digital Forensic Readiness

Forensik digital merupakan salah satu bidang spesialis pemahaman komputer yang sangat luas. Forensik digital menjadi salah satu bentuk spesialisasi untuk melakukan investigasi yang berhubungan dengan kejahatan komputer. Forensik digital mengacu pada proses akuisisi, pelestarian, analisis, dan penyajian bukti digital yang dihasilkan dari kejahatan terkait digital (Sant, 2014). Forensik digital akan melakukan pemeriksaan setiap barang bukti elektronik dalam rangka mencari data-data digital yang berkaitan dengan kesus kejahatan dan pelakunya.

Dalam ilmu forensik digital, seorang ahli dalam bidang forensik digital harus memahami prinsip-prinsip dasar. Hal ini menjadi dasar seorang ahli forensik digital dalam melakukan invesitigasi kejahatan komputer. Menurut (ACPO, 2012), prinsip-prinsip dasar forensika digital adalah :

1. Sebuah lembaga hukum atau petugasnya dilarang mengubah data data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.
2. Untuk seorang 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.
3. Terdapat catatan teknik 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.
4. *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.

Pengumpulan bukti digital melalui forensik langsung dan postmortem, dapat dikaitkan erat dengan proses analisis bukti digital yang ditangkap. Forensik digital reaktif adalah proses manual untuk memperoleh dan menganalisis bukti digital setelah insiden terjadi. Forensik digital proaktif, pada gilirannya, adalah tempat proses akuisisi forensik

dilakukan secara langsung dan analisis awal dilakukan oleh sistem otomatis. Sehingga, kesiapan forensik adalah kebijakan dan prosedur yang dibuat untuk memungkinkan investigasi forensik digital yang sukses.(Ras, 2018)

2.2 Cloud Forensics Readiness

Cloud forensics adalah bagian dari forensik digital, dan ini menunjukkan kebutuhan untuk investigasi digital di lingkungan cloud berdasarkan prinsip dan prosedur forensik. Penyelidik kejahatan di lingkungan cloud harus menangani sejumlah masalah berbeda dibandingkan dengan investigasi jaringan atau komputer (forensik digital). Yang paling penting adalah bahwa bukti dapat berada di mana saja di dunia dalam lingkungan virtualisasi. Ada juga masalah yang terkait dengan yurisdiksi, multi-tenancy, dan ketergantungan pada CSP yang unik untuk cloud forensik dan membuatnya semakin kompleks..(Simou et al., 2016)

Tergantung dari jenisnya, layanan awan dapat memengaruhi bukti yang tersedia bagi penyelidik dan cara pengumpulannya. Misalnya, platform IaaS menghadirkan antarmuka ke pengguna yang tidak dapat dibedakan dari server fisik jarak jauh. Namun, data yang mewakili server berbasis IaaS secara inheren lebih tidak stabil. Sedangkan, model SaaS dan PaaS membatasi fleksibilitas yang dapat digunakan pengguna untuk berinteraksi dengan platform komputasi awan, dengan menawarkan serangkaian aplikasi terbatas, atau menentukan batasan di mana perangkat lunak baru dapat dibuat. Penyimpanan data pada layanan ini tidak dilakukan oleh pengguna, melainkan oleh pemilik cloud. (Grispos et al., 2013)

Sejumlah peneliti telah mendefinisikan *cloud forensic*s sebagai bidang ilmu forensik digital di lingkungan cloud. Secara teknis, bidang tersebut bergantung pada pendekatan forensik hibrida (misalnya, jarak jauh, virtual, jaringan, langsung, skala besar, klien tipis, klien tebal, termasuk perangkat titik akhir yang digunakan untuk mengakses layanan cloud) untuk menemukan bukti digital. Secara organisasi, bidang tersebut melibatkan interaksi di antara Pengguna komputasi awan (Provider, Consumer, Broker, Carrier, Auditor) untuk tujuan memfasilitasi penyelidikan internal dan eksternal. Secara hukum, ini sering kali menyiratkan situasi multi yurisdiksi dan multi-penyewa. Berbagai model proses telah dikembangkan untuk forensik digital, termasuk delapan model berikut:

1. Otoritas pencarian.

   Otoritas hukum diperlukan untuk melakukan pencarian dan / atau penyitaan data.

2. *Chain of Custody*.

   Dalam konteks hukum, dokumentasi kronologis akses dan penanganan barang bukti diperlukan untuk menghindari dugaan perusakan atau kesalahan bukti.

3. Imaging/*hashing function*.

   Ketika item yang mengandung bukti digital potensial ditemukan, masing-masing harus diduplikasi dengan hati-hati dan kemudian di-hash untuk memvalidasi integritas salinan.

4. Alat yang tervalidasi.

   Jika memungkinkan, alat yang digunakan untuk forensik harus divalidasi untuk memastikan keandalan dan ketepatan.

5. Analisis.

   Analisis forensik adalah pelaksanaan teknik investigasi dan analitik untuk memeriksa, menganalisis, dan menafsirkan artefak pembuktian yang diambil. Pengulangan dan reproduktifitas (jaminan kualitas). Prosedur dan kesimpulannya analisis forensik harus dapat diulang dan direproduksi oleh forensik yang sama atau lainnya analis.

6. Pelaporan.

   Analis forensik harus mendokumentasikan prosedur analitisnya dan kesimpulan untuk digunakan oleh orang lain.

7. Presentasi.

   Dalam kebanyakan kasus, analis forensik akan mempresentasikan temuannya dan kesimpulan pengadilan atau audiensi lain.(NIST, 2014)

Penyedia layanan komputasi awan (*Cloud Service Provider*) sengaja menyembunyikan lokasinya untuk mengakomodasi pergerakan dan replikasi. Permasalahan yang perlu diperhatikan juga adalah kontrol fisik atas komponen arsitektur yang kurang memadai. Tergantung dari variasi untuk 3 Model Layanan (SaaS, PaaS, IaaS), masalah kurangnya control fisik ini menjadi lebih besar di dalam penyedia yang menyediakan layanan SaaS, dan lebih besar di pada pelanggan yang menggunakan layanan IaaS. Dalam Komputasi awan juga memiliki permasalahan lain seperti kurangnya standar pada beberapa format file log, dan tidak adanya sinkronisasi cap waktu di antara beberapa pusat data dan server. Masalah lainnya Layanan Cloud yang diakses melalui jaringan melalui platform klien bersifat heterogen, tetapi tidak seperti pada Forensik Jaringan,

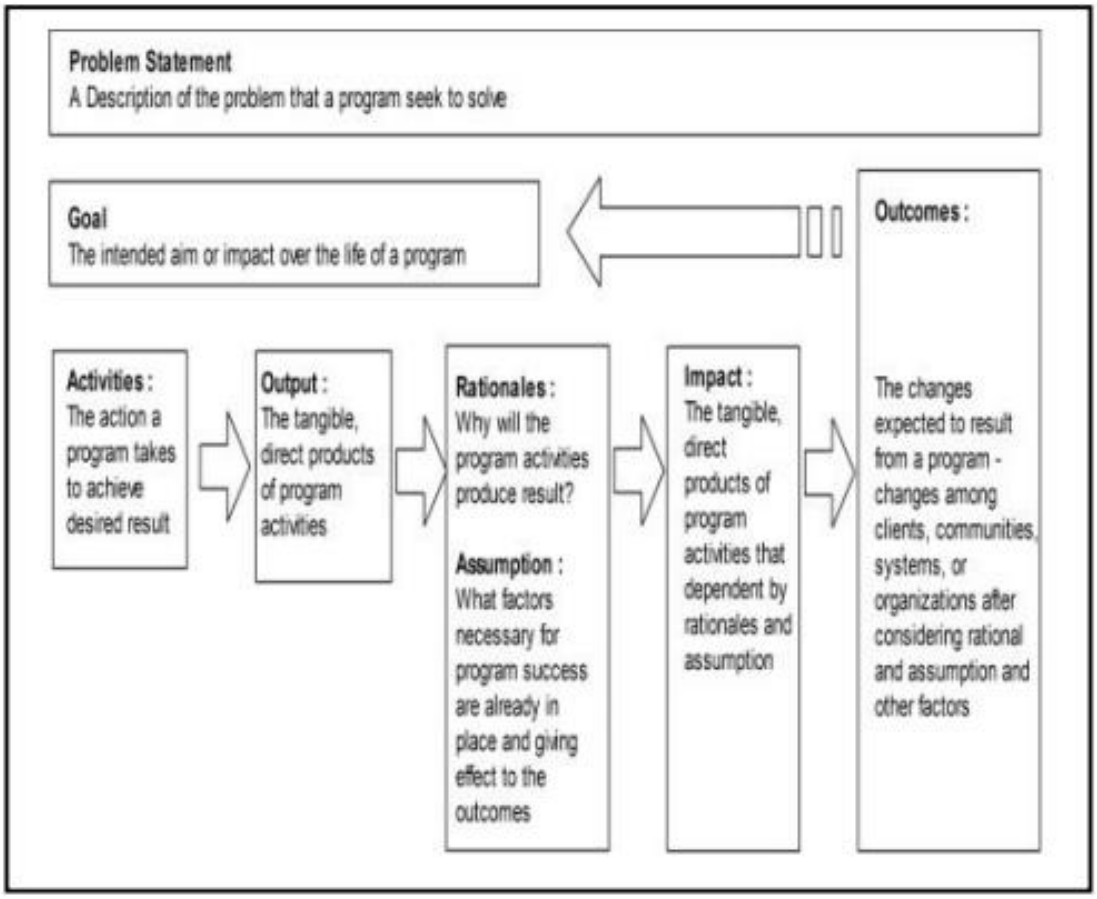
Dalam komputasi awan tidak ada informasi pe-rute-an untuk mendapatkan informasi mengenai sumber serangan digital (Marco et al., 2013)

Menilik dari segi barang bukti komputasi awan menawarkan tantangan lebih banyak seperti tentang data dan proses pembuktian barang bukti. Riwayat objek digital yang menyimpan informasi pengguna yang mengakses objek tertentu disimpan dalam meta-data yang selanjutnya dapat diproses sebagai data dan proses pembuktian. Hal ini menjadi bagian penting dalam sebuah Investigasi Digital Forensik, dan pertanyaan akan terus muncul jika logs (Riwayat objek) yang dibutuhkan tidak ada.(Trenwith & Venter, 2013)

Setiap usaha yang bersifat defensif dari sebuah system keamanan informasi dan berdasarkan penilian resiko akan selalu menyisakan resiko individu. Hal ini lebih dikarenakan bahwa pengguna dipercaya untuk tidak menyebabkan insiden yang membahayakan keamanan informasi. Dalam jangka panjang, penilaian tersebut mungkin saja lebih aman dan persiapan usaha defensive tidak perlu dilakukan. Namun dalam halnya Kesiapan Forensic (Forensic Readiness), penting untuk berasumsi bahwa sebuah insiden akan terjadi, bahkan jika penilaian resiko beranggapan tidak akan ada insiden. Situasi seperti ini menjadi lebih penting lagi untuk diperhatikan pada resiko insiden yang disebabkan oleh orang dalam. Tergantung dari impactnya, sebuah organisasi akan memerlukan usaha kesiapan untuk mengidentifikasi pelaku dan mendapatkan bukti yang dibutuhkan untuk mengadakan tindakan keadilan terhadapnya. (Rowlingson, 2004)

2.3 Logic Model

Logic model dapat digunakan untuk identifikasi *Timeframe* yang akan di buat. Hal ini akan membantu dalam memperoleh hasil jangka pendek, menengah, dan jangka panjang serta membuat keputusan yang baik tentang sumber daya dan keputusan. Struktur logic model dapat digunakan untuk perencanaan program dengan menentukan parameter program dengan jelas. Banyak model logic yang ada, namun pada dasarnya semua mengandung konsep yang sama. Model logic akan bermanfaat untuk pemangku kepentingan untuk memperoleh masukan dalan kegiatanya (Mccawley, 2015).



Gambar 2.1.Template Logic Model

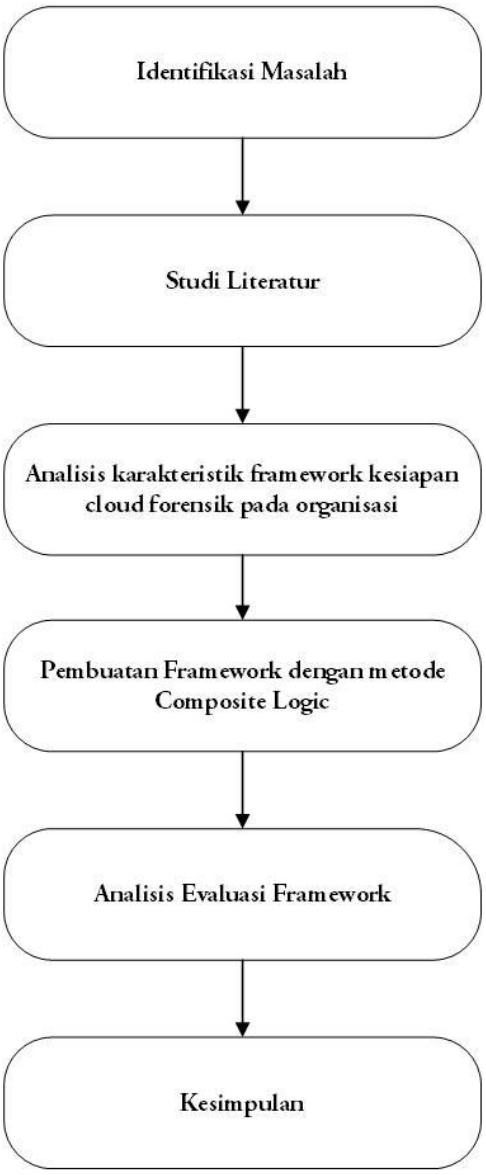
2.4 Composite Logic Model

Composite Logic digunakan untuk mengkombinasikan beberapa struktur model menjadi sebuah model kesatuan yang tetap mempertahankan hirarki ataupun susunan awal kerangkan model yang ada. Hal yang paling penting dalam *Composite Logic* model adalah menentukan role model dari setiap variabel ataupun pola awal yang ingin dikolaborasikan. Role model menjelaskan bagaimana beberapa objek berkolaborasi, satu ataupun dua peran yang bersamaan dalam sebuah pola untuk mencapai tujuan yang sama. Sebuah peran mewakili sudut pandang dari beberapa objek yang bekerjasama dengan berpegang pada sebuah tujuan. Pemodelan ini dapat membantu peneliti dalam mengeksplorasi keterhubungan dari aktivitas berbeda dengan tujuan yang sama. Sehingga memudahkan peneliti dalam melakukan klasifikasi dan kolaborasi beberapa *framework* yang pada akhirnya akan menghasilkan satu set *framework* (Lizarti et al., 2017).

Kelebihan lain dari composite adalah composite dapat meringkas realitas multi-dimensi yang kompleks dengan maksud untuk mendukung para pembuat keputusan dan Lebih mudah diinterpretasikan untuk banyak indikator terpisah serta mengurangi ukuran yang terlihat dari serangkaian indikator tanpa menjatuhkan basis informasi yang mendasarinya. Dibalik beberapa kelebihan yang dimiliki composite, namun ada beberapa kekurangan antara lain dapat mengirim pesan kebijakan yang menyesatkan jika dibangun dengan buruk atau disalahtafsirkan. Selain itu dapat mengundang kesimpulan kebijakan yang sederhana yang memiliki kemungkinan untuk disalah artikan, serta pemilihan indikator dan bobot bisa menjadi subyek perselisihan politik. (Nardo et al., 2008).

BAB III
Metode Penelitian

Bab ini menjelaskan tentang bagaimana urutan cara penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1. Metodologi Penelitian

Gambar 3.1 menjelaskan bahwa metodologi penelitian ini menggunakan 6 tahapan yakni (1) Identifikasi Masalah (2) Studi Literature (3) Analisis Karakteristik framework *Cloud Forensic Readiness*pada organisasi (4) Pembuatan Framework Dengan Metode Composite Logic (5) Analisis Evaluasi Framework (6) Kesimpulan.

3.1 Identifikasi Masalah

Identifkasi Masalah merupakan tahap awal dalam penelitian ini, hal ini dilakukan untuk memperoleh dan menemukan topik masalah dalam penelitian yang akan diteliti lebih lanjut. Proses identifikasi masalah ini sangat diperlukan untuk membuat *framework* terintegrasi Cloud Forensic Readiness pada organisasi untuk menghindari pembahasan topik yang terlalu melebar dari topik masalah yang telah dijadikan arahan. Hal ini merupakan langkah yang tepat untuk memastikan penelitian berjalan sesuai yang diharapkan.

Pada tahapan ini akan dilihat berbagai macam fenomena, kejadian dan informasi yang didapatkan dengan berbagai macam cara yang berhubungan dengan penelitian yang dilakukan. Dalam penelitian ini yang akan dilakukan adalah membuat *Cloud Forensic Readiness Framework* terintegrasi dengan menggunakan metode *Composite Logic Model* sehingga dapat dijadikan sebagai referensi standar oleh stakeholder sebuah organisasi maupun para provider komputasi awan (CSP).

3.2 Studi Literatur

Tinjauan pustaka dilakukan untuk mengumpulkan bahan-bahan informasi mengenai topik penelitian yang dapat bersumber dari buku, artikel, paper, jurnal, makalah, yang berupa teori, laporan penelitian, atau penemuan sebelumnya. Selain itu pengumpulan bahan data penelitian dapat juga di dapat dengan cara mengunjungi beberapa situs yang terdapat pada internet terkait dengan teori-teori tentang *Digital Forensic Readiness*, bentuk barang bukti yang kerap ditemukan dalam komputasi awan, framework kesiapan (readiness), aspek procedure dan legalitas barang bukti dalam komputasi awan.

3.3 Analisis Karakteristik Framework *Cloud Forensic Readiness* Pada Organisasi

Pada tahapan ini akan melakukan analisa terhadap model proses kesiapan investigasi forensik digital apa saja yang dapat dilakukan dalam komputasi awan dalam lingkup organisasi. Dengan melakukan analisa terhadap karakteristik proses investigasi forensik digital ini akan mempermudah investigasi internal maupun external dalam proses analisa dan investigasi bukti digital yang di dapatkan dari model yang berhasil diterapkan

3.4 Pembuatan Framework Dengan Metode Composite Logic

Pada tahapan ini akan menerapkan metode *Composite Logic* untuk membangun sebuah *framework* baru. Metode ini akan menggabungkan beberapa *Cloud Forensic Readiness framework* sehingga dapat menghasilakan sebuah *Integrated Cloud Forensic Readiness* .

Metode *Composite Logic* ini akan mengkombinasikan beberapa struktur model yang memiliki kesamaan menjadi sebuah model yang menyatu dengan tetap mempertahankan susunan awal dari kerangka model yang telah ada sebelumnya. Selain itu *Composite Logic* juga akan menentukan role model dari setiap variabel yang akan dikolaborasikan serta membantu dalam menentukan keterhubungan dari variabel yang ada.

Metode *Composite Logic* ini akan melakukan Identifikasi, Ekstraksi, serta kolaborasi dari beberapa *Cloud Forensic Readiness* (Kesiapan forensic dalam komputasi awan) models yang telah ada, sehingga hasil dari kolaborasi tersebut akan menghasilkan kerangka untuk membuat dan mengembangkan sebuah *framework* baru.

3.5 Analisis Evaluasi Framework

Tahapan ini merupakan proses evaluasi terhadap *framework* yang telah dirancang. Evaluasi terhadap *framework* digunakan untuk melihat kekurangan-kekurangan dalam tahapan-tahapan *framework* yang telah rancang dan di uji coba. Tahapan inilah yang akan menjadi penentu keberhasilan *framework* yang dirancang. Tahapan ini akan menghasilkan hasil pengujian yang telah dilakukan dengan studi kasus yang telah ada. Metode yang akan digunakan untuk mengevaluasi framework yang baru nanti adalah dengan cara membandingkan komponen dan tahapan yang ada dalam frame work baru ini dengan komponen dan tahapan yang ada pada *Integrated Cloud Forensic Readiness* (*icfr*) model

framework lainnya. Sehingga didapatkan kelebihan dan kekurangan dari masing-masing framework.

3.6 Kesimpulan

Pada tahapan ini adalah tahapan pengambilan kesimpulan, setelah sistem yang dibuat telah di analisa dinyatakan lulus uji, langkah berikutnya adalah penjelasan tentang kesimpulan dari keberhasilan framework yang telah dibuat.

BAB IV
Hasil dan Pembahasan

4.1 Karakteristik Kesiapan Forensik Komputasi awan

Dalam pendekatan *Forensic Readiness*, kesiap-siagaan insiden menjadi tujuan perusahaan dan terdiri dari tindakan atau langkah, teknis dan non-teknis, yang memaksimalkan kemampuan organisasi untuk menggunakan bukti digital. Setiap data komputer dapat digunakan dalam proses formal dan mungkin perlu tunduk pada praktik forensik. Kemampuan organisasi untuk mengeksploitasi data inilah yang menjadi fokus *Forensic Readiness*. Sepuluh langkah berikut menurut (Rowlingson, 2004) dapat menjelaskan kegiatan utama dalam melaksanakan program kesiapan forensik.

1. Tentukan skenario bisnis yang membutuhkan bukti digital.
2. Mengidentifikasi sumber yang tersedia dan berbagai jenis bukti potensial.
3. Tentukan persyaratan pengumpulan bukti.
4. Membangun kemampuan untuk mengumpulkan dengan aman bukti yang dapat diterima secara hukum untuk memenuhi persyaratan.
5. Menetapkan kebijakan untuk penyimpanan yang aman dan penanganan bukti potensial.
6. Pastikan pemantauan ditargetkan untuk mendeteksi dan mencegah insiden besar.
7. Tentukan keadaan ketika eskalasi ke penyelidikan formal penuh (yang mungkin menggunakan bukti digital) harus diluncurkan.
8. Melatih staf dalam kesadaran insiden, sehingga semua yang terlibat memahami peran mereka dalam proses bukti digital dan kepekaan hukum dari bukti.
9. Mendokumentasikan kasus berbasis bukti yang menggambarkan insiden dan dampaknya.
10. Pastikan tinjauan hukum untuk memfasilitasi tindakan dalam menanggapi insiden tersebut

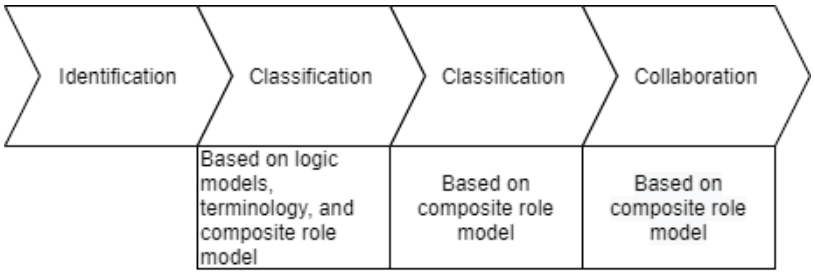
4.2 Pembuatan Framework Dengan Metode Composite Logic

Composite indicator dibentuk ketika beberapa indicator dikompilasi menjadi indeks tunggal berdasarkan model yang mendasarinya. Indikator gabungan idealnya mengukur

konsep multi dimensi yang tidak dapat dirangkum dalam satu indikator, mis. daya saing, industrialisasi, keberlanjutan, integrasi pasar tunggal, masyarakat berbasis pengetahuan, dll.(Mattes & Sloane, 2015)

Sedangkan *logic model* adalah penggambaran naratif atau grafis dari proses dalam kehidupan nyata yang mengkomunikasikan asumsi yang mendasari suatu aktivitas yang diharapkan untuk mengarah pada hasil tertentu. Model logika menggambarkan urutan hubungan sebab-akibat sebuah pendekatan sistem untuk mengkomunikasikan jalur menuju hasil yang diinginkan.(Mccawley, 2015)

Penelitian ini menggunakan Composite Logic, sebuah metode yang menggabungkan kedua teori diatas untuk mengkolaborasikan beberapa model framework Cloud Forensic Readiness yang telah ada sebelumnya. Setiap tahapan yang sama secara termilonologi akan digabungkan dan di kolaborasi sesuai *role model* nya menjadi sebuah model framework *Integrated Cloud Forensic Readiness* yang baru.



Gambar 4.1. Skema Penerapan Composite Logic

4.2.1 Identifikasi Framework *Cloud Forensic Readiness*

Sebuah *Cloud Forensic Readiness Framework* yang terangkai dengan baik dapat membantu mempercepat dan mempermudah dalam pengambilan keputusan yang berkenaan dengan sebuah insiden terjadi dalam lingkungan komputasi awan. Telah ada beberapa framework digital forensic readiness yang dikemukakan oleh peneliti lain, namun sebuah framework yang khusus membahas kesiapan forensic di lingkungan komputasi awan dalam sebuah organisasi mempunyai banyak hal untuk dibahas terlebih belum adanya sebuah standar *Integrated Cloud Forensic Readiness* yang bisa menjadi jalan tengah ketika beberapa framework lain dirasa kurang cocok dengan peraturan dan kondisi sebuah organisasi. Hal ini dikarenakan sifat dari komputasi awan yang disediakan oleh provider dan aspek legalitas setiap negara yang berbeda-beda.

Disisi lain ada juga organisasi yang membutuhkan servis tersebut karena kemudahananya maka dari itu stakeholder dalam organisasi tersebut harus menyatakan kesiapannya terhadap masalah yang bekenaan tentang pelanggaran atau kriminalitas yang bisa kapanpun terjadi, Sehingga tahapan-tahapan yang rinci dan lengkap akan dapat membantu sebuah organisasi untuk mencapai status kesiapan tertinggi sewaktu-waktu terjadi insiden dam kasus yang memerlukan investigasi digital forensic di lingkungan awan.

Pada tahapan ini, akan dilakukan identifikasi terhadap tiga jenis framework *Cloud Forensic Readiness* (*Integrated Cloud Forensic Readiness*) yang telah ada sebelumnya. Beberapa model framework ini akan dikembangkan untuk membangun *Integrated Cloud Forensic Readiness* yang dapat menjadi panduan untuk organisasi dalam membangun ekosistem Kesiapan Forensik dalam lingkungan awan. Ada tiga jenis yang akan dijadikan kajian dalam penelitian ini diantaranya sebagai berikut:

1. *A Digital Forensic Readiness Framework for South African SME's*. (Barske et al., 2010)
2. *Requirement for achieving digital forensic readiness in the environment using an NMB Solution*. (Kebande & Venter, 2016)
3. *Digital Forensic in the Cloud*. (Trenwith & Venter, 2013)
4. *Research on digital forensic readiness design in a cloud computing-based smart work environment.* (Park et al., 2018)

Berikut ini merupakan tabel hasil identifikasi dari framework *Cloud Forensic Readiness* yang disebutkan diatas.

Tabel 4.1. Hasil identifikasi *Cloud Forensic Readiness*

No	**A Digital Forensic Readiness Framework for South African SME's(Barske et al., 2010)**	**Requirement for achieving digital forensic readiness in the environment using an NMB Solution (Kebande & Venter, 2016)**	**Digital Forensic in the Cloud (Trenwith & Venter, 2013)**	**Research on digital forensic readiness design in a cloud computing-based smart work environment (Park et al., 2018)**
1	Strategy	Forensic logging capability & management	Collection of log data	Policy Readiness outside the organization environment
2	Policy & Procedure	Integrity &Authenticity	Compression	Policy Readiness Within the organization guideline

Tabel 4.2 Hasil identifikasi *Cloud Forensic Readiness* (Lanjutan)

No	A Digital Forensic Readiness Framework for South African SME's(Barske et al., 2010)	Requirement for achieving digital forensic readiness in the environment using an NMB Solution (Kebande & Venter, 2016)	Digital Forensic in the Cloud (Trenwith & Venter, 2013)	Research on digital forensic readiness design in a cloud computing-based smart work environment (Park et al., 2018)
3	Technology	Timestamping	Communication channel	Technical Readiness of system information
4	Digital Forensic Responsive	Digital Evidence Characterization	Encryption	Technical Readiness of Terminal Information
5	Compliance & Monitoring	Non-modification of existing cloud Architecture	Authentication the client & server	Technical Readiness of User Information
6		Security Implementation	Authentication of log data & proof of integrity	Technical Readiness of Usage Information
7		Obfuscation	Timestamping	Technical Readiness of Additional Information
8		Event Reconstruction		
9		Legal Requirement		
10		Forensic Reporting		

4.2.2 Proses Ekstraksi Menggunakan Pemodelan Logic, Terminologi, dan *Composite Role Model*

Pada langkah selanjutnya, tahapan-tahapan dari setiap model framework *Cloud Forensic Readiness* yang di paparkan dalam Tabel 4.1 tersebut akan dikolaborasikan. Proses ini menerapkan metode composite logic dimana setiap tahapan akan di urai berdasarkan kesesuaian terminologi dari tahapan itu sendiri. Proses ekstraksi dari empat model framework *Cloud Forensic Readiness* yang telah di identifikasi dilakukan dengan pemodelan logic, terminologi, dan *composite role model*. Kemudian pada indicator impact menggunakan role model dari *composite* yang terdiri dari *Prohibit, Implies*, dan *Don't Care.* Berikut ini merupakan uraian tata cara setiap elemen dan role model yang digunakan.

a. *Activity* merupakan tahapan yang dilakukan untuk memenuhi kebutuhan output.
b. *Output* merupakan tahapan hasil dari kegiatan yang di *input*.
c. *Rationale* merupakan tahapan secara terminologi yang di peroleh dari sumber literatur yang terkait.

d. *Assumption* merupakan tahapan yang berisikan fakta/pendapat yang diyakini benar dan memberikan pengaruh terhadap outcomes.
e. *Impact* merupakan tahapan dari hasil analisa terhadap *rationale* dan *assumption* di dalam tahapan yang saling berhubungan. Penentuan impact dari table logic model dilakukan dengan mengadaptasi role model dari *Composite Logic* model yaitu:
    - Sebuah tahapan "n" dikatan "*Implies*" jika melakukan kolaborasi terhadap tahapan lainnya. Indicator ini dapat menyebabkan terjadinya pemberian nama baru setelah dikolaborasikan karena memiliki kesamaan terminologi dengan tahapan lainnya.
    - Sebuah tahapan "n" dikatakan "*Prohibit*" jika tahapan tersebut merupakan tahapan dengan terminologi umum yang di anggap penting namun tidak terdapat dalam *Integrated Cloud Forensic Readiness* lainnya. Indikator ini dapat menyebabkan penambahan secara langsung pada tahapan ini.
    - Sebuah tahapan "n" dikatakan "*don't care*" jika tahapan tersebut memang harus tetap berada pada tahapan semula karena tidak dapat dikolaborasikan dan tidak memiliki terminlogi yang sama dengan tahapan lainnya.
f. *Outcomes* merupakan hasil akhir yang diharapkan setelah mempertimbangkan asumsi dan rasio yang ada.

Lebih jelasnya proses ini dilakukan dengan menilai atau menganalisis hasil identifikasi menggunakan enam elemen dasar dari *logic model* yaitu *Activity, Output, Rationale, Assumption, Impact,* dan *Outcomes.* Berikut ini merupakan hasil dari proses ekstraksi model framework yang sudah di identifikasi di atas:

1. Ekstraksi *A Digital Forensic Readiness Framework for South African SME's*

    Proses ekstrasi akan dilakukan terhadap *A Digital Forensic Readiness Framework for South African SME's* dengan menggunakan enam elemen dasar dari *Logic Model* dan menerapkan formula implikasi dari *Composite Logic*. Setiap tahapan akan dianalisis menurut terminologi yang mendasarinya.

Tabel 4.3. Hasil Ekstraksi "*A Digital Forensic Readiness Framework for South African SME's"*

No	Activity	Output	Impact/Indicator	Outcomes
1	**Strategy**	**Resources Identification**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Merumuskan kebutuhan regulasi dan kebutuhan sumber daya serta berbagai skenario kejahatan di lingkungan komputasi awan dalam skala organisasi.		**Assumption :** Tahapan ini dapat menjadi tahapan utama dalam Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi	
2	**Policy and procedure**	**Policy and procedure**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Merumuskan peraturan otoritas yang diperlukan untuk menyelenggarakan sebuah investigasi dan pengumpulan barang bukti berdasarkan aspek legalitas dan otentifikasi barang bukti		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
3	**Technology**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Menyiapkan kebutuhan *forensic tools* baik berupa software ataupun hardware yang menunjang pengumpulan barang bukti		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
4	**Digital Forensic Response**	**Digital Forensic Response**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Membangun mekanisme investigasi digital forensic dalam lingkungan komputasi awan pada organisasi dan proses pengumpulan barang bukti.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
5	**Compliance and Monitoring**	**Evaluation and Report**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Melakukan evaluasi berkala dan maintenance berkala		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Tabel diatas merupakan table hasil proses ekstraksi terhadap 5 tahapan *A Digital Forensic Readiness Framework for South African SME's* dengan menggunakan template logic model dan *Composite Role Model* maka dihasilkan 4 tahapan role model yang bersifat *Implies* yang memberikan output yaitu *Policy and Procedure, Technical Readiness, Digital Forensic Response, Report*.

2. Ekstraksi *Digital Forensic Readiness in the Cloud*

Proses ekstrasi akan dilakukan terhadap *Digital Forensic Readiness in the Cloud* dengan menggunakan enam elemen dasar dari *Logic Model* dan menerapkan formula implikasi dari *Composite Logic*. Setiap tahapan akan dianalisis menurut terminologi yang mendasarinya.

Tabel 4.4 Hasil Ekstraksi "*Digital Forensic Readiness in the Cloud"*

No	**Activity**	**Output**	**Impact/Indicator**	**Outcomes**
1	**Collection of Log Data**	**Digital Forensic Response**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Mengumpulkan bukti-bukti dari data log.		**Assumption :** Tahapan ini dapat menjadi tahapan utama dalam Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi	
2	**Compression**	**Digital Forensic Response**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Mengkompress kumpulan data yang berpotensi menjadi barang bukti		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
3	**Communication Channel**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Membangun jalur komunikasi antar client dan server khusus bagi data yang berpotensi menjadi barang bukti		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Tabel 4.5. Hasil Ekstraksi "*Digital Forensic Readiness in the Cloud"*(Lanjutan)

4	**Encryption**	**Digital Forensic Response**	**Tahapan ini memiliki ciri role model yang bersifat *Prohibit***	**Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi**
	Rationale /Terminologi : Mengenkripsi data yang berpotensi menjadi barang bukti		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
5	**Authentication of the client and server**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Proses validasi client dan server		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
6	**Authentication of log data and proof of integrity**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Proses validasi data log dan validasi bukti integritas		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
7	**Timestamping**	**Digital Forensic Response**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Perumusan regulasi perekaman waktu data log		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Setelah dilakukan proses ekstraksi terhadap 7 tahapan *Digital Forensic Readiness in the Cloud* dengan menggunakan template *logic model* dan *Composite Role Model* dihasilkan menghasilkan 2 tahapan role model yang bersifat *Implies* yang memberikan output *Technical Readiness, Digital Forensic Response, Policy and Procedure*.

3. Ekstraksi *Requirement for achieving digital forensic readiness in the environment using an NMB Solution*

Proses ekstrasi akan dilakukan terhadap *Requirement for achieving digital forensic readiness in the environment using an NMB Solution* dengan menggunakan enam elemen dasar dari *Logic Model* dan menerapkan formula implikasi dari *Composite Logic*. Setiap tahapan akan dianalisis menurut terminologi yang mendasarinya

Tabel 4.6. Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution"*

No	Activity	Output	Impact/Indicator	Outcomes
1	**Forensic logging capability and management**	**Resources Identification**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Log Forensik yang akan digunakan sebagai bukti digital harus dikumpulkan dalam lingkungan virtual		**Assumption :** Tahapan ini dapat menjadi tahapan utama dalam Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi	
2	**Integrity and Authenticity**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Keaslian verifikasi harus dimungkinkan jika ada kebutuhan untuk investigasi forensik digital.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
3	**Timestamping**	**Digital Forensic Response**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Setiap data log harus memiliki timestamp untuk mempertahankan integritas		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
4	**Digital Evidence characterization**	**Resources Identification**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Bukti digital harus dikelompokkan dalam format file masing-masing untuk kemungkinan identifikasi insiden. Analisis aktivitas harus dilakukan untuk mengisolasi potensi insiden keamanan.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Tabel 4.7 Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution"* (Lanjutan)

No	Activity	Output	Impact/Indicator	Outcomes
5	**Non-modification of existing cloud architecture**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Fungsi arsitektur cloud yang ada tidak diubah atau dirusak karena aktivitas pembuktian dilakukan di luar lingkungan cloud.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
6	**Security implementation**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Aplikasi perangkat lunak harus diterapkan di lingkungan awan tepercaya		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
7	**Obfuscation**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Pola aplikasi perangkat lunak diubah dengan cara yang tidak masuk akal untuk menghalangi pengawasan tanpa ijin dan untuk menghindari kegagalan mencapai tujuannya		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
8	**Event reconstruction**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Prohibit*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Hipotesis yang harus membuktikan fakta di pengadilan dikembangkan berdasarkan peristiwa.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Tabel 4.8 Hasil Ekstraksi "*Requirement for achieving digital forensic readiness in the environment using an NMB Solution" (lanjutan 2)*

No	**Activity**	**Output**	**Impact/Indicator**	**Outcomes**
9	**Legal requiement**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Perspektif hukum dan ketentuan di berbagai yurisdiksi harus diketahui sebelum investigasi forensik digital.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
10	**Forensic reporting**	**Evaluation and Report**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Laporan kesiapan yang menunjukkan proses interpretasi sebagai hasil dari penyimpanan bukti digital.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Setelah dilakukan proses ekstraksi terhadap 7 tahapan *Requirement for achieving digital forensic readiness in the environment using an NMB Solution* dengan menggunakan template *logic model* dan *Composite Role Model* dihasilkan menghasilkan 2 tahapan role model yang bersifat *Implies* yang memberikan output *Technical Readiness, Digital Forensic Response, Policy and Procedure*.

4. Ekstrasi *Research on digital forensic readiness design in a cloud computing-based smart work environment*

   Proses ekstrasi akan dilakukan terhadap *Research on digital forensic readiness design in a cloud computing-based smart work environment* dengan menggunakan enam elemen dasar dari *Logic Model* dan menerapkan formula implikasi dari *Composite Logic*. Setiap tahapan akan dianalisis menurut terminologi yang mendasarinya

Tabel 4.9. Hasil Ekstraksi "*Research on digital forensic readiness design in a cloud computing-based smart work environment"*

No	Activity	Output	Impact/Indicator	Outcomes
1	**Policy Readiness outside the organization environment**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Standar / pedoman dan persyaratan hukum terkait forensik digital, kemudian membangun kontak tunggal dengan organisasi penegak hukum		**Assumption :** Tahapan ini dapat menjadi tahapan utama dalam Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi	
2	**Policy Readiness Within the organization guideline**	**Policy and Procedure**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Menyiapkan solusi forensik, Siapkan peralatan forensik, dll. Validitas rata-rata dalam organisasi		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
3	**Technical Readiness of system information**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Analisis informasi sistem dasar, waktu sistem hidup/mati		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
4	**Technical Readiness of Terminal Information**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : mengamankan memori volatilitas di dalam terminal, pengumpulan barang bukti seperti microSD, Flash disk, dll		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

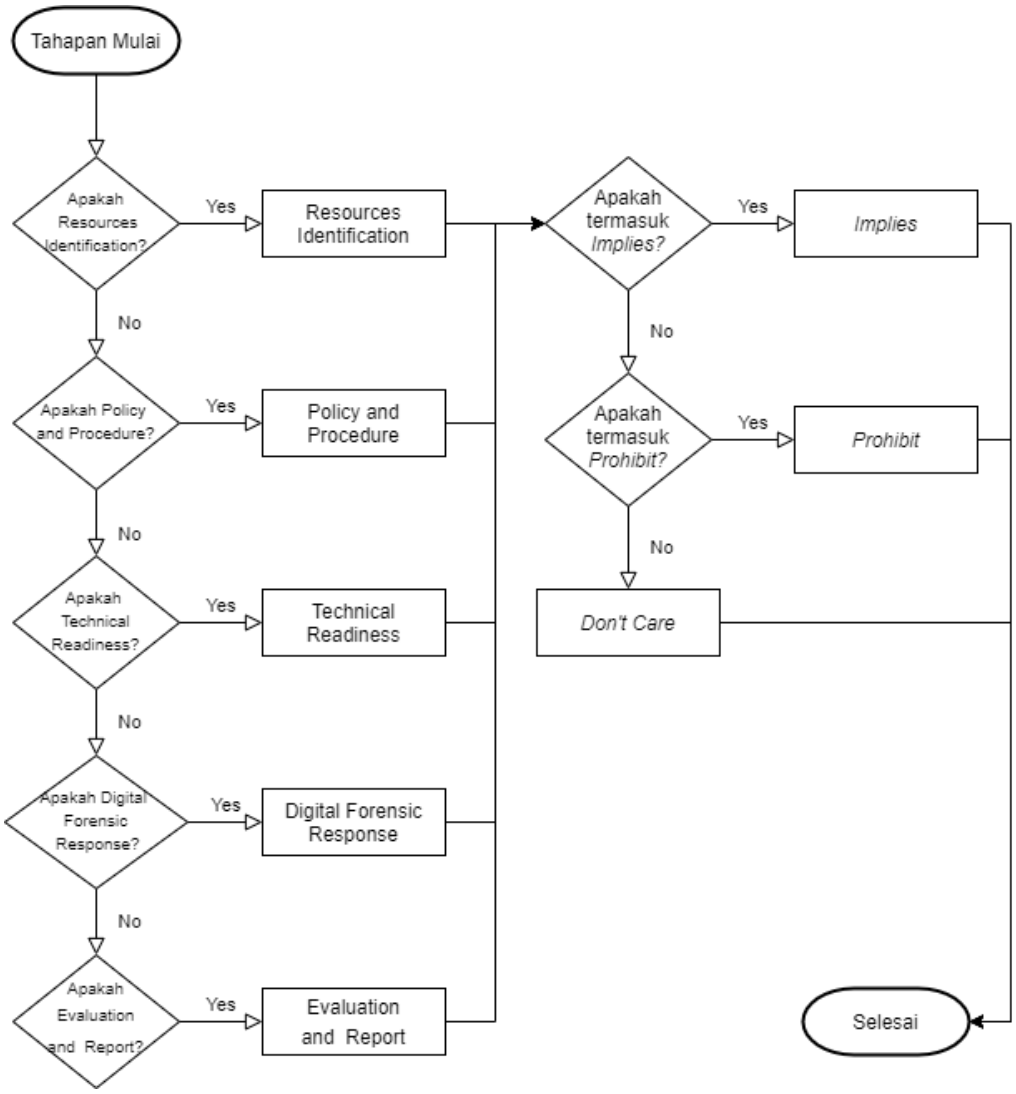
Tabel 4.10 Hasil Ekstraksi "*Research on digital forensic readiness design in a cloud computing-based smart work environment"*(Lanjutan)

No	Activity	Output	Impact/Indicator	Outcomes
5	**Technical Readiness of User Information**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Analisis informasi akun pengguna Teknis, Analisis registri pengguna, Analisis informasi situs web yang dikunjungi pengguna		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
6	**Technical Readiness of Usage Information**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Analisis timeline artefak window, Analisis timeline artefak OS seluler (Android / iOS, dll.),Analisis timeline MAC file, Analisis tindakan berdasarkan timeline.		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	
7	**Technical Readiness of Additional Information**	**Technical Readiness**	Tahapan ini memiliki ciri role model yang bersifat *Implies*	Tahapan ini dibutuhkan dalam perancangan Framework *Integrated Cloud Forensic Readiness* terintegrasi pada organisasi
	Rationale /Terminologi : Pencarian file yang cepat, Analisis pencarian file besar, Analisis keberadaan file yang tidak sah dan pencarian file terenkripsi dan dekripsi		**Assumption :** Tahapan ini dapat dikolaborasikan karena memiliki terminologi yang sama dengan tahapan lainnya	

Setelah dilakukan proses ekstraksi terhadap 7 tahapan *Research on digital forensic readiness design in a cloud computing-based smart work environment* dengan menggunakan template *logic model* dan *Composite Role Model* dihasilkan menghasilkan 2 tahapan role model yang bersifat *Implies* yang memberikan output *Technical Readiness, Policy and Procedure.*

4.2.3 Klasifikasi Menggunakan Composite *Logic* Model

Setelah proses ekstraksi empat *Cloud Forensic Readiness models* dilakukan, selanjutnya akan dilakukan proses klasifikasi dari empat model tersebut berdasarkan variabel output yaitu dan indikator *role model* yaitu *Implies, Prohibit, dan Don't care.*



Gambar 4.2. Flowchart Proses Pengklasifikasian

Proses klasifikasi ini dilakukan untuk mempermudah proses pembuatan *framework* baru karena hasil dari variabel *output* merupakan tahapan-tahapan hasil ekstraksi dari setiap framework *Integrated Cloud Forensic Readiness* yang ada. Hasil dari variabel Output ini kemudian dapat dijadikan sebagai kerangka awal untuk perancangan *framework* baru. Pada proses kolaborasi ini, indikator *role model* yang bersifat *Implies* akan olaborasikan karena memiliki terminology yang sama dengan tahapan *Integrated Cloud Forensic Readiness* yang lainnya. Alur proses pengklasifikasian dapat dilihat seperti gambar 4.2.

Proses pengklasifikasian akan dilakukan seperti pada gambar 4.2, Hasil dari klasifikasi ini akan menghasilkan sebuah tabel yang menampilkan indikator role model.

Indikator *implies*, indikator prohibi, dan indikator Don't Care. Proses visualisasi dengan perwarnaan ini dilakukan untuk mempermudah dalam membedakan indikator yang ada.

Tabel 4.11. Hasil Klasifikasi Menggunakan *Composite Logic*

Jenis	Resources Identification	Policy & Procedure	Technical Readiness	Digital Forensic Response	Evaluation & Report
Implies	Strategy	Authentication of the client and server	Non-modification of esixting cloud architecture	Digital Forensic Response	Forensic Reporting
		Authentication of log data and proof of integrity	Technical Readiness of System Information	Collection of Log data	
		Integrity and authenticity	Technical Readiness of terminal information	Timestamping	
		Security Implementation	Technical Readiness of usage information	Timestamping	
		Legal requirement	Technical Readiness of additional information		
		Policy readiness outside organization			
		Policy readiness within organization			
Prohibit	Forensic logging capability & management	Policy & Procedure	Technology	Compression	Compliance & Monitoring
	Digital Evidence Characterization		Communication Channel	Encryption	
				Event Reconstruction	
Don't Care		Obfuscation			

Tabel 4.11 merupakan tabel hasil klasifikasi berdasarkan *role model*. Proses klasifikasi yang terlihat pada tabel 4.6 dilakukan dengan mengadaptasi role dari *Composite Role Model* yaitu :

a. Sebuah tahapan n dikatakan "*Implies*" jika melakukan kolaborasi terhadap tahapan lainnya, indikator ini dapat menyebabkan terjadinya pemberian nama

baru setalah dikolaborasikan dikarenakan memiliki kesamaan terminologi dengan tahapan lainnya. Pada setiap entry role model yang dilakukan dengan menggunakan persamaan sebagai berikut:

Formula implikasi logika $(A \Rightarrow B)$ (4.1)

b. Sebuah tahapan n dikatakan "*Prohibit*" jika tahapan tersebut merupakan tahapan dengan terminologi umum, dianggap penting namun tidak terdapat dalam framework *Integrated Cloud Forensic Readiness* lainnya. Indikator ini dapat menyebabkan penambahan secara langsung tahapan ini.

Formula implikasi logika $(A \Rightarrow B)$ (4.2)

c. Sebuah tahapan n dikatakan "*Don't care*" jika tahapan tersebut memang harus tetap berada pada tahapan semula karena tidak dapat dikolaborasikan dan tidak memiliki terminologi yang sama dengan tahapan lainnya.

4.2.4 Kolaborasi Menggunakan *Composite Role Model*

Setelah proses klasifikasi dilakukan, tahapan selanjutnya adalah tahapan kolaborasi dengan menggunakan *Composite Role Model*. Pada tahapan kolaborasi ini, akan dikolaborasikan role model yang bersifat *Implies.* Proses ini adalah kolaborasi terhadap tahapan yang memiliki penamaan dan terminologi yang sama, sehingga indikator ini dapat menyebabkan terjadinya pemberian nama baru setelah dikolaborasikan. Kolaborasi tahapan yang memiliki role model *Implies* dengan nama dan terminologi

Tabel 4.12. Hasil Kolaborasi Menggunakan *Composite Role Model*

Resources Identification	**Policy & Procedure**	**Technical Readiness**	**Digital Forensic Response**	**Evaluation & Report**
Forensic logging capability & management	Policy & Procedure	Technology	Digital Forensic Response	Compliance & Monitoring
Digital Evidence Characterization	Integrity and authenticity	Communication Channel	Compression	Forensic Reporting
	Security Implementation	Non-modification of esixting cloud architecture	Encryption	
	Legal requirement		Event Reconstruction	

4.2.5 Perancangan Framework

Dari hasil kolaborasi dengan menggunakan *Composite Logic*, maka dihasilkan sebuah *framework* hasil kolaborasi yang akan digunakan sebagai perancangan *framework*

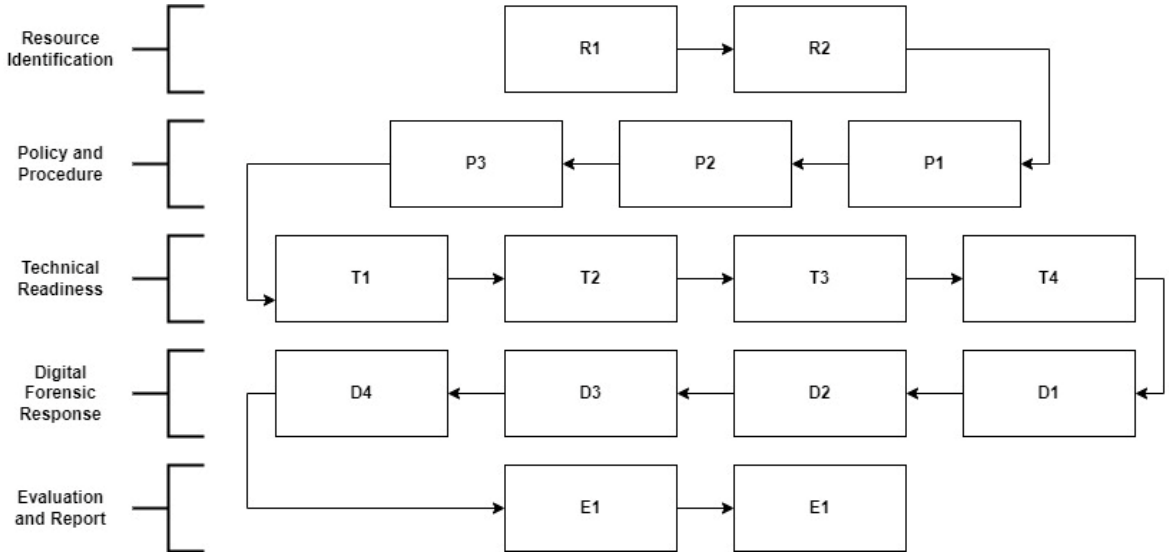
Setelah tahapan-tahapan tersebut diklasifikasikan berdasarkan variabel output dan indikatornya (role model) maka proses selanjutnya adalah mengkolaborasikan setiap tahapan dengan indikator (role model) "*implies"*. Pengkolaborasian tahapan ini hanya akan diterapkan pada tahapan dengan indikator "*implies*" dikarenakan tahapan tersebut memiliki kesamaan terminologi satu dengan yang lainnya.

Pemilihan nama/istilah pada tahapan dengan terminologi yang sama akan merujuk kepada definisi dan terminologi yang dianggap bisa mewakili tahapan lainnya, atau tahapan dengan terminologi yang lebih bersifat umum yang merujuk kepada beberapa sumber literature dan dokumen resmi. Dengan kata lain, tahapan ini merupakan proses merger dan bukan merupakan proses eliminasi.

Tabel 4.13. Tahapan *Framework* awal

No	**Tahapan *Framework* Hasil Kolaborasi**	**ID**
Resources Identification		**R**
1	Forensic logging capability & management	**R1**
2	Digital Evidence Characterization	**R2**
Policy & Procedure		**P**
3	Policy & Procedure	**P1**
4	Integrity and authenticity	**P2**
5	Security Implementation	**P3**
6	Legal requirement	**P4**
Technical Readiness		**T**
7	Technology	**T1**
8	Communication Channel	**T2**
9	Non-modification of esixting cloud architecture	**T3**
Digital Forensic Response		**D**
10	Digital Forensic Response	**D1**
11	Compression	**D2**
12	Encryption	**D3**
13	Event Reconstruction	**D4**
Evaluation and Report		**E**
14	Compliance & Monitoring	**E1**
15	Forensic Reporting	**E2**

Untuk alur dalam *framework* hasil kolaborasi tersebut dapat dilihat pada gambar 4.3. Alur ini menjelaskan tahapan awal sampai tahapan akhir dalam tahapan *framework* hasil kolaborasi yang kemudian akan dijadikan sebagai *Cloud Forensic Readiness Framework* terintegrasi.



Gambar 4.3. Alur *framework*

Pada tabel 4.13, ada beberapa tahapan hasil rancangan *framework* baru tidak terdapat tahapan pada *framework Cloud Forensic Readiness Models* yang dijadikan dasar untuk perancangan *framework* baru. Selain itu, pada *Cloud Forensic Readiness Framework* terintegrasi, memiliki jumlah tahapan *framework* yang lebih sedikit dibandingan jumlah tahapan pada *framework* yang di jadikan dasar perancangan. Hal ini terjadi karena ada beberapa tahapan pada tahapan pada *Cloud Forensic Readiness Models* yang telah di kolaborasikan dan diberikan penamaan yang baru. Penjelasan dari setiap tahapan pada rancangan awal *Cloud Forensic Readiness Framework* terintegrasi ini sebagai berikut :

A. Tahapan *Resource Identification* **(R)** merupakan tahapan awal untuk menganalisis sumber daya yang dapat ditemukan atau dimiliki oleh sebuah organisasi dalam menerapkan .
    1. *Forensic logging capability and management* **(R1)** merupakan tahapan mengukur kapasitas kemampuan menyimpan catatan rekaman log forensic dan kapasitas pengolahannya.
    2. *Digital Evidence Characterization* **(R2)** adalah proses identifikasi bukti digital berdasrkan kriteria seperti format file, dll. Proses identifikasi harus di

analisis dengan cermat untuk menghindari insiden yang berpotensi menyebabkan kesalahan keamanan.

B. Tahapan *Policy and Procedure* **(P)** merupakan tahapan yang menjelaskan dan memaparkan kebuthan aturan dan prosedur dalam pelaksanaan investigasi forensic dalam lingkungan awan
    1. *Policy & Procedure* **(P1)** merupakan tahapan mengukur kapasitas kemampuan menyimpan catatan rekaman log forensic dan kapasitas pengolahannya.
    2. *Integrity and atuthenticity* **(P2)** merupakan proses penyimpanan barang bukti yang dapat dipertanggungjawabkan validitas dan keasliannya.
    3. *Security Implementation* **(P3)** merupakan proses untuk memastikan bahwa software tools tambahan didapat dari vendor yang dapat dipercaya dan system kemanannya terjamin.
    4. *Legal Requirement* **(P4)** merupkan proses dalam rangka mengetahui keseluruhan persyaratan legal yang mengatur ketentuan sebuah investigasi computer forensik
C. Tahapan *Technical Readiness* **(T)** merupakan tahapan untuk mengukur kesiapan organisasi yang bersifat teknis.
    1. *Technology* **(T1)** merupakan tahapan mengukur kesiapan infrastruktur yang dapat digunakan dalam proses investigasi.
    2. *Communication Channel* **(T2)** adalah tahapan pembangunan inovasi oleh (Trenwith & Venter, 2013) dimana beliau mengemukanan sebuah model perpindahan data log atau bukti digital dalam suatu mekanisme yang menjamin keaslian dan validitas data.
    3. Non-modification of esixting cloud architecture **(T3)** merupakan tahapan untuk memastikan keadaan arsiktekur komputasi awan yang ada tidak terjamah atau belum pernah terjamah.
D. Tahapan *Digital Forensic Response* **(D)** merupakan tahapan yang mencakup proses respon ketika sebuah insiden terjadi.
    1. *Digital Forensic Response* **(D1)** merupakan tahapan untuk memastikan kesiapan sebuah respon terhadap insiden yang terjadi dan kesiapan

melaksanakan investigasi baik melalui organisasi independent maupun secara internal organisasi.

2. *Compression* (**D2)** adalah proses menggabungkan semua informasi baik barang bukti maupun data log investigasi yang dibutuhkan dalam satu file.
3. *Encryption* **(D3)** adalah proses mengamankan data informasi untuk menjamin keamanannya.
4. *Event Recontruction* **(D4)** adalah sebuah hipotesa yang runtut berdasarkan waktu kejadian untuk memudahkan investigator dalam menganalisis alur kasus.

E. Tahapan *Evaluation and Report* **(E)** merupakan tahapan proses evaluasi terhadap kesiapan forensik digital yang di terapkan dalam sebuah organisasi.

1. *Compliance & Monitoring* **(E1)** merupakan upaya menjaga komitmen terhadp system kesiapan forensic yang disepakati dan melakukan pemeliharaan secara berkala.
2. *Forensic Reporting* **(E2)** adalah proses mempresentasikan hasil investigasi forensic yang telah selesai dilakukan.

4.3 Implementasi *Cloud Forensic Readiness* Terintegrasi

Implementasi dari *Cloud Forensic Readiness* terintegrasi yang selesai dirancang akan dilakukan dalam sebuah skenario kasus. Tahapan skenario kasus ini dilakukan untuk melakukan pengujian terhadap *framework* yang telah di rancang. Skenario kasus yang digunakan untuk pengujian *framework* ini kasus tentang sebuah organisasi (instansi) Pengadilan Agama Bantaeng yang memanfaatkan layanan komputasi awan pribadi dimana jaringan computer local dokumen penting yang diperlukan dalam pelaksanaan program kerja sehari-hari oleh instansi Pengadilan Agama Bantaeng.

Menimbang dari pentingnya media penyimpanan ini untuk digunakan sebagaimana mestinya, dan untuk menghindari penyalah-gunaan dari fasilitas ini, maka stake holder organisasi (Instansi) Pengadilan Agama Bantaeng berinisiatif untuk menerapkan aturan dan prosedur yang berkaitan dengan penggunaannya.

4.4 Analisa Evaluasi *Framework*

Dalam hal penerapan framework kesiapan forensik, *Integrated Cloud Forensic Readiness* akan bertindak sebagai tindakan yang akan lebih meningkatkan penggunaan dan manfaat infrastruktur tersebut dan mengurangi kemungkinan penyalahgunaan infrastruktur. Dalam hal ini, karena *Integrated Cloud Forensic Readiness* adalah kerangka kerja yang dibangun dengan asumsi bahwa insiden pasti akan terjadi, penting untuk mengevaluasi apakah kerangka kerja tersebut cukup memenuhi syarat untuk dapat dilakukan berdasarkan kemampuan organisasi, dan atau jika kemungkinan insiden yang terjadi masih dapat diselesaikan dalam lingkup pribadi instansi itu sendiri.

4.4.1 Evaluasi Terhadap Framework yang ada

Berdasarkan data dan fakta yang telah diperoleh dalam penelitian ini rancangan cloud forensic readiness ini dapat digunakan dalam proses development sebuah system kesiapan investigasi forensic sewaktu-waktu terjadi insiden pada organisasi. Beberapa tahapan yang tidak ada dalam framework lain, menjadi terlengkapi dengan framework ini seperti yang terlihat pada table 4.15. Perancangan framework ini dilakukan dengan menggunakan metode Composite Logic.

Perancangan framework ini dilakukan dengan menggunakan metode Composite Logic.Penerapan metode Composite Logic pada perancangan framework ini dilakukan dengan melakukan kolaborasi terhadap tahapan-tahapan yang terdapat pada empat framework A *Digital Forensic Readiness Framework for South African SME's* (Barske et al., 2010), *Digital Forensic in the Cloud* (Trenwith & Venter, 2013)**,** *Requirement for achieving digital forensic readiness in the environment using an NMB Solution* (Kebande & Venter, 2016), dan *Digital Forensic in the Cloud Research on digital forensic readiness design in a cloud computing-based smart work environment* (Park et al., 2018).

Tabel dibawah ini merupakan table evaluasi framework yang didasarkan pada perbandingan literatur review dari beberapa rancangan *Integrated Cloud Forensic Readiness* sebelumnya dan rancangan *Integrated Cloud Forensic Readiness* terintegrasi. Dari hasil evaluasi terlihat bahwa Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness mencakupi beberapa tahapan yang belum ada dalam penelitian rancangan *Integrated Cloud Forensic Readiness* sebelumnya.

Tabel 4.14. Evaluasi *framework*

No	Tahapan-tahapan	**Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness**	**Conceptual Forensic Readiness Framework for Infrastructure as a Service Consumers** (Moussa et al., 2014)	**A Framework for Cloud Forensic Readiness in Organizations** (Alenezi et al., 2017)
1	Forensic logging capability & management	✓	**x**	✓
2	Digital Evidence Characterization	✓	**x**	**x**
3	Policy & Procedure	✓	✓	✓
4	Integrity and authenticity	✓	✓	✓
5	Security Implementation	✓	**x**	**X**
6	Legal requirement	✓	✓	✓
7	Technology	✓	✓	✓
8	Communication Channel	✓	**x**	**X**
9	Non-modification of existing cloud architecture	✓	**x**	✓
10	Digital Forensic Response	✓	✓	**X**
11	Compression	✓	✓	**X**
12	Encryption	✓	**x**	**X**
13	Event Reconstruction	✓	**x**	**X**
14	Compliance & Monitoring	✓	✓	**X**
15	Forensic Reporting	✓	**X**	**X**

Tahapan-tahapan *pada Cloud Forensic Readiness Models* yang memiliki penamaan dan terminologi yang sama di kolaborasikan dan diberikan penamaan yang baru sesuai dengan kebutuhan framework ini. Perancangan framework ini menghasilkan beberapa tahapan yang belum ada pada tahapan lainnya. Beberapa penelitian sebelumnya telah mengembangkan berbagai jenis *framework* untuk kebutuhan investigasi dalam bidang *Digital Forensic* di lingkungan komputasi awan. Penelitian tersebut antara lain seperti *Framework for Infrastructure as a Service Consumers(Moussa et al., 2014)* dan *Forensic Readiness in Organizations* (Alenezi et al., 2017).

Akan tetapi, berbagai pengembangan *framework* tersebut belum mencangkup dan memenuhi kebutuhan untuk parameter kesiapan investigasi forensik secara keseluruhan seperti yang terlihat dalam table di atas. Tahapan-tahapan yang terdapat dalam *Integrated*

Cloud Forensic Readiness terintegrasi yang baru ini tidak hanya mampu menjebatani kebutuhan legalitas dengan kesiapan forensic digital di linkungan awan namun juga memberikan tahapan detail yang diperlukan dalam sebuah pembangungan sistem kesiapan dalam sebuah organisasi. Dimana ini merupakan manfaat dari perancangan terintegrasi yang berasal dari beberapa framework kesiapan lingkungan awan, dikaji dan dikolaborasikan sesuai dengan etimologi nya sehingga mengasilkan tahapan yang terintegrasi.

4.4.2 Evaluasi Terhadap Implementasi Framework

Evaluasi yang akan dilakukan terhadap implementasi framework dilakukan menggunakan metode quantitative/black-box dimana, metode ini memfokuskan pada evaluasi fungsi dan utilitas setiap tahapan framework yang diterapkan dalam sebuah organisasi dari rangkaian pertanyaan yang menggambarkan kemampuan organisasi dalam penerapan setiap tahapan dalam *Integrated Cloud Forensic Readiness* di lingkungan organisasi/ Institusi pengadilan Agama Bantaeng.

Aplikasi SIPP adalah salah satu aplikasi pengelohan perkara pengadilan dan beberapa aplikasi lokal pada pengadilan Agama Bantaeng berjalan dalam *private cloud environment* menggunakan jaringan LAN lokal yang menghubungkan server utama dengan beberapa user pengguna (workstation). Jaringan ini kemudian juga terhubung dengan jaringan ethernet melalui teknologi microtik untuk memadai pada saat proses synchronisasi database yang dilakukan setiap hari. Oleh karena itu keamanan jaringan seharusnya menjadi perhatian yang cukup penting, mengingat system jaringan yang rentan terhadap insiden yang di akibatkan resiko virus dan malware yang di bawa oleh PC pengguna dalam kantor. Untuk mencapai hal itu selain menerapkan prosedur pencegahan insiden, stakeholder dapat memilih untuk menerapkan kerangka kerja *Integrated Cloud Forensic Readiness* untuk mengatasi hal-hal yang berkaitan dengan pasca insiden.

Gambar 4.4. Tampilan Muka Aplikasi SIPP

Evaluasi di laksanakan dengan wawancara langsung kepada tim IT yang menjadi admin dan pejabat penanggung jawab keseluruhan infrastruktur IT dalam lingkungan Pengadilan Agama Bantaeng. Berikut merupakan hasil dari evaluasi yang dilaksanakan.

Tabel 4.15. Tabel evaluasi framework terhadap organisasi Pengadilan Agama Bantaeng

Resource Identification **(R)**	
Forensic logging capability and management **(R1)**	Pengadilan Agama Bantaeng **tidak** memiliki peralatan elektronik khusus yang dapat merekam informasi khususnya yang berkaitan dengan penyelidikan forensic, namun memiliki kapasitas dalam penyelidikan forensic yang terbatas dengan menggunakan bantuan software pihak ketiga.
Digital Evidence Characterization **(R2)**	Walaupun pengadilan agama bantaeng memiliki sumber daya yang memungkinkan untuk setidaknya mengidentifikasi bukti digital potensial dan membuat kerangka kerja dalam penyelidikan internal.
Policy and Procedure **(P)**	
Policy & Procedure **(P1)**	Organisasi memiliki kebijakan mendefinisikan scenario bisnis yang memerlukan bukti digital, informasi apa yang harus dipertahankan dalam keadaan tertentu, tenggang waktu, aksesbilitasnya, dan kondisi yang diperlukan sesuai dengan undang-undang atau peraturan organisasi dalam hal ini tercantum dalam SKKMA no 268 tahun 2018.
Integrity and authenticity **(P2)**	Organisasi memiliki tahapan prosedur yang dapat diandalkan dalam mengumpulkan bukti pasca-insiden yang dapat diterima/divalidasi hal ini telah tercantum dalam SKKMA no 268 tahun 2018.
Security Implementation **(P3)**	Organisasi mempunyai prosedur dalam pembanguna infrastruktur IT dan penggunaan software tools tambahan pendukungnya telah didapat dari vendor yang dapat dipercaya dan system kemanannya terjamin.
Legal Requirement **(P4)**	Organisasi memiliki kebijakan yang menetapkan perlunya kepatuhan terhadap kerangka aturan organisasi, undang-undang dan/atau peraturan pemerintah. Organisasi juga mendefinisikan otoritas hukum dalam manajemen dan proses yang diperlukan selama pemantauan dan pemeriksaan selama penyidikan.
Technical Readiness **(T)**	
Technology **(T1)**	Organisasi memiliki kemampuan untuk melakukan investigasi forensic secara mandiri berdasarkan peralatan infrastrukturnya namun masih terbatas.
Communication Channel **(T2)**	Organisasi memiliki prosedur dan aplikasi pencatatan data (log) data terpusat sehingga mudah untuk dilakukan audit terhadap datanya sekaligus memudahkan pemantauan akses data dari pusat instansi, hal ini tertuang dalam SKKMA no 268 tahun 2018.
*Non-modification of existing cloud architecture **(T3)***	Organisasi memiliki panduan prosedur formal yang menekankan autentifikasi arsitektur infrastruktur IT dan ketentuan untuk tidak memodifikasi arsitektur tersebut, hal ini tertuang dalam SKKMA no 268 tahun 2018.

Tabel 4.16. Tabel evaluasi framework terhadap organisasi Pengadilan Agama Bantaeng Lanjutan..

Digital Forensic Response **(D)**	
Digital Forensic Response **(D1)**	Organisasi **tidak** memiliki prosedur pembentukan tim ketika terjadi insiden dikarenakan keterbatasan sumber daya manusia, namun memiliki prosedur penanganan insiden seperti yang tertuang dalam SKKMA no 268 tahun 2018.
Compression (**D2)**	Organisasi **tidak** memiliki teknologi pencitraan dengan fungsi kompressi dan hashing lossless untuk melestarikan autentifikasi barng bukti
Encryption **(D3)**	Organisasi **tidak** menggunakan standar enkripsi dalam penanganan barang bukti dikarenakan masih terbatasnya pengetahuan mengenai fungsi enkripsi dalam penanganan barang bukti
Event Reconstruction **(D4)**	Organisasi dapat dan memiliki aturan prosedur untuk menarik linimasa, durasi insiden berdasarkan alur waktu kejadiaan insiden dan mengantisipasi kebutuhan penemuan serta mempercepat penyelidikan.
Evaluation and Report **(E)**	
Compliance & Monitoring **(E1)**	Organisasi memiliki prosedur yang menjelaskan konfigurasi dan penggunaan mekanisme pemantauan dan pencatatan aktif (log) dari data yang mengalir dalam usahanya untuk mendeteksi dan mencegah insiden dalam kegiatan penggunaan sistem informasi.
Forensic Reporting **(E2)**	Organisasi memiliki aturan prosedur untuk membuat laporan berdasarkan pelaksanaan kegiatan teknologi informasi termasuk keberhasilan dalam menangani dan memulihkan sistem dari sebuah insiden.

Tabel 4.16 dan 4.17 diatas menjelaskan pertanyaan atau pernyataan yang ditujukan kepada organisasi untuk menilai komitmen pelaksanakan kerangka kerja (framework) kesiapan cloud forensic terintegrasi yang telah dirancang. Dapat dilihat bahwa organisasi/ institusi Pengadilan Agama Bantaeng menilai positif pernyataan tersebut yang mengartikan bahwa kerangka kerja (framework) tersebut dapat difungsikan sesuai dengan keadaan organisasi (institusi). Namun menjadi perhatian karna ada beberapa tahap yang tidak bisa difungsikan dikarenakan terbatasnya sumberdaya yang ada seperti pengadaan alat perekaman informasi, dan terbatasnya pengetahuan akan ilmu forensic untuk menerapkan SOP yang berkaitan dengan pelestarian bukti digital.

Dalam framework cloud forensic readiness erat kaitannya dengan pembentukan tim khusus agar dapat menangani insiden dan melakukan penyidikan forensic secara internal agar insiden dapat segera tertangani sebelum organisasi mendapatkan kerugian secara fisik (nama baik) maupun materiil(finansial). Namun dalam sistem informasi pemerintahan (e-

gov) dimana penanganan resiko insiden secara internal belum menjadi perhatian utama dalam pembangunan infrastruktur dikarenakan sumberdaya yang terbatas, sulit untuk menerapkan framework kesiapan berbasis komputasi awan ini.

Integrated Cloud Forensic Readiness justru menjadi kekuatan yang cukup membantu jika di terapkan di organisasi/intitusi berbasis consumen dan profit dimana penanganan insiden yang cepat dan akurat serta kredibilitas barang bukti menjadi sangat penting untuk penyelesaian sebuah insiden. Dengan penanganan insiden yang cepat, organisasi/institusi/perusahaan berpotensi menyelematkan nama baik yang bisa mudah terpengaruh oleh opini masyarakat tentang keamanan data privasi yang mereka simpan di organisasi/institusi/perusahaan tersebut, seperti perusahaan game, asuransi dll. Sama halnya dengan manfaat kesiapan forensic di lingkungan awan yang juga berpengaruh pada keuntungan (profit) dan keamanan data keuangan seperti halnya pada pelayanan perbankan.

BAB V
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, maka didapatkan kesimpulan bahwa metode composite logic dapat diterapkan dalam membangun sebuah framework cloud forensic readiness terintegrasi dengan cara mengidentifikasi, mengektraksi, mengklasifikasi, dan mengkolaborasi beberapa *Integrated Cloud Forensic Readiness* models yang berbeda dengan menggunakan pemodelan logic berdasarkan terminologi dan composite role model yang menghasilkan 5 tahapan utama dengan 15 sub-tahapan. Penggunaan metode composite logic mampu membantu peneliti dalam menggabungkan beberapa framework menjadi satu kesatuan dengan tidak menghilangkan fungsi dan struktur dasar dari framework yang peneliti jadikan sebagai bahan kajian.

Dalam framework cloud forensic readiness erat kaitannya dengan pembentukan tim khusus agar dapat menangani insiden dan melakukan penyidikan forensic secara internal agar insiden dapat segera tertangani sebelum organisasi mendapatkan kerugian secara fisik (nama baik) maupun materiil(finansial). Namun dalam system informasi pemerintahan (e-gov) dimana penanganan resiko insiden secara internal belum menjadi perhatian utama dalam pembangunan infrastruktur dikarenakan sumberdaya yang terbatas, sulit untuk menerapkan framework kesiapan berbasis komputasi awan ini.

Integrated Cloud Forensic Readiness justru mempunyai potensi menjadi kekuatan yang cukup membantu jika di terapkan di organisasi/intitusi berbasis *consumers* dan profit dimana penanganan insiden serta pengumpulan barang bukti kredibel dan akurat yang cepat menjadi sangat penting untuk meningkatkan kepercayaan masyarakat/pengguna jasa organisasi/ institusi tersebut.

5.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut :

- Framework Kesiapan forensic di lingkungan awan masih mempunyai banyak celah untuk diteliti seperti penelitian untuk melakukan evaluasi pada layanan

komputasi awan yang berbasis patform dan jasa dimana dalam pelaksanaannya akan melibatkan pihak ketiga seperti CSP (*Cloud Service Provider*)

- Sebuah framework kesiapan yang akan di terapkan dalam sebuah organisasi selayaknya mudah dimengerti bahkan untuk orang awam sehingga memudahkan para stake holder sebuah organisasi untuk menarik keputusan.
- Sebuah penelitian framework kesiapan yang lebih merucut dan berfokus pada salah satu bentuk tipe sistem informasi, misalnya: e-gov, enterprise, perbankan dll. Karena fokus pelayanan dalam penyajian informasi dari berbagai tipe system informasi berbeda sehingga memungkinkan perbedaan prosedur seperti halnya dalam e-gov yang mengedepankan transparasi sebanyak mungkin data selain data privasi, enterprise yang membatasi transparasi data namun tetap ingin mempertahankan kredibilitas.

Daftar Pustaka

ACPO. (2012). ACPO Good Practice Guide. *Acpo*, *March*, 43.

Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*(1). https://doi.org/10.1186/s13677-019-0133-z

Alenezi, A., Hussein, R. K., Walters, R. J., & Wills, G. B. (2017). A Framework for Cloud Forensic Readiness in Organizations. *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, *April*, 199–204. https://doi.org/10.1109/MobileCloud.2017.12

Alex, M. E., & Kishore, R. (2017). Forensics framework for cloud computing. *Computers and Electrical Engineering*, *60*, 193–205. https://doi.org/10.1016/j.compeleceng.2017.02.006

Barske, D., Stander, A., & Jordaan, J. (2010). A digital forensic readiness framework for South African SME's. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. https://doi.org/10.1109/ISSA.2010.5588281

Grispos, G., Storer, T., & Glisson, W. B. (2013). Calm before the storm: The challenges of cloud computing in digital forensics. *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*, *May 2014*, 211–233. https://doi.org/10.4018/978-1-4666-4006-1.ch015

Karie, N., & Karume, S. (2017). Digital Forensic Readiness in Organizations: Issues and Challenges. *The Journal of Digital Forensics, Security and Law*, *January*. https://doi.org/10.15394/jdfsl.2017.1436

Kebande, V., & Venter, H. (2016). Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*, *March*, 399–406.

Lizarti, N., Sugiantoro, B., & Prayudi, Y. (2017). *Penerapan Composite Logic Dalam Mengkolaborasikan*. *2*(1), 26–33.

Marco, L. De, Ferrucci, F., & Kechadi, M. (2013). *Cloud Forensics Challenges and Readiness Cloud Forensic Challenges and Readiness*. *April 2020*.

Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: OwnCloud as a case study. *Digital Investigation*. https://doi.org/10.1016/j.diin.2013.08.005

Mattes, M. D., & Sloane, M. A. (2015). Reflections on hope and its implications for end-

of-life care. In *Journal of the American Geriatrics Society* (Vol. 63, Issue 5). https://doi.org/10.1111/jgs.13392

Mccawley, P. F. (2015). *for Program Planning and Evaluation*. *September*, 1–5.

Moussa, A. N., Ithnin, N. B., & Miaikil, O. A. M. (2014). Conceptual forensic readiness framework for infrastructure as a service consumers. *Proceedings - 2014 IEEE Conference on System, Process and Control, ICSPC 2014, January 2018*, 162–167. https://doi.org/10.1109/SPC.2014.7086250

Nardo, M., Saisana, M., Saltelli, A., & Tarantola, S. (2008). *Handbook of Contructing Compsoite Indicators: Methodology and user guide*. https://doi.org/10.1787/9789264043466-en

NIST. (2014). NIST - Draft NISTIR 8006 - NIST Cloud Computing Forensic Science Challenges. *Nist*. http://safegov.org/media/72648/nist_digital_forensics_draft_8006.pdf

Park, S., Kim, Y., Park, G., Na, O., & Chang, H. (2018). Research on digital forensic readiness design in a cloud computing-based smart work environment. *Sustainability (Switzerland)*, *10*(4), 1–24. https://doi.org/10.3390/su10041203

Ras, D. J. (2018). *Digital Forensic Readiness Architecture for Cloud Computing Systems*.

Rowlingson, R. (2004). *International Journal of Digital Evidence Winter 2004 , Volume 2 , Issue 3 A Ten Step Process for Forensic Readiness International Journal of Digital Evidence*. *2*(3), 1–28. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

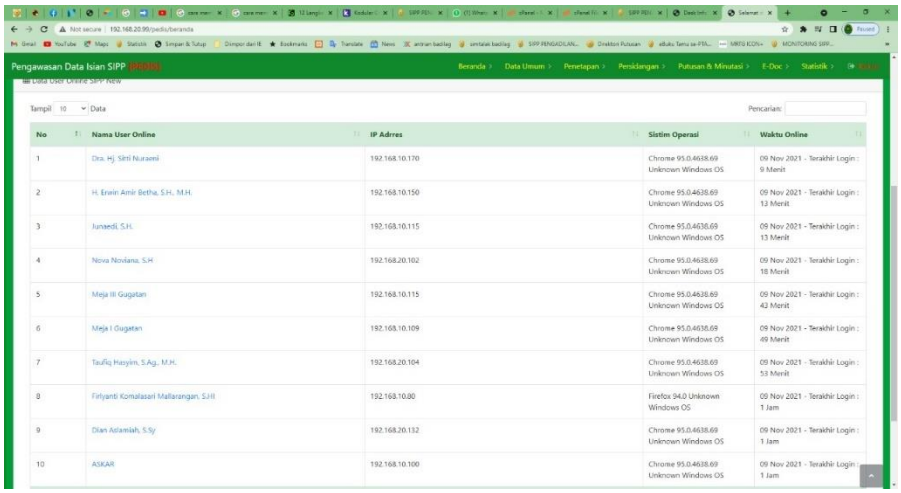
Sant, P. (2014). *Digital Forensics : the need for Integration Digital Forensics : the need for Integration Keywords*. *June*.

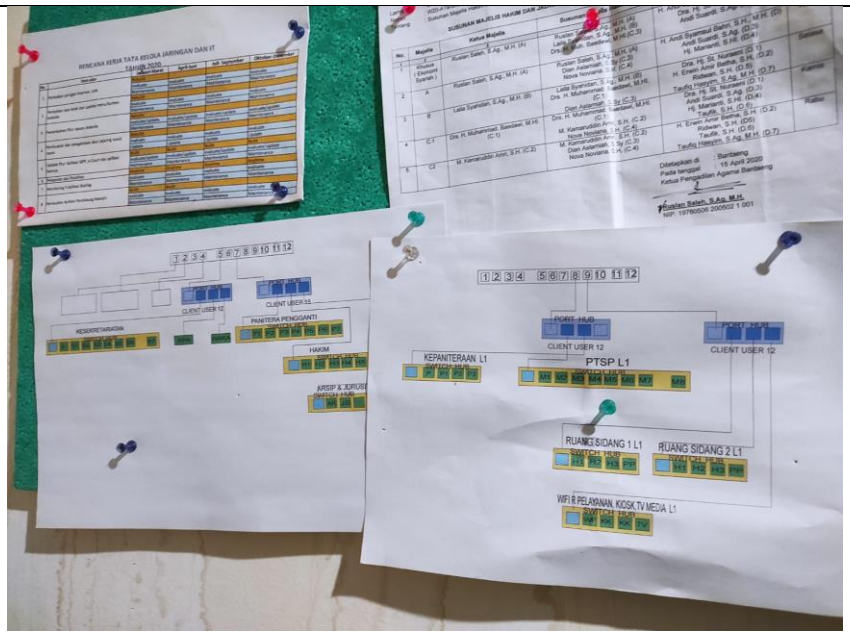
Simou, S., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2016). A survey on cloud forensics challenges and solutions. *Security and Communication Networks*, *9*(18), 6285–6314. https://doi.org/10.1002/sec.1688

Trenwith, P. M., & Venter, H. S. (2013). Digital forensic readiness in the cloud. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, March 2016*. https://doi.org/10.1109/ISSA.2013.6641055

Lampiran

Tabel 7.1. Tabel Hasil wawancara evaluasi penerapan *Integrated Cloud Forensic Readiness* pada organisasi Pengadilan Agama Bantaeng

ID	Pertanyaan	Respons
R1	Organisasi memiliki registri aset untuk item peralatan elektronik yang dapat merekam informasi. Penjelasan: Pengadilan Agama Bantaeng tidak memiliki peralatan elektronik khusus yang dapat merekam informasi khususnya yang berkaitan dengan forensic	Tidak
	Organisasi menyimpan catatan (log)perilaku pengguna dengan aplikasi berbasis jaringan dan membuat dokumen pengamatan. Penjelasan: Pengadilan Agama Bantaeng memiliki aplikasi tambahanyang terintegrasi dengan SIPP (aplikasi utama peradilan) yang dapat mencatat dan merekam penggunaan aplikasi SIPP 	Yes
	Organisasi menyimpan catatan (log) konfigurasi jaringan dan sistem yang kemudian didokumentasikan. Penjelasan: Pengadilan Agama Bantaeng mencatat konfigurasi jaringan yang kemudian didokumentasikan dalam catatan tim IT pengadilan Agama Bantaeng	Yes

		
R2	Organisasi mengetahui informasi apa dan dalam format apa yang diperlukan sebagai bukti dalam proses pidana serta cara menggunakannya untuk menemukan penyebab suatu peristiwa. Penjelasan: Pengadilan Agama Bantaeng tidak memiliki informasi mendalam mengenai penyelidikan forensic dan tata cara pengumpulan barang bukti, seperti kebanyakan organisasi lain yang mengalami kendala dalam respons insiden.	Tidak
	Organisasi dapat mengidentifikasi, mengklasifikasikan, dan memprioritaskan sumber dan jenis bukti potensial dengan mempertimbangkan legalitas dan efektivitas biaya dari proses pengumpulan, sumber bukti alternatif, dan potensi eskalasi ke dalam penyelidikan formal yang melibatkan lembaga penegak hukum. Penjelasan: Walaupun pengadilan agama bantaeng memiliki sumber daya yang memungkinkan untuk setidaknya mengidentifikasi bukti digital potensial dan membuat kerangka kerja dalam penyelidikan internal, namun belum ada sop (prosedur operasi) dalam insiden respons.	Yes
P1	Organisasi memiliki kebijakan yang mengklarifikasi kepemilikan data dan penggunaan sumber daya sistem informasi oleh anggota organisasi Penjelasan: Kebijakan penggunaan sumber daya informasi diatur oleh peraturan terpusat dalam hal ini mahkamah agung	Yes

	 KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA KEPUTUSAN KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA Nomor : 269 /KMA/SK/XII/2018 TENTANG TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUNGAN MAHKAMAH AGUNG DAN BADAN PERADILAN YANG BERADA DI BAWAHNYA KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA, Menimbang : a. bahwa proses peradilan yang transparan merupakan salah satu syarat terwujudnya akuntabilitas badan peradilan dalam rangka meningkatkan kepercayaan masyarakat; b. bahwa untuk mewujudkan transparansi dan	
	Organisasi ini memiliki kebijakan yang mendefinisikan skenario bisnis yang memerlukan bukti digital, informasi apa yang harus dipertahankan dalam keadaan tertentu, tenggang waktu, aksesibilitasnya, dan kondisi yang diperlukan sesuai dengan undang-undang. Penjelasan: Dikutip dari peraturan Pengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 35. IT *Governance* Adalah merupakan Tata Kelola TIK yang meliputi Manajemen Layanan, Keamanan, dan Audit terhadap sumber daya TIK. Umumnya *best practices* yang digunakan untuk Manajemen Layanan adalah ITIL, Keamanan (ISO/IEC 27001 dan ISO/IEC 27002) dan Audit (COBIT). 36. IT *Infrastructure Library* Merupakan suatu panduan standar untuk pengelolaan TIK, dikeluarkan oleh *Office of Government Commerce* (OGC), UK. IT *Infrastructure Library* menyediakan kerangka *best practices* untuk Manajemen Layanan TIK (pengelolaan infrastruktur, pengembangan, serta operasi TIK).	Yes
	Organisasi memiliki kebijakan yang melarang penggunaan akses intranetnya saat menangani bukti digital Penjelasan: ketika terjadi insiden, admin dari tim IT akan mematikan langsung jaringan dan meminta pengertian pegawai.	Yes

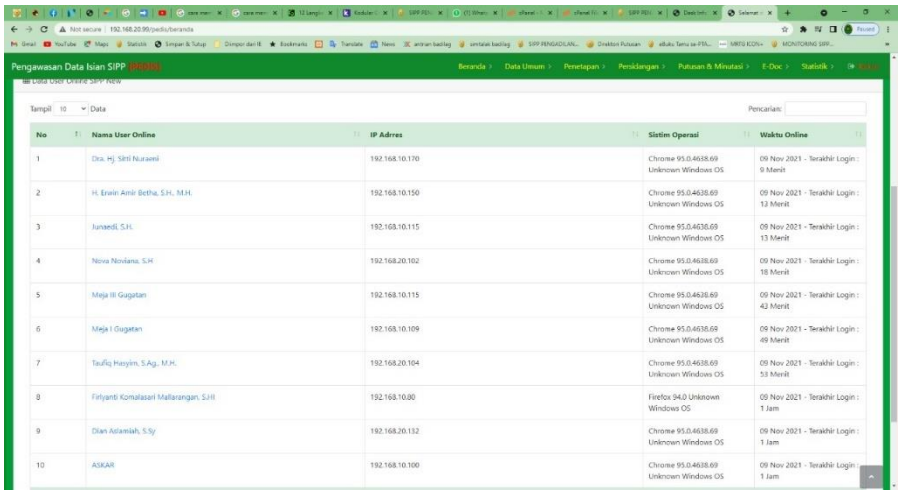
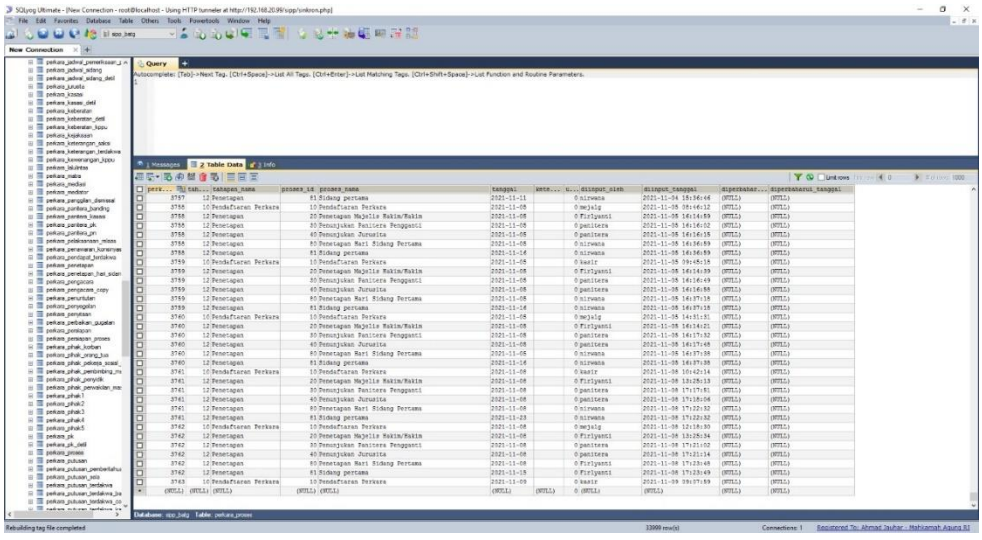
	Organisasi ini memiliki kebijakan keamanan perusahaan yang mengatur aset digital, peristiwa forensik, pengumpulan/penyimpanan data, keamanan pencegahan insiden , dan kode etik. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.  KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA KEPUTUSAN KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA Nomor : 269 /KMA/SK/XII/2018 TENTANG TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUNGAN MAHKAMAH AGUNG DAN BADAN PERADILAN YANG BERADA DI BAWAHNYA KETUA MAHKAMAH AGUNG REPUBLIK INDONESIA, Menimbang : a. bahwa proses peradilan yang transparan merupakan salah satu syarat terwujudnya akuntabilitas badan peradilan dalam rangka meningkatkan kepercayaan masyarakat; b. bahwa untuk mewujudkan transparansi dan	Yes
P2	Organisasi ini memiliki tahapan prosedur yang dapat diandalkan untuk mengumpulkan bukti pasca-insiden yang dapat diterima yang meliputi: cara menemukan data tersembunyi, kriteria tertimbang yang memandu pengumpulan bukti berdasarkan volatilitas penyimpanan, teknik pengambilan sampel & pengurangan, memverifikasi integritas data, dan cara menyimpan dan memanipulasi data Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.	Yes

	F. Prinsip Teknologi. 1. Mahkamah Agung menetapkan standar TIK dengan mengadopsi teknologi yang telah mapan dan legal, meminimalkan biaya integrasi, pelatihan, pemeliharaan dan perubahan. 2. TIK Mahkamah Agung membuat rencana pemulihan bencana (*Disaster Recovery Plan*) yang teruji dalam mengatasi dampak bencana untuk menjamin keberlangsungan kegiatan. 3. Rencana pemulihan bencana yang telah ditetapkan oleh TIK Mahkamah Agung menjadi pedoman bagi TIK Badan Peradilan yang berada di bawahnya.	
	Organisasi ini memiliki prosedur formal yang tidak bias untuk pemeriksaan bukti digital dan fisik pasca-insiden tanpa memodifikasinya. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. d. Terkini Data harus direkam sesegera mungkin setelah suatu kejadian atau kegiatan dan harus tersedia untuk penggunaan dalam jangka waktu tertentu. Data harus tersedia secara cepat dan tepat untuk mendukung pemenuhan kebutuhan informasi, pelayanan atau pengambilan keputusan. e. Aman Data harus terlindungi dari tindakan perusakan, bencana atau penggunaan oleh pihak yang tidak memiliki kewenangan. Semua perubahan dan pembatalan perubahan data harus melalui proses yang dapat diaudit.	Yes
	Organisasi menerapkan autentikasi dan peran pengguna yang kuat dalam pembagian kontrol akses berbasis dengan prinsip hak istimewa dengan log terkait alur data per pengguna. Penjelasan: Dikutip dari peraturan Pengadilan agama bantaeng yang	

	menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 2. Petugas Keamanan Informasi bertanggung jawab dalam menjamin pelaksanaan perlindungan kerahasiaan sesuai dengan tingkatannya dan berhak melakukan pemeriksaan dalam bentuk apapun untuk menguji ketertiban pelaksanaannya oleh pemilik dan pengguna data.	
P3	Teknologi organisasi -- seperti perangkat keras, perangkat lunak, dan alat forensik -- telah disertifikasi atau divalidasi. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 3) mendata dan menganalisa keberadaan dan kelengkapan *Standard Operating Procedure* (SOP) yang sudah dimiliki oleh TIK Mahkamah Agung dan Badan Peradilan yang berada di bawahnya dipetakan ke dalam *Control Objective for Information and Related Technology* (COBIT) maupun *Information Technology Infrastructure Library* (ITIL), untuk dapat disempurnakan, dilengkapi dan dimanfaatkan secara bersama-sama; dan 4) target kinerja layanan yang akan dicapai dinyatakan secara jelas, dimonitor secara berkala realisasinya, dan memiliki peta jalan dalam rangka pencapaian target.	Yes
P4	Organisasi memiliki kebijakan yang menetapkan perlunya kepatuhan terhadap kerangka aturan organisasi, undang-undang dan/atau peraturan pemerintah, bahkan tanpa adanya insiden forensik. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.	Yes

	III. Tata Kelola Teknologi Informasi dan Komunikasi di lingkungan Mahkamah Agung dan Badan Peradilan yang berada di bawahnya. A. Umum. 1. Penyesuaian (*alignment*) proses kerja Mahkamah Agung dengan TIK: a. setiap unit eselon I harus memiliki Rencana Strategis (Renstra) yang diperlukan untuk dijadikan acuan penyesuaian proses kerjanya dengan TIK; b. setiap unit eselon I mengimplementasikan sasaran strategis dan program kerjanya ke dalam kebutuhan TIK; c. kontribusi TIK menjadi pendorong dalam pencapaian organisasi yang efisien sehingga dipercaya oleh publik; dan d. setiap unit eselon I menguraikan, mendefinisikan uraian tugas, memahami proses kerjanya secara lengkap dan menentukan skala prioritas berdasarkan dampak dan upaya implementasi sebagai acuan awal aplikasi TIK yang dibutuhkan.	
	Organisasi mendefinisikan otoritas hukum dan menejemen yang diperlukan untuk pencarian dan pemeriksaan selama penyelidikan untuk memastikan kepatuhan terhadap keamanan dan peraturan informasi. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 3. Pertukaran Data Internal a. pemilik data tidak membatasi efektifitas aliran informasi, baik di dalam unit eselon I, antar unit eselon I maupun badan peradilan yang berada di bawahnya, kecuali ditentukan lain dalam peraturan perundang-undangan; b. pengguna data bertanggung jawab untuk menjaga kerahasiaan data sesuai dengan tingkat sensitivitasnya; c. pengguna data hanya dapat menggunakan data sebagai referensi dan tidak diperkenankan menyampaikan, mempergunakan, menggandakan dan/atau menyebarluaskan informasi atas suatu	Yes
T1	Organisasi memiliki kemampuan untuk melakukan investigasi forensic secara mandiri.	Yes

	Penjelasan: Organisasi Pengadilan Agama Bantaeng memiliki kemampuan untuk melakukan investigasi forensic secara mandiri namun masih terbatas pada perangkat pembantu penyidikan. Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018 dan screenshot aplikasi pemantuan data F. Prinsip Teknologi. 1. Mahkamah Agung menetapkan standar TIK dengan mengadopsi teknologi yang telah mapan dan legal, meminimalkan biaya integrasi, pelatihan, pemeliharaan dan perubahan. 2. TIK Mahkamah Agung membuat rencana pemulihan bencana (*Disaster Recovery Plan*) yang teruji dalam mengatasi dampak bencana untuk menjamin keberlangsungan kegiatan. 3. Rencana pemulihan bencana yang telah ditetapkan oleh TIK Mahkamah Agung menjadi pedoman bagi TIK Badan Peradilan yang berada di bawahnya.	
T2	Organisasi memiliki prosedur formal untuk meantau pencatatan (log) lalu lintas data dan penyimpatan terpusat sehingga mudah untuk dilakukan audit serta memiliki kemampuan dalam menjaga kemasan, transportasi, penyimpanan, penanganan, dan pelestarian bukti fisik dan digital Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018 dan aplikasi untuk memantau pencatatan (log) dan lalu lintas data.	Yes

	3) mendata dan menganalisa keberadaan dan kelengkapan *Standard Operating Procedure* (SOP) yang sudah dimiliki oleh TIK Mahkamah Agung dan Badan Peradilan yang berada di bawahnya dipetakan ke dalam *Control Objective for Information and Related Technology* (COBIT) maupun *Information Technology Infrastructure Library* (ITIL), untuk dapat disempurnakan, dilengkapi dan dimanfaatkan secara bersama-sama; dan 4) target kinerja layanan yang akan dicapai dinyatakan secara jelas, dimonitor secara berkala realisasinya, dan memiliki peta jalan dalam rangka pencapaian target.  	
T3	Organisasi menyediakan panduan keamanan untuk perilaku aman dalam lingkungan ruang kerja.	Yes

	Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. c. dokumen *Disaster Recovery Plan* (DRP) yang lengkap harus berisi setidaknya *Risk Analysis* (RA), *Business Impact Analysis* (BIA), *Recovery Strategy* (RS), *Disaster Recovery Center* (DRC) *Design* (*site and system*), *Disaster Recovery* -24- *Organization*, *Standard Operating Procedure* (SOP) dan *Testing Strategy* (TS); dan d. pembangunan *Disaster Recovery Center* (DRC) hanya dilakukan setelah dokumen *Disaster Recovery Plan* (DRP) tersedia.	
	Organisasi dapat mengontrol dan mendokumentasikan dengan aman dan efektif di tempat kejadian insiden (tkp) forensik digital. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.	Yes

	e. Aman Data harus terlindungi dari tindakan perusakan, bencana atau penggunaan oleh pihak yang tidak memiliki kewenangan. Semua perubahan dan pembatalan perubahan data harus melalui proses yang dapat diaudit. Petugas Keamanan Informasi bertanggung jawab dalam menjamin pelaksanaan perlindungan kerahasiaan sesuai dengan tingkatannya dan berhak melakukan pemeriksaan dalam bentuk apapun untuk menguji ketertiban pelaksanaannya oleh pemilik dan pengguna data.	
D1	Tim respons forensik /investigasi multi-disiplin organisasi dibentuk dengan sifat lebih internal daripada eksternal. Penjelasan: Pengadilan Agama Bantaeng tidak memiliki prosedur pembentukan tim penyidikan forensic digital Ketika terjadinya insiden karena terbatasnya sumber daya manusia.	No
	Organisasi memiliki model forensik digital yang luas dan lengkap yang mendefinisikan fase standar (menangkap, menyimpan, menganalisis, melestarikan, mengintegrasikan, dan menyajikan bukti) dari proses respons dan penyelidikan. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.	Yes

	2. *Business Continuity Management* (BCM) dan *Disaster Recovery Plan* (DRP). a. pengembangan standar rencana pemulihan bencana *Disaster Recovery Plan* (DRP) untuk tingkat nasional merupakan tanggung jawab unit TIK Mahkamah Agung; b. pengembangan Rencana Kerja Berkelanjutan *Business Continuity Plan* (BCP) merupakan tanggung jawab unit TIK Mahkamah Agung; c. dokumen *Disaster Recovery Plan* (DRP) yang lengkap harus berisi setidaknya *Risk Analysis* (RA), *Business Impact Analysis* (BIA), *Recovery Strategy* (RS), *Disaster Recovery Center* (DRC) *Design* (*site and system*), *Disaster Recovery*	
	Organisasi memiliki prosedur respons insiden formal yang menjelaskan peristiwa pemicu untuk memulai pemantauan aktif dan pengumpulan sistematis bukti digital potensial (termasuk pengumpulan data pra-insiden), pedoman respons pertama untuk mempertahankan bukti, kapan dan bagaimana melaporkan insiden, cara memilih model investigasi, dan cara menetapkan rencana tindakan. Penjelasan: Pengadilan Agama Bantaeng tidak memiliki prosedur respon tertentu dalam pengumpulan barang bukti namun memiliki prosedur penanganan insiden.	No
D2	Organisasi ini menggunakan teknologi pencitraan dengan fungsi kompresi dan hashing lossless untuk melestarikan bukti forensik. Penjelasan: Pengadilan Agama Bantaeng tidak memiliki teknologi pencitraan dengan fungsi kompresi dan hashing lossless untuk melestarikan bukti forensik karena pembangunan infrastruktur masih dalam tahap pengembangan menuju kesempurnaan dalam hal pelayanan masyarakat.	No
D3	Organisasi ini menggunakan standar enkripsi dan hash kriptografi untuk file bukti/evidence. Penjelasan: Pengadilan Agama Bantaeng tidak menggunakan standar enkripsi dan hash kriptografi untuk file bukti/evidence, dikarenakan masih terbatasnya pengetahuan mengenai pentingnya otentifikasi file bukti/evidence.	No

D4	Jika terjadi insiden cyber, organisasi akan dapat menentukan waktu, garis waktu peristiwa, dan durasi insiden. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. b. Akurat Data harus akurat dan dapat digunakan sesuai peruntukannya. Data seharusnya hanya direkam 1 (satu) kali meskipun dapat digunakan berulangkali untuk pelbagai kepentingan. Data wajib direkam pada titik kejadian atau kegiatan.	Yes
	Jika terjadi insiden cyber, organisasi dapat mengantisipasi kebutuhan penemuan dan mempercepat penyelidikan untuk menemukan bukti tepat waktu dan dapat digunakan Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 2. Petugas Keamanan Informasi bertanggung jawab dalam menjamin pelaksanaan perlindungan kerahasiaan sesuai dengan tingkatannya dan berhak melakukan pemeriksaan dalam bentuk apapun untuk menguji ketertiban pelaksanaannya oleh pemilik dan pengguna data.	Yes
E1	Organisasi memiliki prosedur yang menjelaskan konfigurasi dan penggunaan mekanisme pemantauan dan pencatatan aktif untuk terus mendeteksi dan mencegah insiden dalam kegiatan sistem dan komunikasi elektronik, termasuk prosedur untuk mencegah perubahan komunikasi yang disadap. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018.	Yes

	d. Terkini Data harus direkam sesegera mungkin setelah suatu kejadian atau kegiatan dan harus tersedia untuk penggunaan dalam jangka waktu tertentu. Data harus tersedia secara cepat dan tepat untuk mendukung pemenuhan kebutuhan informasi, pelayanan atau pengambilan keputusan.	
E2	Organisasi membuat laporan tentang pelajaran yang dipelajari dari insiden, termasuk keberhasilan dalam menangani dan memulihkan diri dari insiden. Penjelasan: Dikutip dari peraturanPengadilan agama bantaeng yang menentukan infrastruktur teknologi IT mengacu pada skkma no 268 tahun 2018. 5. Pelaporan dan Analisis Data. a. pelaporan dibuat secara tertulis memuat waktu yang dibutuhkan, keterkaitan antarsumber data dan penanggung jawab sesuai dengan format yang ditentukan; b. pusat data yang dibangun di tingkat Mahkamah Agung harus memperhatikan kehandalan data untuk mendukung kemampuan data analisis secara lengkap; dan -18- c. pelaporan atas data merupakan hak dan kewajiban pemilik data.	Yes