



الجامعة الإسلامية
INDONESIA

Pengembangan Konseptual Framework untuk Investigasi Cyber Fraud

Anisa Nur Hidayati

18917106

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 Konseptual Framework untuk Investigasi Cyber Fraud

Anisa Nur Hidayati

18917106



Yogyakarta, 27 April 2021

Pembimbing I

Dr. Imam Riadi S.Pd., M.Kom.

Pembimbing II

Erika Ramadhani, ST., M.Eng.

Lembar Pengesahan Penguji

Pengembangan Konseptual Framework untuk Investigasi Cyber Fraud

Anisa Nur Hidayati

18917106

Yogyakarta, 1 Juni 2021

Tim Penguji,

Dr. Imam Riadi, S.Pd., M.Kom

Ketua

Dr. Ir. Bambang Sugiantoro, S.Si., MT.

Anggota I

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

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia



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

Abstrak

Pengembangan Konseptual Framework untuk Investigasi Cyber Fraud

Naiknya jumlah penggunaan internet di Indonesia sebanyak 175,4 juta sebagaimana tercatat di laporan datareportal.com serta 4,83 miliar secara global berdampak dengan naiknya jumlah *cyber fraud* yang dilakukan oleh oknum yang memahami cara mengambil data privasi seperti data finansial dari seseorang. Jumlah penetrasi internet di Indonesia pun telah menjadi 64% pada bulan Januari 2020. Data hasil curian yang disalahgunakan untuk keuntungan pribadi maupun untuk membuat orang lain rugi merupakan jenis fraud yang sedang berkembang atau sering disebut *cyber fraud*. Kasus-kasus *cyber fraud* ini memerlukan suatu framework baru untuk investigasi dikarenakan dalam kasus fraud ini terdapat barang bukti digital yang sangat rawan untuk rusak, hilang maupun termodifikasi sehingga tidak layak untuk diajukan ke meja pengadilan. Penelitian *Fraud Investigation* sekarang ini lebih banyak tertuju kepada *Fraud Detection* baik menggunakan *data mining* maupun *artificial intelligence*, sehingga pada penelitian ini berfokus pada pengajuan framework untuk investigasi kasus *cyber fraud*.

Dalam pembuatan framework ini akan menggunakan metode Jabareen yang terdiri dari 6 tahapan yakni, *Mapping the selected data source, extensive reading and categorizing of the selected data, Identifying and naming object, Deconstructing and categorizing the concept, Integrating concept, Synthesis, resynthesis and make it all sense, Validating the conceptual framework*, dan *Rethinking the conceptual framework*. Metode ini menggabungkan konsep dari beberapa bidang ilmu yang berkaitan pada penelitian ini yakni bidang Digital Forensic dan Audit Fraud.

Framework yang diajukan terdiri dari 7 tahapan dengan 1 Concurrent proses yang merupakan integrasi dari berbagai konsep yang dipilih dari Digital Forensik dan Audit Fraud. Framework ini diharapkan dapat menjadi referensi untuk melakukan investigasi cyber fraud menjadi lebih efisien.

Kata kunci

cyber fraud, digital evidence, fraud audit, fraud forensics

Abstract

Development of Conceptual Framework for Cyber Fraud Investigation

The increase in the number of internet users in Indonesia as many as 175.4 million as recorded in the Datareportal.com report and 4.83 billion globally resulted in an increase in the number of cyber frauds committed by individuals who understand how to retrieve privacy data such as financial data from someone. The number of internet penetration in Indonesia also increased to 64% in January 2020. Stolen data that is misused for personal gain or to make other people lose is a type of fraud that is on the rise or often called cyber fraud. These cyber fraud cases require a new framework for investigation because in this fraud case there is digital evidence that is very prone to being damaged, lost or modified so it is not feasible to be submitted to court. Current Fraud Investigation research focuses more on Fraud Detection using both data mining and artificial intelligence, so this research focuses on proposed a framework for investigating cyber fraud cases.

In making this framework, we will use the Jabareen method which consists of 8 stages, namely, Mapping the selected data source, extensive reading and categorizing of the selected data, Identifying and naming objects, Deconstructing and categorizing the concept, Integrating concept, Synthesis, resynthesis and make it all sense, Validating the conceptual framework, and Rethinking the conceptual framework. This method combines concepts from several fields of science related to this research, namely the field of Digital Forensics and Fraud Audit.

The proposed framework consists of 6 stages with 1 Concurrent process which is an integration of various concepts selected from Digital Forensics and Fraud Audit. This framework is expected to be a reference for making cyber fraud investigations more efficient.

Keywords

cyber fraud, cyber crime, fraud audit, fraud forensics

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Mei 2021



Anisa Nur Hidayati

Daftar Publikasi

Paper yang dihasilkan:

(Anisa Nur Hidayati, Imam Riadi, Erika Ramadhani, Sarah Ulfah Al Amany, 2021),
Development of conceptual framework for cyber fraud investigation, Register, Vol. 7, Issue.
2, Edisi July 2021).

Kontributor	Jenis Kontribusi
Anisa Nur Hidayati	Mendesain eksperimen (70%) Menulis <i>paper</i> (80%)
Imam Riadi	Mendesain eksperimen (30%) Menulis dan mengedit <i>paper</i> (20%)
Erika Ramadhani	Melakukan review paper
Sarah Ulfah Al Amany	Melakukan validasi metodologi dan hasil

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain



Halaman Persembahan

Alhamdulillah Robbil 'Alamin. Segala puji dan syukur atas kehadiran Allah Subhana Wa Ta'ala yang telah memberikan rahmat, ridho, dan karunia-Nya kepada saya. Shalawat serta salam kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam, sebagai pembawa risalah Allah terakhir dan penyempurna seluruh risalah-Nya. Tesis ini saya persembahkan kepada:

1. Allah Subhana Wa Ta'ala yang telah memberiku nikmat iman dan islam, serta suri teladan kami Nabi Muhammad Shalallahu 'Alaihi Wa Salam.
2. Orang tua dan keluarga tersayang yang selalu mengiringi doa, motivasi, serta nasehat dalam hidup kami.
3. Dosen dan Seluruh pengurus Akademik MI UII yang berjasa serta bersedia memberikan waktu dan ilmu pengetahuan selama menempuh masa studi.
4. MI UII 2018 khususnya Konsentrasi Forensika Digital yang selalu memberikan semangat, dan motivasi dalam menempuh masa studi.
5. Pihak lain yang tidak dapat penulis sebutkan satu-persatu yang ikut mendukung penulis dalam penyusunan Laporan Tesis ini, maupun dalam menempuh masa studi magister.

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur penulis sampaikan kehadirat Allah SWT., Tuhan Yang Maha Pemurah lagi Maha Penyayang. Berkat rahmat, hidayah, dan inayah-Nya, akhirnya penulis dapat menyelesaikan laporan tesis yang berjudul “Pengajuan Konseptual Framework untuk Investigasi Cyber Fraud”.

Tesis ini merupakan syarat wajib yang harus ditempuh dalam mencapai Magister Strata-2 pada Program Studi Magister Informatika. Penulisan laporan tesis ini terselesaikan karena bantuan dari berbagai pihak. Untuk itu, penulis menyampaikan terima kasih kepada semua pihak yang telah membantu penulis dalam menyelesaikan laporan tesis ini.

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Selaku Rektor Universitas Islam Indonesia.
2. Bapak Hari Purnomo, Prof., Dr., Ir., M.T., Selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D., Selaku Ketua Program Studi Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Dr. Imam Riadi S.Pd., M.Kom, Selaku Dosen Pembimbing 1 yang berkenan membimbing dan mengarahkan penulis, sehingga Penelitian Tesis ini dapat selesai.
5. Ibu Erika Ramadhani ST., M.Eng, Selaku Dosen Pembimbing 2 yang berkenan membimbing dan mengarahkan penulis, sehingga Penelitian Tesis ini dapat selesai.
6. Semua pihak yang tidak dapat penulis sebutkan satu persatu, baik secara langsung maupun tidak langsung membantu dalam penulisan tesis ini.

Semoga atas bantuan dan kerjasama yang telah diberikan menjadi amal baik dan mendapat balasan dari Allah SWT. Penulis menyadari bahwa penelitian ini jauh dari sempurna, untuk itu diperlukan saran dan masukan demi sempurnanya penyusunan laporan tesis ini. Akhir kata, penulis berharap semoga laporan tesis ini dapat bermanfaat bagi semua yang membutuhkan.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 08 Mei 2021

Anisa Nur Hidayati

Daftar Isi

Lembar Pengesahan Pembimbing	ii
Lembar Pengesahan Penguji.....	ii
Abstrak	ii
Abstract.....	v
Pernyataan Keaslian Tulisan	vi
Daftar Publikasi	vii
Halaman Kontribusi.....	viii
Halaman Persembahan	ix
Kata Pengantar.....	x
Daftar Isi.....	xi
Daftar Tabel.....	xiii
Daftar Gambar	xiv
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
1.6 Tinjauan Pustaka.....	6
1.7 Metodologi Penelitian.....	10
1.8 Sistematika Laporan	10
BAB 2 Tinjauan Pustaka	12
2.1 Fraud	12
2.2 <i>Cyber Fraud</i>	13
2.3 Accounting Forensik/ Fraud Audit	14
2.4 <i>Digital Evidence</i>	16

2.5	Penanganan Bukti Digital	17
2.6	<i>Digital Forensic Investigation Process (DFIP)</i>	19
2.7	<i>Delphi Method</i>	21
BAB 3 Metodologi		24
3.1	Pengembangan Framework.....	24
3.2	Modifikasi Framework	25
3.3	Mapping the selected data sources.....	26
3.4	Extensive reading and categorizing of the selected data.....	26
3.5	Identifying and naming concept.....	27
3.6	Deconstructing and categorizing the concepts.....	27
3.7	Integrating concepts	28
3.8	Synthesis, Resynthesis and making it all make sense.....	28
3.9	Evaluasi Framework	29
3.10	Simulasi Kasus.....	30
BAB 4 Hasil dan Pembahasan.....		32
4.1	Mapping Selected Data	32
4.2	Extensive reading and categorizing of the selected data	32
4.3	Identifying and naming concept.....	33
4.4	Deconstructing and categorizing the concepts.....	37
4.5	Integrating concepts	42
4.6	Synthesis, Resynthesis and making it all make sense.....	43
4.7	Evaluasi Framework	47
4.8	Simulasi Framework	50
BAB 5 Kesimpulan dan Saran.....		59
5.1	Kesimpulan	59
5.2	Saran	59
Daftar Pustaka.....		61

Daftar Tabel

Tabel 1.1 Ulasan Kritis dari berbagai penelitian	7
Tabel 2.1 Kriteria ISO EIC (Valjarevic et al., 2017).....	20
Tabel 3.1 Tabel kategori data	27
Tabel 3.2 Tabel klasifikasi konsep data.....	27
Tabel 3.3. Instrumen kuisisioner	29
Tabel 3.4 Modifikasi Instrumen kuisisioner.....	30
Tabel 4.1 Kata kunci pencarian data.....	32
Tabel 4.2 Kategorisasi data	33
Tabel 4.3 Konsep Audit Forensik.....	36
Tabel 4.4 Ringkasan konsep data Digital Forensik	37
Tabel 4.5 Tabel Konsep Audit Forensik.....	40
Tabel 4.6 Ringkasan sifat konsep	41
Tabel 4.7 Integrasi konsep.....	42
Tabel 4.8 Ringkasan Hasil Kuesioner	48

Daftar Gambar

Gambar 1.1 Laporan Kerugian Fraud FTC Amerika 2019	2
Gambar 1.2 Laporan Kerugian Fraud FTC Amerika 2020	2
Gambar 1.3 Infografik kasus fraud di Inggris (which.co.uk)	3
Gambar 1.4 Tantangan fraud dilingkungan <i>cyberspace</i> (Fletcher, 2007)	4
Gambar 1.5 Model Metodologi Penelitian	10
Gambar 2.1 Cyber Fraud Model (Bryan 2007:Verisign iDefence,2007)	13
Gambar 3.1 Metode Pengembangan Framework	24
Gambar 3.2 Modifikasi Metode Pengembangan Framework.....	25
Gambar 3.3 Simulasi Kasus Cyber Fraud.....	31
Gambar 4.1 Framework Digital Forensik yang digunakan	33
Gambar 4.2 Konsep digital forensic Lee – ISO 27043.....	34
Gambar 4.3 Konsep digital forensic DFRWS-Dimitriadis.....	34
Gambar 4.4 Konsep digital forensic Ahmad-Gayatri.....	35
Gambar 4.5 Konsep digital forensic Suratno-Bebe	35
Gambar 4.6 Framework cyber fraud yang diajukan	43
Gambar 4.7 Tahapan Readiness yang dilakukan instansi UMJ.....	50
Gambar 4.8 Barang Bukti PC Asus All in One	51
Gambar 4.9 Rincian meta data file menggunakan exiftool	51
Gambar 4.10 Incremental update dari InvoiceUMJ.pdf.....	532
Gambar 4.11 Select incremental update dari InvoiceUMJ.pdf	542
Gambar 4.12 Perintah dump dari file InvoiceUMJ.pdf.....	543
Gambar 4.13 Hasil dump file InvoiceUMJ.pdf.....	553
Gambar 4.14 Menyimpan hasil dump menjadi recoveredInvoiceUMJ.pdf	554
Gambar 4.15 Hasil dump di explorer	565
Gambar 4.16 File recoveredInvoiceUMJ.pdf.....	565
Gambar 4.17 File InvoiceUMJ.pdf yang berisi manipulasi data	576

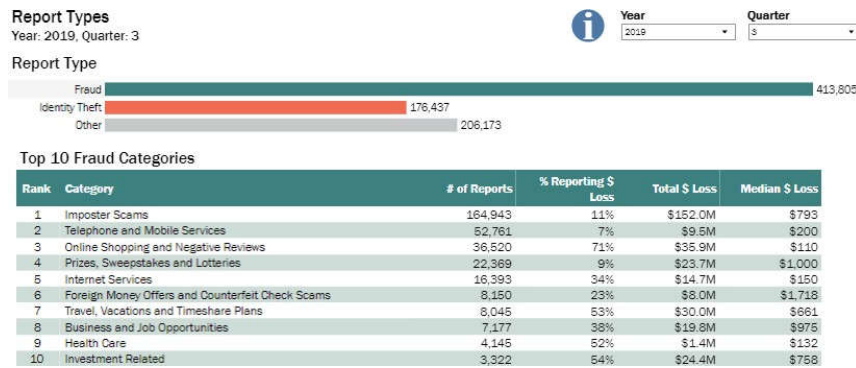
BAB 1

Pendahuluan

1.1 Latar Belakang

Dalam laporan perusahaan multinasional KPMG yang bergerak dibidang finansial audit pada tahun 2019 terdapat 4 jenis fraud yang mengalami peningkatan jumlah dari tahun ke tahun yakni *Card Not Present*, *Social Engineering*, *Scams*, dan *Cyber/Online Fraud* di 3 bagian dunia yakni Asia Pasific, Amerika, Eropa dan Timur Tengah(KPMG Australia, 2019). Pada panduan yang dikeluarkan oleh Microsoft menjelaskan mengenai berbagai macam jenis online fraud yang dilakukan oleh penjahat dengan menggunakan internet seperti *phising scam*, *rogue security software*, *fake technical support*, *fraudulent contest and winning*, serta *financial scam*(Microsoft, 2020). IC3 menerbitkan sebuah laporan yang menyebutkan bahwa media atau alat yang digunakan untuk tindak kejahatan ini menggunakan sosial media atau mata uang digital (Federal Bureau of Investigation, 2019). Menurut Accenture walaupun berbagai institusi finansial dan bisnis berusaha mengadopsi strategi terbaru untuk membuat pembayaran secara digital lebih aman dari fraud , para penjahat semakin inovatif dalam melakukan pencurian data pribadi yang sensitif dengan bantuan platform digital(Accenture, 2018)

Data yang dipublikasikan oleh salah satu perusahaan *Business Analytical Software* FICO mengenai perkembangan fraud di Eropa pada tahun 2018 memaparkan bahwa jenis kejahatan *Card Not Present* atau CNP mengalami kenaikan yang signifikan di beberapa daerah. Pada Gambar 1.1 menggambarkan laporan dari *Federal Trade Commission* atau FTC di Amerika yang menyebutkan bahwa pada tahun 2019 kasus kejahatan yang paling banyak dilaporkan adalah kejahatan fraud yang dilaporkan paling tinggi diikuti tindakan *Identity Theft* dan kejahatan lainnya. Jenis *fraud* yang paling banyak dilaporkan *imposter scam* yang menimbulkan kerugian hingga 152 Juta Dollar Amerika. FTC juga menyebutkan bahwa masyarakat yang menjadi korban fraud tidak selalu melaporkan kasus yang mereka hadapi sehingga bagi aparat penegak hukum mengalami kesulitan dalam mengungkapkan kasus fraud ini.



Gambar 2.1 Laporan Kerugian Fraud FTC Amerika 2019
(<https://public.tableau.com/profile/federal.trade.commission#!>).

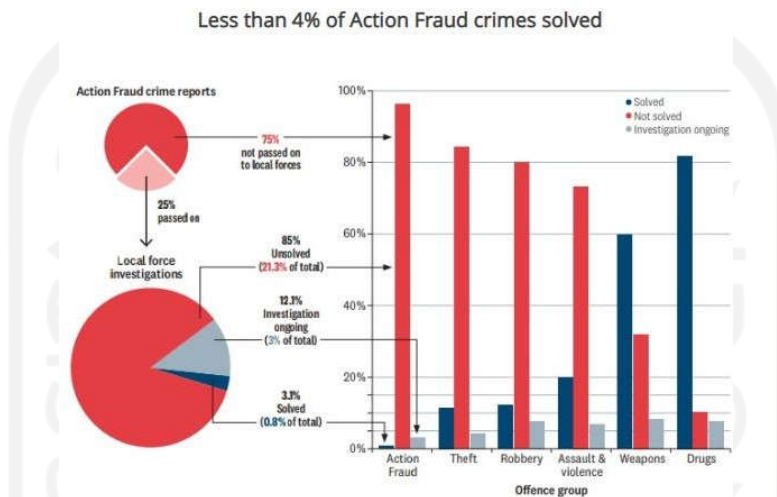
Tahun 2020 sejak adanya pandemic Covid-19 FTC seperti yang ditunjukkan pada Gambar 1.2 telah menerima banyak aduan mengenai fraud yang menimbulkan kerugian sebanyak 44,56 Juta Dollar Amerika pada semester awal tahun 2020. Hal ini didukung dengan adanya *Work From Home* yang diterapkan beberapa instansi untuk mengurangi penularan Covid-19, sehingga membuat tingkat kejahatan berbasis cyber menjadi semakin meningkat.



Gambar 2.2 Laporan Kerugian Fraud FTC Amerika 2020
(<https://www.ftc.gov/>).

Dalam berita yang publikasikan di Inggris disebutkan sebanyak lebih dari 96% kasus fraud tidak terselesaikan walaupun sudah dilaporkan dipihak yang berwajib. Penyebab utama dari kesulitan mengungkapkan kasus fraud dikarenakan kebanyakan pelaku *anonymous* atau kebanyakan kejahatan terjadi secara online. Bahkan badan *The Office for*

National Statistics (ONS) memperkirakan bahwa sekitar 55% kasus fraud memiliki element penggunaan digital. Data mengenai banyaknya kasus fraud yang tidak terselesaikan ini dapat dilihat pada infografik yang ditunjukkan pada Gambar 1.3. Kasus yang dilaporkan dan diproses oleh kepolisian kurang dari 4% yang berhasil diselesaikan, 86 % tidak terselesaikan dan 12% sedang dilakukan proses investigasi. Laporan yang lain juga disebutkan bahwa 63% kasus fraud terjadi secara online dimana tidak ada kontak fisik langsung antara pelaku dengan korban(Megan, 2019).

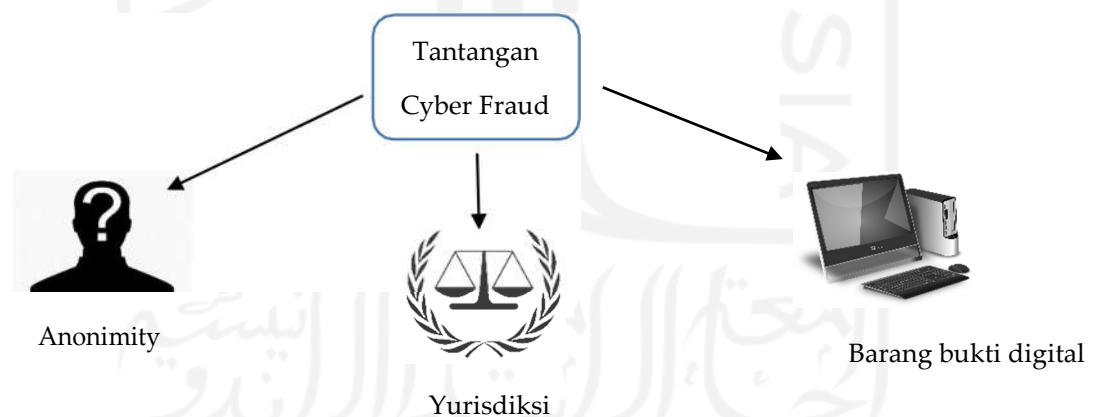


Gambar 2.3 Infografik kasus fraud di Inggris (which.co.uk)

Laporan survey yang dilaksanakan oleh ACFE pada tahun 2016, sebanyak 77% kasus kerugian akibat fraud di Indonesia didominasi oleh kasus korupsi. Di posisi kedua ditempati oleh Penyalahgunaan aktiva/kekayaan Negara dan perusahaan sebesar 19% sedangkan posisi terakhir berupa 4% ditempati oleh kecurangan laporan keuangan tetapi hal survey tersebut berbeda dengan survey yang dilakukan ACFE bahwa fraudulent financial report lah yang paling banyak merugikan Indonesia. Perbedaan hasil survey ini dikarenakan masih banyaknya kejahatan keuangan yang belum terungkap seperti penipuan informasi di bursa efek dan penipuan informasi pajak. Laporan ini menyebutkan bahwa dibutuhkan waktu selama 12 bulan untuk mendeteksinya adanya fraud dimana deteksi fraud paling banyak dikarenakan adanya laporan baik dari pihak internal, pihak tanpa nama atau anonim, pelanggan atau yang lainnya(Murdock & Murdock, 2018)

Terdapat beberapa hal yang mendukung terjadinya kasus fraud di lingkungan *cyberspace* dan merupakan tantangan bagi aparat hukum seperti yang digambarkan pada gambar 1.4, yang pertama adalah faktor *anonymity* dimana penjahat dapat melakukan tindak kejahatan secara rahasia bagi instansi yang dituju dimana ketika instansi tersebut sadar ketika menjadi korban fraud sudah terlalu terlambat bagi pihak yang berwenang untuk

mengidentifikasi siapa yang bertanggung jawab atas kasus ini. Walaupun *anonymity* merupakan bentuk *freedom of speech*, tetapi hal ini juga tidak menjadi jaminan bahwa pengguna tidak akan menyalahgunakan fitur ini (Nawang, 2017) yang membuat kendala bagi penegakan hukum. Yurisdiksi merupakan alasan selanjutnya kenapa kejahatan *cyberfraud* ini semakin banyak, hal ini dikarenakan kejahatan yang dilakukan dalam *cyberspace* akan menyulitkan aparat hukum dalam memilih yurisdiksi dimana proses hukum akan diproses. Karakter tersebut juga disebut dengan *borderless* dan salah satu hal yang membuat penegakan hukum mengenai kendala adalah kurangnya kerjasama yurisdiksi antar Negara semisal negara-negara di Asia Tenggara, Amerika Selatan dan di Afrika (Hayes et al., 2015). Alasan selanjutnya yakni sulitnya mencari barang bukti yang harus dicari penegak hukum (Fletcher, 2007). Barang bukti digital memiliki beberapa karakteristik yakni sangat mudah untuk terhapus, dan dimodifikasi, sensitif terhadap waktu, *cross* yurisdiksi dan tersembunyi (National Forensic Science Technology Center, 2014). Barang bukti digital nilai memiliki jangkauan yang lebih luar, lebih berisi data-data pribadi yang sensitif, dapat dibawa dengan mudah serta membutuhkan latihan dan alat-alat yang lebih canggih dibandingkan dengan barang bukti biasa (Goodison et al., n.d.) sehingga dari karakteristik tersebut dibutuhkan tenaga ahli karena apabila yang menangani kasus ini adalah tenaga yang kurang terlatih dapat menyebabkan barang bukti mengalami kerusakan (Ajayi, 2016).



Gambar 2.4 Tantangan fraud dilingkungan *cyberspace* (Fletcher, 2007)

Saat ini belum adanya framework yang secara spesifik mengakomodasi kasus *cyber fraud* dan untuk mengamankan data-data tersebut sehingga dapat digunakan sebagai barang bukti yang sah dimata hukum sehingga diperlukan suatu framework yang membahas mengenai investigasi *cyber fraud*. Upaya yang dapat digunakan untuk membantu menyelesaikan kasus *cyber fraud* ialah menggunakan framework investigasi yang

mendukung karakteristik barang bukti digital, dimana pada penyelesaian kasus masih menggunakan metode konvensional sedangkan penelitian mengenai fraud sebelumnya masih berfokus pada metode deteksi fraud dan belum membahas mengenai investigasi kasus *cyber fraud*. Penelitian ini bertujuan untuk mengembangkan framework *investigasi cyber fraud* dikarenakan tingginya kasus fraud yang tidak terselesaikan akibat penggunaan perangkat digital pada kejahatan ini serta dari tantangan investigasi *cyber fraud* seperti yang dijelaskan pada gambar 1.4. Pengembangan framework investigasi *cyber fraud* ini diharapkan dapat membantu penyidik maupun audit untuk menyelesaikan kasus fraud sehingga persentase kasus penyelesaian *cyber fraud* semakin tinggi. Metode pengembangan framework pada penelitian ini menggunakan metode pengembangan konseptual framework dari Jabareen yang mendukung pengembangan framework lintas disiplin ilmu yakni digital forensik dan audit fraud. Metode pengembangan ini terdiri dari 6 tahap proses dengan menggunakan 22 framework digital forensik dan 6 framework audit fraud sebagai acuan.

12 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana pengembangan *cyber fraud framework* untuk mendukung proses investigasi?
2. Bagaimana evaluasi dari pengembangan *cyber fraud framework* untuk mendukung proses investigasi?
3. Bagaimana implementasi penggunaan framework yang dikembangkan pada kasus *cyber fraud*?

13 Batasan Masalah

Batasan masalah yang ada pada penelitian ini adalah sebagai berikut :

1. Penelitian ini hanya fokus dalam kasus kejahatan *cyber fraud* dimana dalam pembuktian kasus fraud tersebut terdapat barang bukti digital
2. Framework yang dikembangkan merupakan pengembangan dari framework untuk fraud forensik / audit forensik dengan digital forensik
3. Pengujian framework ini akan dibatasi pada kasus penggelapan dana institusi dengan rekayasa digital bukti keuangan.

14 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut :

1. Mengembangkan framework yang dapat digunakan untuk proses investigasi *cyber fraud*.
2. Mengevaluasi framework yang dikembangkan sehingga dapat dijadikan sebagai referensi untuk proses investigasi *cyber fraud*.
3. Mengimplementasikan framework yang dikembangkan pada kasus *cyber fraud*.

15 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Memberikan referensi bagi para auditor untuk menginvestigasi *cyber fraud*
2. Menambah pengetahuan baru bagi dunia akademisi untuk mengembangkan framework yang lebih mendalam

16 Tinjauan Pustaka

Dalam penelitiannya menyatakan dalam survey yang dilakukan untuk mendeteksi fraud dengan metode *Artificial Intelligence dan Machine Learning* dimana dalam survey tersebut terdapat adanya gap antara deteksi *fraud* dalam system dan dalam praktek secara nyata (Ryman-Tubb et al., 2018). Ryman menyarankan penggunaan *cognitive computing approach* sebagai arah penelitian ke depan bagi deteksi fraud.

Sebuah penelitian mencoba mengkolaborasikan antara penggunaan *computer forensic* dalam *accounting forensic* dikarenakan kebanyakan informasi accounting sudah berbentuk digital pada masa ini (Cusack & Ahokovi, 2016). Cusack mengembangkan suatu *support tools* untuk membantu mendeteksi fraud lebih cepat dan lebih baik dikarenakan fraud sekarang semakin kompleks. Rekomendasi untuk *support tools* ini ialah dengan mengadopsi analisis rasio finansial sebagai basis dalam software pendeteksi fraud.

Dalam konferensi IEEE terdapat suatu pengajuan framework untuk investigasi forensik *Smart Home Environment* yang terdiri dari 7 phase investigasi walaupun dalam dunia nyata mungkin hanya beberapa fase yang dilaksanakan seperti fase persiapan, pencarian dan mengakuisisi barang bukti, serta analisis data yang telah didapat dari proses akuisisi (Goudbeek et al., 2018). Untuk proses case study sebagai pengujian dilakukan dengan menggunakan *Zigbee protocol* untuk komunikasi *wireless*.

Penelitian yang mengusulkan framework digital forensik untuk egovernment di Uganda (Kigwana et al., 2017) dimana sebelumnya belum ada standar mengenai proses digital forensik yang diterapkan pada egovernment sehingga diusulkan suatu framework untuk memudahkan dalam proses investigasi digital forensik. Framework ini terdiri dari tiga fase yakni *Proactive Process*, *EGovernment Forensics*, dan *Reactive Process*. Dalam proses ini dilakukan *Concurrent Process* untuk meningkatkan potensi dari diterimanya barang bukti di pengadilan.

Sebuah penelitian dilakukan untuk mengajukan framework investigasi forensik pada perangkat IoT yang terdiri dari tiga fase yakni Identification, Preservation dan Analysis (Sathwara et al., 2018). Dalam proses dinilai dapat membantu dalam proses investigasi kejahatan siber yang menggunakan perangkat IoT.

Dengan adanya perangkat IoT yang semakin banyak digunakan dan terjadi tindak kejahatan yang menggunakan perangkat ini sebagai medianya, dikembangkanlah suatu model akuisisi perangkat IoT (Harbawi & Varol, 2017). Dalam penelitian ini, peneliti mengembangkan model akuisisi berdasarkan *Last-On-Scene Algorithm* yang memiliki 7 langkah prosedural. Dan untuk memaksimalkan hasil yang didapat dalam proses investigasi ditambahkan konsep management platform dalam model framework untuk akuisisi perangkat IoT. Dalam penelitian ini tidak melakukan testing terhadap model yang dikembangkan sehingga memungkinkan untuk menjadi bahan riset kedepannya.

Sudah terdapat beberapa framework untuk investigasi digital forensik untuk perangkat android lalu dibuatlah suatu framework yang merupakan pengembangan dari framework dasar digital forensik yang terdiri dari Collection, Examination, Analysis dan Reporting. Framework ini memiliki 7 tahapan yakni *preparation*, *determine scope of crime scene*, *secure evidence devices collection*, *documentation and preservation*, *examination and analysis*, *presentation*, *review* dan satu tahap lagi yakni *trace/loop* untuk memastikan apakah ada tahapan yang dirasa kurang sempurna (Htun & Thwin, 2017). Penelitian lain tentang pengembangan framework/model pada digital forensik pada dilihat pada tabel 1.1.

Tabel 2.1 Ulasan Kritis dari berbagai penelitian

No	Peneliti	Tema	Metode	Hasil
1	(Ahmad et al., 2016)	Pembuatan Network Forensic Framework	Pembuatan dengan mengembangkan model digital forensic yang sudah ada	Framework menghasilkan 8 tahapan untuk IaaS Cloud Computer
2	(Cusack & Ahokovi, 2016)	Penggunaan computer forensics pada	Mengembangkan support tools untuk deteksi fraud	Tools yang diadopsi dengan analisis financial ratio dapat

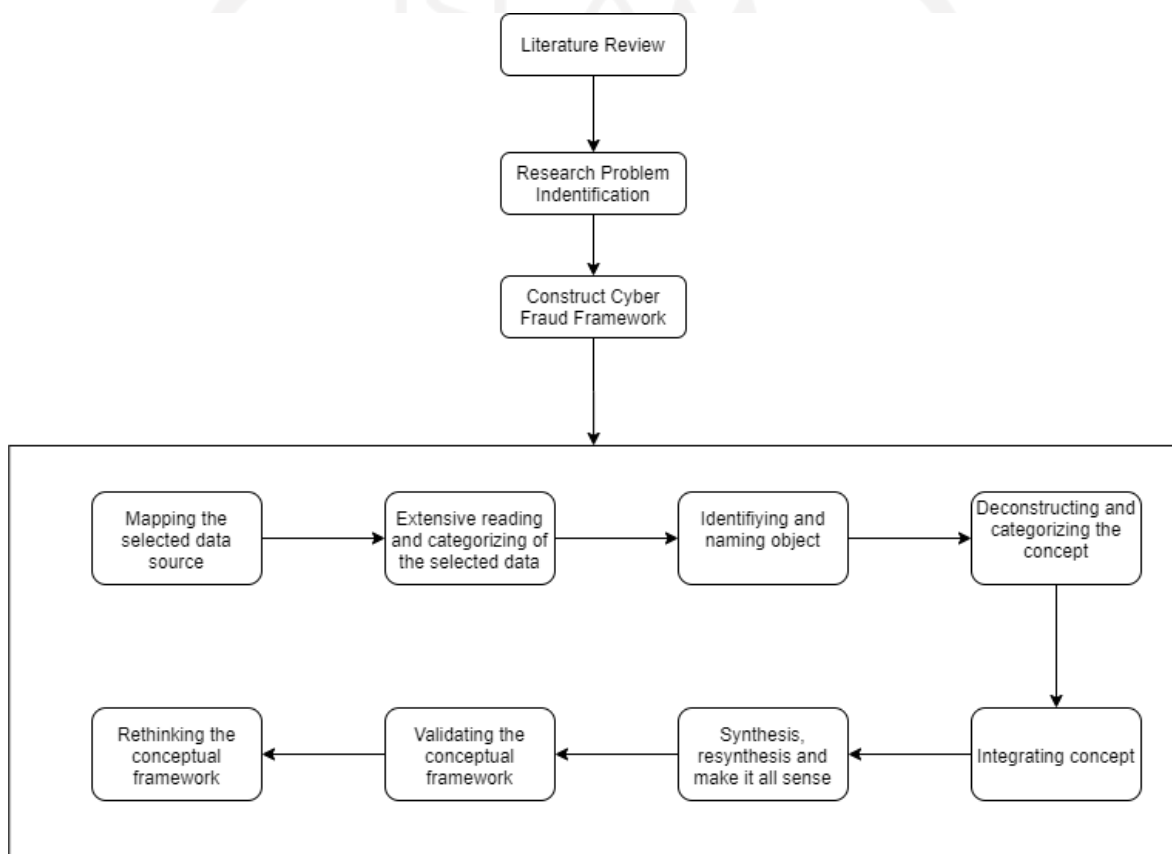
		forensic accounting		digunakan untuk mendeteksi fraud
3	(Manoj & Bhaskari, 2016)	Pembuatan Framework untuk investigasi Cyber Attack di Cloud	Pembuatan framework berdasarkan kendala investigasi dan tantangan yang ada pada Cloud Forensic	Framework yang dikembangkan menggunakan Trusted Third Party dan Cloud Forensics Investigation Team
4	(Kigwana et al., 2017)	Framework Digital Forensic untuk E-government di Uganda	Pembuatan Framework berdasarkan ISO/IEC 27043:2015	Framework ini terdiri dari tiga fase yakni Proactive Process, EGovernment Forensics, dan Reactive Processes
5	(Harbawi & Varol, 2017)	Pengembangan Model akuisisi perangkat IoT	Mengembangkan model akuisisi berdasarkan Last-On-Scene Algorithma	Terdapat 7 langkah procedural pada model untuk mengakuisisi perangkat IoT
6	(Htun & Thwin, 2017)	Mengembangkan Framework untuk Investigasi Digital Forensik untuk Perangkat Android.	Pengembangan dilakukan dari model NIST yang terdiri dari Collection, Examination, Analysis, Reporting	Framework ini memiliki 7 tahapan yakni preparation, determine scope of crime scene, secure evidence devices collection, documentation and preservation, examination and analysis, presentation, review dan satu tahap lagi yakni trace/loop
7	(Alex & Kishore, 2017)	Framework untuk Cloud Computing	Pengembangan framework berdasarkan karakteristik Cloud yang memiliki ketergantungan pada Cloud Service Provider	Penggunaan Forensic Monitoring Plane dan Forensic Server untuk membantu investigasi Cloud Forensics
8	(Ryman-Tubb et al., 2018)	Penggunaan <i>Cognitive Computing</i> Approach untuk deteksi Fraud	Melakukan Survey untuk memeriksa adanya Gap pada metode AI dan ML	Adanya gap dalam deteksi fraud dalam system dan praktek secara nyata
9	(Goudbeek et al., 2018)	Framework untuk Investigasi Forensic Smart Home Environment	Pembuatan framework berdasarkan dari tantangan yang ada pada Smart Home Environment	Terdapat 7 phase dalam framework ini
10	(Sathwara et al., 2018)	Framework untuk Investigasi	Pengembangan Framework berdasarkan tantangan	framework untuk investigasi forensic

		Forensic pada Perangkat IoT	yang ada pada ecosystem IoT	pada perangkat IoT yang terdiri dari tiga fase yakni Identification, Preservation dan Analysis
11	(Afra & Alhadj, 2019)	Pembuatan Integrated Framework untuk ekstraksi jaringan criminal di web	Pengembangan framework dengan karakter dari jaringan criminal di website/online	Framework yang dikembangkan diaplikasikan pada suatu aplikasi website
12	(Sharma et al., 2020)	Pengembangan proses forensic pada cloud based-mobile application	Meningkatkan proses forensic di lingkungan mobile cloud menggunakan metadata yang potensial sebagai barang bukti	Pengembangan dilakukan dengan menjaga timeline secara kronologis dan diuji coba pada aplikasi WeChat
13	(Dimitriadis et al., 2020)	Pengembangan digital forensic framework untuk mereview dan investigasi serangan digital	Pengembangan framework dikarenakan kurangnya instruksi secara detail pada tahapan pemeriksaan dan analisis	Menghasilkan framework bernama D41 yang berfokus pada peningkatan pada tahapan pemeriksaan dan analisis
14	(Koroniotis et al., 2020)	Pengembangan Network Forensik pada jaringan IoT	Pengembangan framework berdasarkan tantangan utama dalam investigasi IoT yakni teknik obfuscating dan encryption	Menghasilkan tiga fungsi baru dan dievaluasi dengan Bot-IoT dan UNSW_NB15
15	(Kumar et al., 2021)	Pengembangan framework untuk perangkat IoT	Pengembangan framework berdasarkan karakter perangkat IoT	Framework yang dihasilkan dinamakan Internet of Forensics yang menggunakan blockchain pada perangkat IoT

Tabel 1.1 menjabarkan berbagai macam pengembangan model atau framework pada digital forensik dimana metode yang digunakan untuk mengembangkan framework biasanya dilakukan berdasarkan karakter, kendala dari objek tersebut atau mengembangkan framework/model yang sebelumnya telah ada berdasarkan kendala yang ditemui. Penelitian ini berfokus mengembangkan framework berdasarkan kendala yang dihadapi pada investigasi *cyber fraud* serta mengembangkan dari framework sebelumnya yang sudah ada. Framework yang dikembangkan menggunakan metode pengembangan konseptual framework miliki Jabareen. Kontribusi yang diharapkan pada penelitian ini yakni dapat membantu proses dalam investigasi kasus *cyber fraud* sehingga tingkat terselesaikan kasus *cyber fraud* semakin meningkat.

1.7 Metodologi Penelitian

Untuk membuat penelitian ini menjadi terarah, maka digunakan suatu metodologi penelitian yang dapat dilihat pada Gambar 1.5. Tahapan pertama yang dilakukan adalah *literature review* untuk mengetahui bagaimana gambaran penelitian terdahulu mengenai tema penelitian, yang selanjutnya ditemukan permasalahan yang menjadi penyebab tema penelitian ini penting untuk diangkat. Tahapan selanjutnya ialah membangun framework berdasarkan metode pengembangan framework yang dirasa cocok dengan tema penelitian ini yakni metode pengembangan konseptual framework yang disebutkan oleh Jabareen.



Gambar 2.5 Model Metodologi Penelitian

1.8 Sistematika Laporan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka laporan penelitian ini disusun atas 5 bagian 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, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penelitian. Pendahuluan berisi mengenai realita dari kasus *cyber fraud* yang

banyak belum terselesaikan dikarenakan adanya komponen barang bukti digital yang membutuhkan penanganan khusus

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori dari berbagai bahan referensi yang terkait guna memecahkan masalah dalam penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ketiga membahas tentang langkah-langkah atau prosedur penelitian, sehingga mampu menyelesaikan masalah secara sistematis. Metode penelitian berisi tahapan metode yang digunakan dalam pengembangan framework *cyber fraud* yakni menggunakan metode pengembangan konseptual framework milik Jabareen serta instrumen untuk evaluasi framework

BAB IV PEMBAHASAN

Bab keempat membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis, dan evaluasi dari penelitian yang diangkat. Hasil dan pembahasan berisi proses dari pengembangan framework dan bagaimana hasil evaluasi framework menggunakan kuesioner

BAB V PENUTUP

Bab kelima merupakan bab terakhir yang memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan. Kesimpulan membahas bagaimana hasil dari pengembangan framework dan evaluasi dan harapan untuk penelitian selanjutnya

BAB 2

Tinjauan Pustaka

2.1 Fraud

Fraud secara umum mengacu pada tindakan yang salah atau tindakan penipuan yang ditujukan untuk memperoleh keuntungan *financial* bagi pribadi atau menyebabkan kerugian *financial* bagi orang lain (Material, 2019).

Sedangkan dalam kamus bisnis, fraud merupakan tindakan penipuan, atau menyembunyikan sesuatu dengan sengaja, tindakan kelalaian, atau memutarbalikan fakta untuk :

1. Melanggar hukum atau mendapatkan keuntungan secara tidak adil
2. Memisahkan sesuatu atau seseorang dengan sesuatu yang berharga, atau menyerahkan hak akan sesuatu
3. Menyebabkan cedera dalam kondisi tertentu

Terdapat 2 jenis fraud yang dikenal dalam dunia *accounting* yakni *management fraud* atau biasa disebut dengan *financial statement fraud* dan *employee fraud* atau *embezzlement* (Durtischi, 2001). Jenis fraud yang lain adalah *tax fraud*, *wire fraud*, *mail fraud*, dan *bank fraud*. Fraud sendiri dibagi menjadi 3 kategori yakni *Financial Frauds*, *Asset Misappropriations*, dan *Corruption*.

Dalam buku *Fraud Auditing and Forensics Accounting* terdapat 3 alasan kenapa seseorang melakukan tindakan fraud atau biasa disebut *Fraud Triangle* yang diperkenalkan oleh Donald Cressey pada tahun 1953 setelah melakukan interview pada penghuni Illinois State Penitentiary. Dari hasil interview didapatkan alasan kenapa orang melakukan fraud yakni :

1. *Pressure*

Seseorang dapat melakukan tindakan yang tidak baik dikarenakan adanya tekanan seperti kekurangan financial, kerakusan, hutang, keinginan untuk memenuhi ekspektasi stakeholder, rekognisi social dan self esteem yang kuat (Hogan et al, 2008; Kassem dan Higns, 2012). Dalam sumber yang lain (Murphy, 2016) menyebutkan fraud terjadi karena adanya kondisi pekerjaan yang buruk dan kemarahan kepada instansi serta perubahan iklim dalam pekerjaan.

2. Opportunity

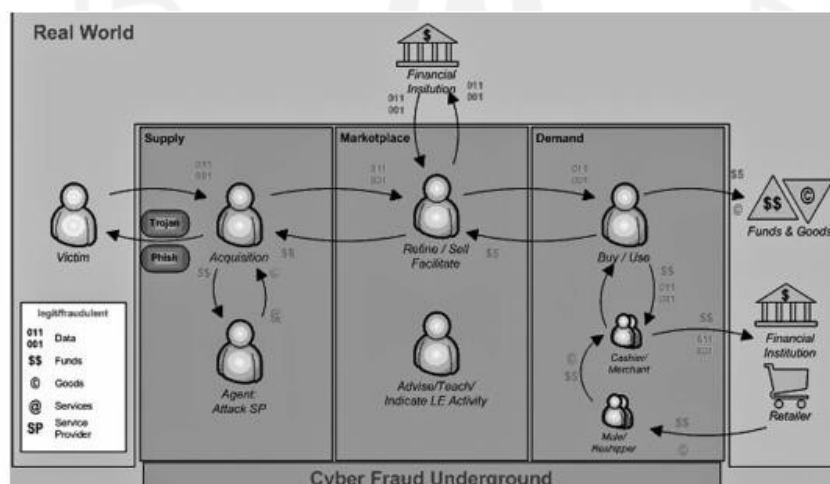
Kesempatan merupakan salah satu alasan kenapa seseorang berani melakukan tindak kejahatan fraud seperti struktur pemerintahan yang lemah, kurang efektifnya control dari pihak internal dan control lingkungan yang buruk (Trompeter et al, 2013). Sedangkan menurut (Donelson et al, 2017) lemahnya control internal di entry level juga menyebabkan fraud.

3. Rationalization

Menurut Cressey yang menginterview para tahanan menyatakan bahwa para pelaku fraud berusaha untuk merasionalisasi tindakan mereka saat melakukan fraud (Cressey, 1953). Mereka menyatakan bahwa melakukan kecurangan merupakan suatu hal yang dinilai wajar, dikarenakan bagi mereka perusahaan telah melakukan kesalahan terhadap mereka.

2.2 Cyber Fraud

Cyber fraud atau *online financial cyber crime* sudah meningkat selama beberapa tahun hal ini dikarenakan oleh penggunaan internet yang semakin tinggi (Howard, 2009). Selain itu, penyebab banyaknya kejahatan jenis adalah mudahnya korban tertipu. Metode yang paling banyak digunakan dalam operasi ini adalah dengan menggunakan metode *Scam*. Bryan menggambarkan sebuah *cyber fraud* model seperti Gambar 2.1 dimana terlihat bagaimana pelaku kejahatan berusaha melakukan akuisisi dari data korban dan melakukan transaksi ke marketplace menggunakan *kredensial* dari korban.



Gambar 2.2 Cyber Fraud Model (Bryan 2007:Verisign iDefence,2007).

Cara mendapatkan informasi finansial merupakan elemen penting untuk melakukan *cyber fraud*, sebagaimana disebutkan dalam metode dibawah ini :

1. *Phising*

Phising dilakukan dengan cara pelaku membuat suatu website resmi dari suatu bank atau institusi *finance* yang lain dimana ketika calon korban terjebak untuk mengklik spam email dari pelaku yang kemudian mengarahkan korban ke website palsu. Selanjutnya pelaku akan menangkap informasi login dan informasi financial lainnya ketika korban memasukkan semua data ke website tersebut yang sebelumnya dikira sebagai website yang asli.

2. *Network Intrusion*

Pelaku dapat mengambil informasi berharga dari calon korban dengan memanfaatkan jaringan yang digunakan oleh korban. Terdapat beberapa software yang digunakan untuk mendapatkan apa yang dilakukan seseorang dan informasi yang ditransfer oleh seseorang didalam suatu jaringan baik jaringan wifi maupun jaringan

3. *Trojan Horses*

Program ini sangat terkenal untuk mencuri data dan terlihat seperti program biasa. Korban biasanya secara tidak sengaja menginstall program berisi trojan yang memiliki fungsi *keylogging*, dimana software ini akan mencatat aktivitas yang dilakukan korban saat memasukkan input transaksi pada marketplace tertentu.

4. *Real World Theft*

Metode ini digunakan dengan skimmer, dimana pelaku akan menaruh alat skimmer pada mesin-mesin ATM. Skimmer ini akan menyimpan data dari ATM korban saat kartu tersebut dimasukkan ke dalam mesin ATM. Terkadang pelaku yang telah mendapatkan banyak informasi kartu ini akan menjualnya di forum online.

Sedangkan pelaku dapat menjual lagi informasi financial tersebut di *Carding Forum*, *Dumps Vendor*, *Noncarding-Related Forums* dan *Notable Carder*

2.3 **Accounting Forensik/ Fraud Audit**

Audit Forensik maupun Fraud Accounting memeriksa dari setiap transaksi dan berfokus apa esensi dari transaksi tersebut (Bologna et al, 2016). Fraud Auditor akan lebih mencari tahu dimana letak titik lemah dari suatu system , bagaimana suatu offline transaksi dihandle dan siapa yang mengotorisasi suatu transaksi, bagaimana cara memanipulasi suatu system dan lain sebagainya.

Seorang *accountanting forensic* harus memiliki skill, kemampuan dan pengetahuan yang cukup baik mengenai siklus fraud termasuk penyelesaian dalam bidang hukum. Audit

untuk fraud sama saja dengan *forensic auditing*. Dibutuhkan sertifikasi untuk menjadi seorang auditor seperti *Certified Fraud Examiner*. Ada beberapa tahap yang dilakukan untuk melakukan *forensic auditing* yakni (Manning, 2005):

1. *Recognition and Planning Stage*

Merupakan tahap perencanaan dimana seorang auditor harus yakin bahwa ada fraud dikasus tersebut. Pemeriksaan pun harus direncanakan dengan matang baik dari segi tim yang akan ditunjuk, metode yang akan dipakai, tempat yang akan diinvestigasi ataupun kebutuhan lain yang mendukung proses pemeriksaan

2. *Evidence Collection*

Tujuan dari proses ini adalah untuk menentukan apakah barang bukti tersebut cocok dengan kasus yang sedang diperiksa. Dan sebagai petunjuk apabila membutuhkan prosedur lain untuk menyelesaikan masalah fraud ini.

3. *Evidence Evaluation*

Proses ini berfungsi untuk menentukan tindakan hukum apa yang akan diambil setelah barang bukti dikumpulkan. Pada tahapan ini membutuhkan kerjasama dari berbagai pihak seperti pihak manajemen, penasehat hukum, internal audit dan pihak penyedia jasa keamanan. Apabila barang bukti sudah cukup kuat untuk digunakan di persidangan maka strategi seterusnya dapat dijalankan.

4. *Communication of Result*

Dalam proses pemeriksaan ini sebuah laporan audit harus dipersiapkan dan dipresentasikan kepada pihak manajemen.

Menurut (Saxunova, 2012), menyebutkan pelaksanaan investigasi fraud dilakukan apabila ada sesuatu kegiatan yang dinilai mencurigkan atau tidak wajar yang dapat berpotensi sebagai tindak kejahatan. Tim investigasi dibentuk dan terdiri dari ketua, anggota, perwakilan pihak manajemen, supervisor dan seorang konsultan hukum. Proses investigasi dilakukan dengan urutan sebagai berikut :

1. Pembuatan rencana investigasi
2. Mendeteksi dan menganalisis tindak kejahatan dan mempersiapkan jadwal kegiatan
3. Pengumpulan bukti
4. Interview
5. Pembuatan dokumentasi dari hasil temuan sesuai protocol yang ada

Berdasarkan Asosiasi Pemeriksa Fraud yang Bersertifikasi atau ACFE, pengumpulan barang bukti termasuk didalamnya dokumen internal seperti file pribadi, catatan telepon, file computer dan perangkat elektronik yang lain.

3.4 *Digital Evidence*

Terdapat 4 jenis barang bukti yang dapat digunakan sebagai landasan untuk melakukan investigasi yakni : *Testimonial Evidence*, *Documentary Evidence*, *Physical Evidence*, dan *Personal Observation* (Albrecht et al., 2012:50). Bukti tersebut dapat dijadikan sebagai kecurigaan atas anomaly kegiatan yang ada sehingga perlu dilakukan investigasi apakah terjadi fraud dalam instansi tersebut. *Testimonial Evidence* berkaitan dengan testimony dari individu yang dilakukan dengan interview, interogasi maupun tes kejujuran. *Documentary Evidence* didapatkan dari dokumen baik tercetak maupun dokumen di computer dengan menggunakan pemeriksaan dokumen, data mining, pencarian data public, audit, pencarian di computer, analisis dokumen keuangan, hingga memeriksa database dan email instansi. *Physical Evidence* didapatkan dari finger print, property yang hilang atau dicuri yang mana dalam mengumpulkan bukti ini dibutuhkan bantuan ahli forensik. *Personal Observation* merupakan sesuatu yang dirasakan baik dilihat, didengar oleh indra dari investigator sendiri. Dalam kasus cyber fraud barang bukti yang akan menjadi barang bukti utama yakni *Documentary Evidence* yang terdiri dari barang bukti digital dan dokumen fisik yang dapat menunjang proses investigasi.

Bukti Digital dapat didefinisikan sebagai informasi atau data yang berharga untuk proses investigasi yang dapat digunakan sebagai bukti untuk mendukung ataupun menolak dugaan tindak criminal dan disimpan, diterima ataupun ditransmisikan menggunakan perangkat elektronik (National Forensic Science Technology Center, 2014). Bukti Digital dapat diambil dari semua perangkat digital mulai dari computer, telepon, laptop, kamera, CCTV, PDA, IoT, harddisk, USB dan lain sebagainya. Bukti digital memiliki beberapa karakteristik yang perlu diperhatikan oleh para investigator agar barang bukti tersebut tetap dapat diterima di meja pengadilan, karakteristik tersebut yakni :

1. Tersembunyi seperti bukti sidik jari atau DNA
2. Tanpa batas atau borderless dan melampaui batas yurisdiksi
3. Dapat diubah, rusak, atau hancur
4. Sensitif terhadap waktu

Untuk melakukan assesmen, harus menggunakan *tools* tertentu dan tenaga yang telah terlatih sehingga barang bukti tetap *authentic*. Setelah barang bukti diamankan akan

dilakukan *imaging* atau akuisisi menggunakan forensics tools seperti Encase, FTK, Belkasoft dan tools lainnya. Untuk pemeriksaan dan analisis menggunakan kopian dari original copy bukti yang sudah diakuisisi. Pemeriksaan bukti digital dilakukan sesuai prosedur yang telah ditetapkan dan dilakukan oleh pemeriksa yang telah dilatih mengenai *digital forensic*. Pemeriksaan yang tidak sesuai prosedur dapat merusak bukti digital dimana hal tersebut akan sangat merugikan bagi penyelidikan yang telah dilaksanakan.

3.5 Penanganan Bukti Digital

Ada beberapa metode penanganan bukti digital yang sudah familiar dalam dunia digital forensik, seperti dari aturan perkap no 10 tahun 2010, perkap no 8 tahun 2014, standar ISO 27037:2012, NIJ US Departement of Justice, ACPO, dan dari MOSTI Malaysia. Dalam pedoman *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (National Institute of Justice (NIJ) US Departement of Justice:2004) ada beberapa metode untuk penanganan bukti digital yakni :

1. *Policy and Procedure Development*
2. *Evidence Assesment*
3. *Evidence Acquisition*
4. *Evidence Examination*
5. *Documenting and Reporting*

ACPO atau Association of Chief Police merupakan asosiasi pimpinan kepolisian di Inggris mengeluarkan sebuah dokumen panduan untuk pengumpulan barang bukti digital yang berjudul “Good Practice Guide For Computer Based Electronic Evidence” (Association of Chief Police:2014). Dalam dokumen ACPO disebutkan beberapa tahap dalam penanganan bukti digital seperti :

1. *Plan* (Perencanaan)
2. *Capture* (Merekam atau Dokumentasi)
3. *Analyse* (Analisis)
4. *Present* (Presentasi Hasil)

Dalam Standard Operating Procedure of Digital Evidence Collection dari MOSTI Malaysia(Khadijah et al., 2013) menyatakan ada beberapa tahapan dalam melakukan pengumpulan barang bukti digital seperti,

a. Identification

Berisi beberapa pertanyaan yang digunakan sebagai pendahuluan untuk mendapatkan informasi mengenai barang bukti digital yang akan dicari.

b. Collection

Tahapan selanjutnya yang berupa pengumpulan barang bukti digital dilakukan dengan beberapa tahapan yakni persiapan, pelaksanaan, pengumpulan dan transportasi barang bukti digital.

c. Analysis

Tahapan ini berisi ekstraksi, analisis dan rekonstruksi data dari barang bukti yang telah didapatkan sebelumnya. Analisis dilakukan dalam laboratorium forensik dan dilaksanakan oleh seorang analis forensik..

d. Presentation

Tahapan untuk melakukan presentasi data dari hasil analisis di tahapan sebelumnya

e. Preservation

Preservasi merupakan tahap dimana barang bukti dijaga agar tidak diubah, integritas barang bukti terjaga dan chain of custody tetap terjaga.

Sedangkan dalam standar ISO 27037:2012 (Smutny & Veber, 2015) terdapat 4 tahapan untuk melakukan penanganan bukti digital yakni :

a. Identification

Merupakan proses pencarian, deteksi dan mendokumentasikan bukti digital baik dalam bentuk fisik maupun dalam bentuk digital

b. Collection

Proses ini dilakukan setelah proses identifikasi selesai, dimana alat tersebut dipindah dari lokasi aslinya dan ditransfer ke laboratorium forensik dimana barang bukti tersebut akan dianalisis dan di proses ke tahap selanjutnya

c. Acquisition

Proses ini menghasilkan copy dari barang bukti, atau disebut proses imaging dan mendokumentasikan proses yang dilakukan pada tahap ini

d. Preservation of Digital Evidence

Preservasi dilakukan untuk menjaga integritas dari barang bukti tersebut agar dapat digunakan hingga ke pengadilan.

Dalam Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 tahun 2009 dalam pemeriksaan barang bukti elektronik harus mengikuti persyaratan teknis berikut,

a. Penanganan barang bukti computer yang berkaitan dengan data yang tersimpan dalam harddisk atau penyimpanan data storage lainnya dari sejak penanganan pertama harus sesuai dengan tata cara yang berlaku, karena barang bukti memiliki sifat yang mudah

hilang dan berubah dan bila penyidik tidak memahami cara penyitaan barang bukti komputer dapat meminta bantuan Labfor Polri

b. Barang bukti dikirim secara lengkap dengan seluruh sistemnya

c. Barang bukti dibungkus, diikat, disegel dan diberi label

d. Pengiriman barang bukti ke Labfor Polri dapat melalui pos sendiri atau kurir

3.6 Digital Forensic Investigation Process (DFIP)

Salah satu badan standar internasional yakni ISO/IEC mempublish sebuah standar ISO/IEC 27043:2015 pada bulan maret yang diberi judul “Information technology – Security techniques – Incident Investigation Principles and Process” . Standar ini merupakan standar yang mengatur Proses Investigasi Digital Forensik dalam scope yang lebih luas atau dapat disebut sebagai umbrella standard yang memayungi beberapa standar ISO dalam digital forensik (Valjarevic et al., 2017) . Terdapat beberapa standar ISO mengenai Digital Forensik yakni :

- ISO/EIC 27037 “*Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*”. Dokumen ini dinilai sebagai awal dari tahap awal penanganan proses investigasi digital forensik. Dokumen ini berisi high level dokumen yang memberikan panduan secara luas pada penanganan potensi bukti digital yang ada.
- ISO/EIC 27038 “*Spesification for digital redaction*”. Merupakan dokumen yang membahas mengenai proses “redaction” pada barang bukti digital. Tidak semua informasi yang ada akan dipublikasikan kepada public sehingga diperlukan suatu proses dimana hanya informasi yang berkaitan dengan kasus saja yang akan disampaikan ke public.
- ISO/EIC 27040 “*Storage Security*”. Dokumen ini membahas mengenai panduan teknis yang berhubungan dengan keamanan penyimpanan data . Keamanan penyimpanan data ini berkaitan dengan melindungi informasi yang rahasia, menjaga integritas dari barang bukti tersebut dan ketersediaan data selama disimpan. Atau dapat juga bermakna melindungi data saat transit pada suatu jaringan.
- ISO/EIC 27041 “*Guidance on assuring suitability and adequacy of incident investigative method*”. Berisi prosedur, metodologi dan proses selama investigasi digital forensik harus diuji secara benar agar hasil dari investigasi dinilai valid dan diterima di pengadilan.

- ISO/EIC 27042 “Guidelines for the analysis and interpretation of digital evidence” . Dokumen standar ini menjelaskan mengenai metodologi dan proses yang dilakukan selama investigasi dapat didesain dan diimplementasikan agar dapat mengevaluasi hasil bukti digital , interpretasi dan laporannya.
- ISO/EIC 30121 “Governance of digital forensic risk framework”. Dokumen ini menjelaskan mengenai persiapan organisasi untuk menghadapi tindak kejahatan yang berhubungan dengan barang bukti digital. Sehingga sebelum tindak kejahatan terjadi, organisasi tersebut telah memiliki prosedur untuk mitigasinya.
- ISO/EIC 27035 “Information security incident management”. Berisi mengenai konsep standard dan tahapan informasi dari manajemen incident security serta bagaimana meningkatkan perfoma dari incident management.
- ISO/EIC 27050 Merupakan dokumen yang menjelaskan mengenai Electronic Discovery, proses dari penemuan Electronically Stored Information (ESI) atau data lain yang terlibat pada proses investigasi.

Tabel 2.2 Kriteria ISO EIC (Valjarevic et al., 2017)

<i>ISO Standard</i>	<i>Focus area and scope</i>	<i>Level of detail</i>	<i>Area of Application</i>	<i>Technology oriented or process oriented</i>
27043	<i>Principles and Process; Complete Digital Forensic Investigation Process</i>	<i>High level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process Oriented</i>
27035-1	<i>Incident Management</i>	<i>High Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process Oriented</i>
27035-2	<i>Incident Response</i>	<i>Mid Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process and Technology Oriented</i>
27035-3	<i>CSIRT Operations</i>	<i>Mid Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process and Technology Oriented</i>

27037	<i>Identification, Collection, Acquisition and Preservation of Digital Evidence</i>	<i>Detailed Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process and Technology Oriented</i>
27038	<i>Digital Redaction</i>	<i>Detailed Level</i>	<i>Digital Redaction of Documents</i>	<i>Technology Oriented</i>
27040	<i>Storage Security</i>	<i>Very Detailed Level</i>	<i>Security of computer storage</i>	<i>Technology Oriented</i>
27041	<i>Incident Investigative Method</i>	<i>High Level</i>	<i>Digital Forensic Methods, Tools, Processes and Procedures</i>	<i>Process Oriented</i>
27042	<i>Analysis and Interpretation of Digital Evidence</i>	<i>High Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process Oriented</i>
27050	<i>Electronic Discovery</i>	<i>Mid Level</i>	<i>Identification, Preservation, Collection, Processing, Review, and Production of Digital Evidence</i>	<i>Process and Technology Oriented</i>
30121	<i>Digital Forensic Risk Framework</i>	<i>High Level</i>	<i>Civil, Criminal, and Enterprise Investigations</i>	<i>Process Oriented</i>

Pada tabel 2.1 dijelaskan mengenai perbedaan fokus area, level detail, area implementasi dan berorientasi teknologi atau proses, yang mana dari tabel dibawah ini disimpulkan bahwa ISO /IEC 27043 merupakan standar yang dapat digunakan sebagai model dalam

investigasi digital forensik dikarenakan fokus area yang sangat luas, dengan memayungi standar sebelumnya.

3.7 Delphi Method

Metode untuk pengujian kualitas framework yang digunakan ini akan menggunakan metode survey dengan Delphi Method. Delphi method ini dikembangkan oleh Rand Corporation sebagai teknologi yang digunakan untuk memprediksi masa depan dan mempengaruhi dalam pengambilan keputusan maupun kebijakan. Awalnya metode survey Delphi ini digunakan pada bidang kesehatan, keperawatan dan penelitian mengenai pelayanan kesehatan namun metode ini selanjutnya digunakan pada berbagai macam jenis bidang penelitian (Hasson et al., 2000). Hal penting yang menjadi dasar pentingnya penggunaan Delphi yakni bahwa metode ini memfasilitasi group diskusi yang sangat kompleks hingga terjalin suatu consensus bersama mengenai permasalahan yang sedang diteliti. Delphi method memiliki 5 karakteristik yakni (Loo, 2002):

1. Sampel yang digunakan atau disebut dengan panel terdiri dari ahli yang dipilih secara hati hati dan ahli tersebut merupakan representasi dari bidang keahlian
2. Peserta biasanya tidak dikenali atau anonim
3. Moderator membuat beberapa seri dari kuesioner yang terstruktur dan laporan umpan balik dari panel
4. Merupakan proses iterasi yang kadang terdiri dari 3-4 ronde kuesioner dan umpan balik
5. Terdapat output yang berupa laporan penelitian dengan hasil dari Delphi method , perkiraan prediksi , kenijakan dan pilihan program dengan berbagai macam pandangan mengenai kekuatan, kelemahan dan rekomendasi untuk manajemen.

Delphi method juga telah digunakan pada penelitian pada bidang Informasi Teknologi , dimana penelitian pada bidang ini digunakan untuk menambah efisiensi dan efektivitas dari infrastruktur IT(Brady, 2015).

Pelaksanaan Delphi Method terdapat beberapa jenis proses dimana proses ini didesain untuk mengabungkan opini menjadi consensus, rincian proses ini terdiri dari :

1. *Pilot testing* ini terdiri dari group kecil
2. *Initial questionnaire* pada tahapan ini komentar kualitatif diminta dari peserta
3. *Initial feedback* dilakukan dengan penghitungan kuantitatif setelah analisis statistik
4. *Subsequent questionnaire* dilakukan dengan mengumpulkan komentar kualitatif lagi dari peserta setelah feedback

5. *Subsequent feedback* memungkinkan bagi peserta untuk menganti opini /jawabannya(Grisham, 2009).

Penggunaan Delphi method sangat bermanfaat pada bidang penelitian dimana untuk mendapatkan jawaban dari permasalahan membutuhkan penilaian secara kolektif tetapi tidak dimungkinkan untuk dilaksanakan dikarenakan beberapa hal seperti perbedaan daerah, jarak , waktu maupun konflik personal(Grime & Wright, 2016)

Delphi method mulai digunakan pada berbagai jenis penelitian, salah satunya pada penelitian bidan Teknologi Informatika maupun Sistem Informasi. Terdapat variansi yang sangat banyak pada jumlah sampel yang digunakan untuk Delphi method baik heterogen maupun homogeny sampel. Tingkat keahlian pun bervariasi dimana pada satu penelitian dan yang lainnya dapat berbeda.satu penelitian dan yang lainnya dapat berbeda. Delphi method masih dipandang sebagai metode yang efektif dan efisien untuk digunakan pada penelitian pada IT atau SI (Skulmoski et al., 2007).

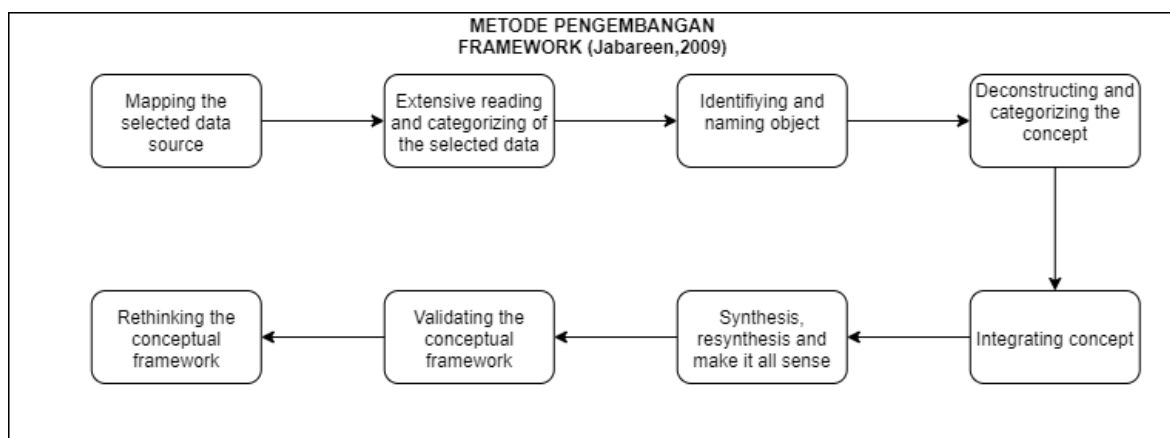
BAB 3

Metodologi

3.1 Pengembangan Framework

Pada bab ini akan dibahas mengenai proses atau metodologi pembuatan framework untuk investigasi kasus fraud yang berbasis siber. Penelitian ini akan mengembangkan suatu konseptual framework untuk investigasi *cyber fraud*, dimana konseptual framework merupakan suatu model yang disusun oleh peneliti untuk menerangkan mengenai hubungan yang ada pada variable-variabel dalam penelitian atau dapat merupakan adaptasi dari model yang sudah ada yang kemudian diadaptasi sesuai dengan tujuan dari penelitian (Adom & Hussain, Emad.Kamil. and Joe, 2018). Konseptual framework berbeda dengan *teoritical* framework dimana pada konseptual framework lebih spesifik tertuju pada objek yang diteliti. Pembuatan suatu konseptual framework akan dibuat sesuai dengan kebutuhan penelitian, dimana peneliti yang lebih memahami mana yang dibutuhkan dalam pembuatan framework (Dickson et al., 2018) sehingga dalam penelitian ini akan menggunakan metode pengembangan konseptual framework berdasarkan jurnal yang ditulis oleh Yosef Jabareen yang berjudul *Building a Conceptual Framework: Philosophy, Definitions, and Procedure*.

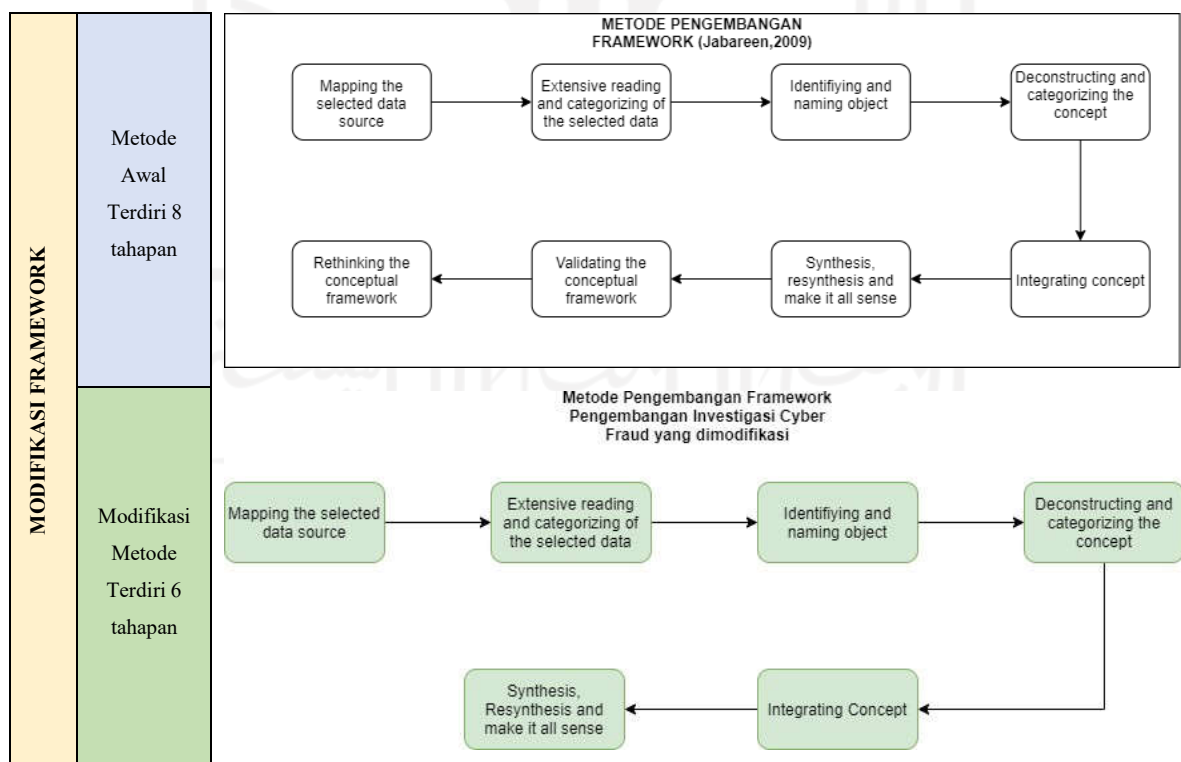
Alasan utama dalam pemilihan penggunaan metode pengembangan milik Jabareen dikarenakan konseptual framework mengakomodir pembuatan framework lintas disiplin (Eizenberg & Jabareen, 2017) sebagaimana penelitian ini yang merupakan penelitian multidisiplin yakni dalam bidang Audit Fraud dan Digital Forensik.



Gambar 3.1 Metode Pengembangan Konseptual Framework.

Dalam penelitian Jabareen disebutkan bahwa konseptual framework merupakan suatu jaringan atau “pesawat” yang menyambungkan beberapa konsep persamaan serta dapat memberikan penjelasan yang komprehensif yang mudah dimengerti pada suatu fenomena. Konseptual framework tidak hanya gabungan dari beberapa konsep tapi lebih mendekati suatu bangunan dimana setiap konsep memegang peranan penting dalam framework ini. Konsep-konsep yang ada pada konseptual framework berfungsi untuk saling memberikan dukungan, memperkuat fenomena yang ada dan membangun filosofi framework yang lebih spesifik. Framework ini tidak hanya kumpulan dari berbagai macam konsep dari multi disiplin ilmu tetapi konsep-konsep tersebut saling membangun dimana setiap konsep memegang peranan penting. Konseptual Framework memiliki 3 asumsi yakni ontological , epistemological dan methodological dimana setiap konsep yang ada pada framework membawa satu jenis peran. Asumsi Ontological berkaitan dengan kenyataan yang ada pada realita, sedangkan epistemological adalah bagaimana sesuatu itu semestinya berjalan dan yang terakhir adalah methodological bagaimana suatu proses dapat membantu membuat framework berjalan semestinya (Jabareen, 2009). Dalam pembuatan konseptual framework terdapat 8 fase sebagaimana yang disebutkan oleh Jabareen seperti yang digambarkan pada Gambar 3.1.

3.2 Modifikasi Framework



Gambar 3.2 Modifikasi Metode Pengembangan Framework

Adapun pada penelitian ini, untuk pengembangan framework akan dimodifikasi menjadi 6 tahapan saja seperti yang ditunjukkan pada gambar 3.2 yang berada di tabel bawah dan berwarna hijau (Haddadi et al., 2016), tahapan *Validating the Conceptual Framework* dan *rethinking conceptual framework* merupakan tahapan yang diharapkan untuk diteliti lebih jauh untuk penelitian selanjutnya, dikarenakan pada tahapan *Validating The Conceptual Framework* akan lebih baik saat dipresentasikan pada suatu konferensi sehingga mendapatkan umpan balik dari peserta sebagai bentuk perbaikan framework kedepannya sehingga pada penelitian ini dua tahapan tersebut tidak dilakukan. Adapun untuk penjelasan masing masing fase dalam metode pengembangan konseptual framework dari Jabareen dapat dilihat pada penjelasan dibawah ini.

3.3 Mapping the selected data sources

Tahapan pertama dalam pembuatan framework ini adalah membuat peta spektrum dari beberapa lintas disiplin literatur yang berkaitan dengan topik atau pertanyaan dari penelitian.

Dalam proses ini juga termasuk mengidentifikasi berbagai tipe teks dan sumber data lain seperti data empirik maupun praktik sehingga data yang dikumpulkan bersifat komprehensif.

Pada penelitian ini terdapat dua disiplin ilmu yang akan diteliti yakni bidang Audit Fraud dan Digital Forensik, sehingga dibutuhkan sebanyak mungkin referensi mengenai dua bidang ilmu tersebut dengan kata kunci pengembangan framework, investigasi fraud, tantangan dalam investigasi fraud, framework *digital forensic*. Referensi yang digunakan merupakan hasil penelitian, buku, maupun berita dari dua disiplin ilmu tersebut.

3.4 Extensive reading and categorizing of the selected data

Fase kedua ini bertujuan untuk membaca keseluruhan data yang telah dikumpulkan dan selanjutnya dikategorikan sesuai dengan disiplin ilmu serta skala kepentingan dan lingkup komprehensif pada tiap disiplin. Fase ini berguna untuk memaksimalkan keefektifan proses investigasi dan menekankan bahwa tiap tahapan merupakan perwakilan yang representatif dari tiap disiplin ilmu.

Dari berbagai referensi yang telah ditemukan kemudian data tersebut dikelompokkan masuk pada kategori bidang ilmu Fraud Audit atau pada Digital Forensik. Apabila ada data yang memiliki persamaan dapat dimasukkan pada baris yang sama dikarenakan sudah ada data lain yang mewakili data tersebut. Untuk mempermudah mengkategorikan dapat menggunakan table seperti yang ditunjukan pada tabel 3.1.

Tabel 3.1 Tabel kategori data

Data	Kategori
- Data A	-Audit Fraud
- Data B	-Digital Forensik

3.5 *Identifying and naming concept*

Digunakan untuk membaca dan membaca lagi dari data yang sudah dipilih dan menemukan konsep yang tepat pada tiap disiplin ilmu. Pada fase ini akan menghasilkan beberapa konsep yang hampir sama atau bahkan saling bertolak belakang. Secara umum, dalam fase ini dapat menggunakan konsep yang sudah ada pada literatur. Pada tahapan ini dari data-data yang telah dikategorisasikan pada proses sebelumnya akan diidentifikasi dan diberi nama konsep.

3.6 *Deconstructing and categorizing the concepts*

Tahapan fase ini adalah untuk mendekonstruksi dari tiap konsep untuk mengidentifikasi atribut utama, karakteristik, asumsi, peran dan untuk mengkategorisasikan masing masing konsep sesuai dengan sifat mereka seperti ontological, epistemological dan methodological.

Pada setiap konsep yang telah dibuat akan dipecah dan dilihat apabila ada kesamaan konsep pada dua bidang ilmu yang ada. Dan selanjutnya akan diklasifikan menurut sifat pada konsep tersebut seperti yang ditunjukkan pada table 3.2.

Tabel 3.2 Tabel klasifikasi konsep data

Konsep	Sumber data	Sifat Konsep
- Konsep A	- Audit Forensik	- Ontological
- Konsep B..dst	- Digital Forensik..dst	- Epistomological..dst

Proses untuk mengurangi konsep yang sama dilakukan dengan metode dibawah ini(Kohn, 2012) :

- Setiap konsep yang memiliki nama yang sama pada beberapa framework dihitung menjadi satu
- Jika ada konsep yang memiliki deskripsi atau arti yang sama dengan konsep yang lainnya walaupun dengan nama yang berbeda, maka akan dihitung menjadi satu saja
- Apabila konsep tersebut berdiri sendiri tanpa memiliki persamaan konsep baik secara bahasa maupun makna dengan konsep diframework yang lain, maka akan dihitung satu
- Ulangi tahapan sehingga konsep menjadi seminimal mungkin tanpa redudansi bahasa/makna

Contoh mengaplikasikan konsep pengurangan redudansi konsep, yakni pada konsep *collect* dan *acquire*. Pengertian *Collect* adalah sebuah tahapan dimana diikuti dengan proses pencarian, identifikasi, pengumpulan dan dokumentasi dari suatu barang bukti digital sedangkan *Acquire* didefinisikan sebagai tahapan yang dilakukan pada barang bukti digital yang rapuh secara kondisi sehingga dapat dirubah, rusak maupun hancur akibat dari proses pemeriksaan yang tidak sesuai dengan standar (Ashcroft et al., 2004). Dari kedua tahapan tersebut dapat disimpulkan bahwan *Acquire* merupakan tahapan praktikal dari proses *Collection*, sehingga untuk pengurangan konsep diilustrasikan sebagai berikut :

Apabila

A merupakan konsep yang memiliki deskripsi “*Collect*”

B merupakan konsep yang memiliki deskripsi “*Acquire*”

Maka $A \setminus B \therefore Collect \equiv Acquire$

Dan pada penggunaan konsep yang baru digunakan nama konsep *Collect* dikarenakan pada proses tersebut lebih banyak muncul dan lebih umum dibandingkan dengan konsep lainnya yang memiliki makna sejenis (Kohn, 2012).

3.7 Integrating concepts

Tahapan ini berguna untuk mengintegrasikan dan mengelompokan konsep yang memiliki persamaan ke dalam satu konsep baru. Pada fase ini dari sekian banyak konsep yang telah dibuat akan mengalami pengurangan secara drastis dan memungkinkan untuk dilakukan manipulasi untuk mendapatkan beberapa langkah konsep yang realistis. Dari konsep yang telah ada akan dipilih konsep yang merepresentasikan yang kemudian diintegrasikan menjadi framework yang utuh.

3.8 Synthesis, Resynthesis and making it all make sense

Tujuan dari fase ini untuk mensintesis konsep pada framework. Peneliti harus terbuka, toleran dan fleksibel dalam proses teorisasi dan membuat teori baru. Proses ini bersifat iteratif dan termasuk didalamnya proses sintesis dan resintesis hingga peneliti menemukan teori umum yang masuk akal. Setelah integrasi konsep telah selesai maka perlu dikomparasikan dengan data pada penelitian sebelumnya.

3.9 Evaluasi Framework

Untuk framework yang telah dikembangkan sebelumnya menggunakan metode Jabareen , selanjutnya framework tersebut dievaluasi oleh praktisi di bidang Audit Fraud dan Digital Forensik menggunakan kuesioner. Kuisisioner dibuat menggunakan delphi method. Delphi method merupakan salah satu metode survey yang cukup populer digunakan pada penelitian sistem informasi.

Metode delphi survey merupakan survey yang dilakukan pada seorang ahli dan menyediakan variasi sesuai dengan tujuan penelitian. Metode ini juga dapat digunakan untuk menyatukan pendapat tentang identifikasi kendala pada permasalahan yang akan diteliti (Abduh et al., 2018). Terdapat dua jenis aplikasi delphi method yakni untuk *forecasting* dan identifikasi masalah, serta untuk menguji konsep/pengembangan framework (Okoli & Pawlowski, 2004)

Untuk survey mengenai pengembangan framework akan menggunakan instrument penelitian yang dikembangkan oleh Bacon (Bacon & Fitzgerald, 2001) yang terdiri dari 6 pertanyaan dengan tiga indikator jawaban seperti pada Tabel 3.3.

Tabel 3.3. Instrumen kuisisioner

No	Pertanyaan	Jawaban		
		Ya	Tidak	Mungkin
1	Apakah framework yang dikembangkan dibutuhkan di lapangan?			
2	Apakah farmework yang dikembangkan layak digunakan untuk dilapangan?			
3	Apakah informasi yang disajikan adalah tema yang cocok pada bidang tersebut?			
No	Pertanyaan	Jawaban		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pengelompokan area utama pada framework dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?			
5	Apakah perbedaan karakter pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			
6	Apakah perbedaan kompetensi pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			

Untuk survey dari para ahli mengenai perkembangan cyber fraud framework akan ada sedikit modifikasi instrument seperti yang ditunjukkan pada Tabel 3.4. Modifikasi ini dilakukan dikarenakan ada beberapa poin yang tidak sesuai seperti variabel area utama,

karakter, maupun kompetensi dirubah menjadi konsep/tahapan disesuaikan dengan tujuan dari penelitian ini.

Tabel 3.4 Modifikasi Instrumen kuisioner

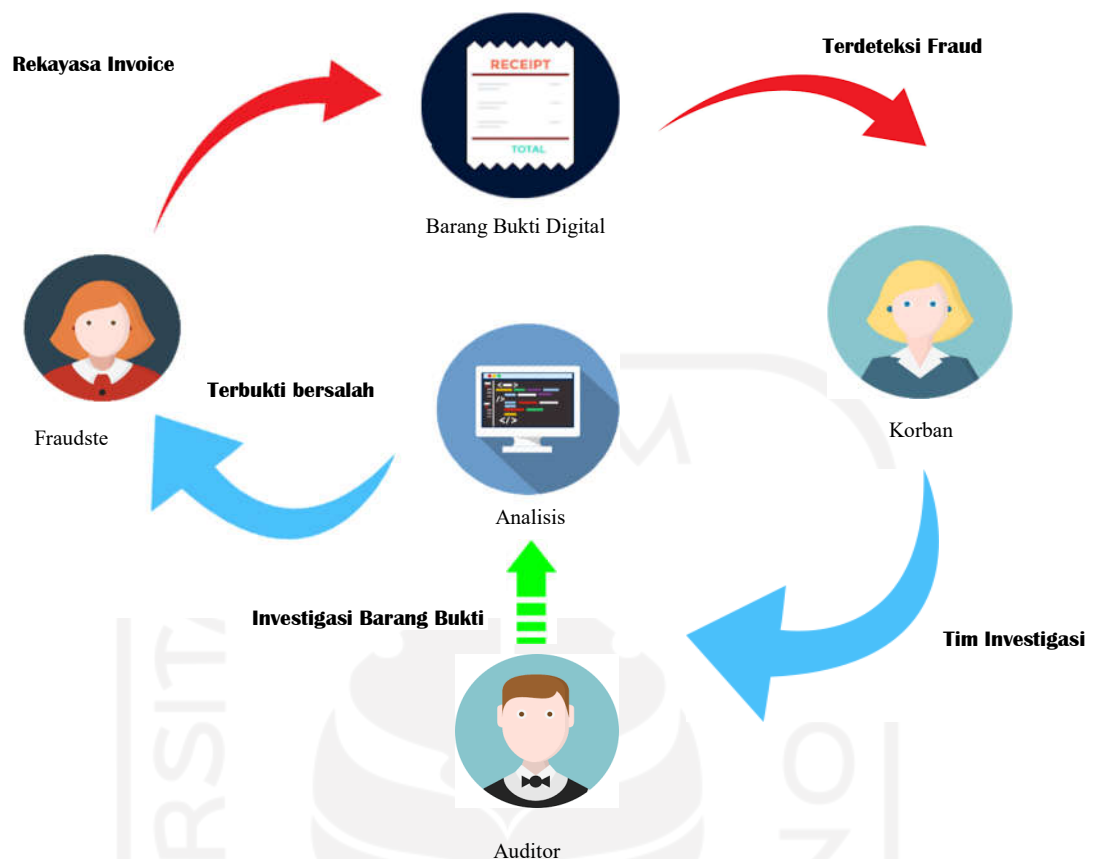
No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Tidak	Mungkin
1	Apakah framework yang dikembangkan dibutuhkan di lapangan?			
2	Apakah framework yang dikembangkan layak digunakan untuk dilapangan?			
3	Apakah konsep/tahapan yang disajikan cocok pada bidang <i>Cyber Fraud</i> ?			
No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pemberian konsep/tahapan pada framework dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?			
5	Apakah perbedaan konsep/tahapan pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			

3.10 Simulasi Kasus

Untuk memudahkan dalam menganalisis penggunaan *cyber fraud* framework, maka digunakan simulasi kasus penggelapan uang pengadaan barang dengan metode rekayasa laporan keuangan dimana barang bukti berupa digital *receipt* yang direkayasa nominalnya oleh pelaku dan barang bukti digital yang asli tersebut dihapus dari device pelaku sehingga penyidik atau auditor tidak dapat menemukan bukti tersebut.

Skema simulasi kasus dapat dilihat pada gambar 3.3 dimana pelaku melakukan rekayasa laporan keuangan dengan memodifikasi file *digital invoice* yang dikirim oleh perusahaan penyedia software dan menyerahkan ke departemen keuangan agar transaksi dapat diproses. Departemen keuangan selanjutnya mentransfer sejumlah uang kepada pelaku sesuai jumlah yang ada pada invoice yang diberikan oleh pelaku.

Kejanggalan dimulai saat ditemukan invoice *hardcopy* yang dikirimkan oleh perusahaan penyedia software yang berada di luar negeri kepada instansi dimana pelaku bekerja, sehingga hal ini membuat stakeholder merasakan adanya kejanggalan dan memutuskan untuk membentuk tim auditor untuk menginvestigasi kecurangan yang dilakukan oleh pelaku.



Gambar 3.3 Simulasi Kasus Cyber Fraud

Tim auditor selanjutnya melakukan pemeriksaan dengan file *invoice* digital yang telah direkayasa pelaku. Tim auditor menggunakan teknik digital forensik untuk mendapatkan bukti apakah terjadi manipulasi yang dilakukan oleh pegawai perusahaan tersebut.

Penggunaan tools digital forensik dapat membantu menemukan bukti bahwa terjadinya manipulasi data pada *invoice* digital yang merugikan perusahaan secara material dalam jumlah yang besar. Tim akhirnya melaporkan hasil investigasi kepada instansi yang berkaitan.

BAB 4

Hasil dan Pembahasan

4.1 *Mapping Selected Data*

Pada bab ini akan dibahas mengenai tahapan pengembangan framework *cyber fraud* dengan menggunakan metode Jabareen yang terdiri dari enam fase. Tahapan pertama yakni *Mapping Selected Data*, data yang akan diambil disini adalah data yang berasal dari buku dan jurnal penelitian. Data yang diambil dari dua disiplin ilmu yakni Audit Fraud dan Digital Forensik, terutama mengenai framework maupun tahapan dalam proses investigasi. Untuk pencarian data menggunakan bantuan *search engine* untuk membantu pemetaan data, dimana jurnal yang diambil berasal dari ScienceDirect, Emerald, ResearchGate, SagePublishing.

Data tersebut diupload dalam Mendeley agar lebih mudah untuk penyimpanan dan pemetaan data dengan rincian yakni dari 128 data diklasifikasikan dengan 53 data mengenai Digital Forensik, 31 data mengenai Audit Forensik sedangkan 44 data lainnya mengenai metode pengembangan framework. Kata kunci untuk pencarian data ini berupa text seperti ditunjukkan pada table 4.1

Tabel 4.1 Kata kunci pencarian data

No	Kata Kunci
1	<i>Digital Forensic Framework</i>
2	<i>Proposed Framework for Digital Forensic</i>
3	<i>Audit Fraud</i>
4	<i>Accounting Forensic</i>
5	<i>Audit Investigation Framework</i>
6	<i>Building Conceptual Framework</i>
7	Framework Digital Forensik
8	Investigasi Audit Fraud

4.2 *Extensive reading and categorizing of the selected data*

Tahapan kedua yakni *Extensive reading and categorizing of the selected data*, padatahapan ini dilakukan pendalaman materi pada berbagai data kemudian melakukan kategorisasi data-data tersebut sesuai dengan disiplin ilmu yang ada. Di tahapan ini data akan dikategorikan sesuai bidang ilmu yang telah ada yakni Audit Fraud dan Digital Forensik sesuai yang digambarkan pada Tabel 4.2.

Tabel 4.2 Kategorisasi data

No	Tema	Jumlah Data	Jumlah Data yang direduksi
1	Digital Forensik	53	22
2	Audit Fraud	31	8
3	Pengembangan Framework	44	

Tabel 4.2 menunjukkan jumlah data yang dikategorikan berdasarkan tahapan pertama yang berisi 128 data. Data dikategorisasikan menjadi 3 topik yakni digital forensik sejumlah 53 data, audit fraud sebanyak 31 data dan pengembangan framework sebanyak 44 data. Data yang telah dikategorisasikan akan direduksi sesuai dengan topik penelitian ini.

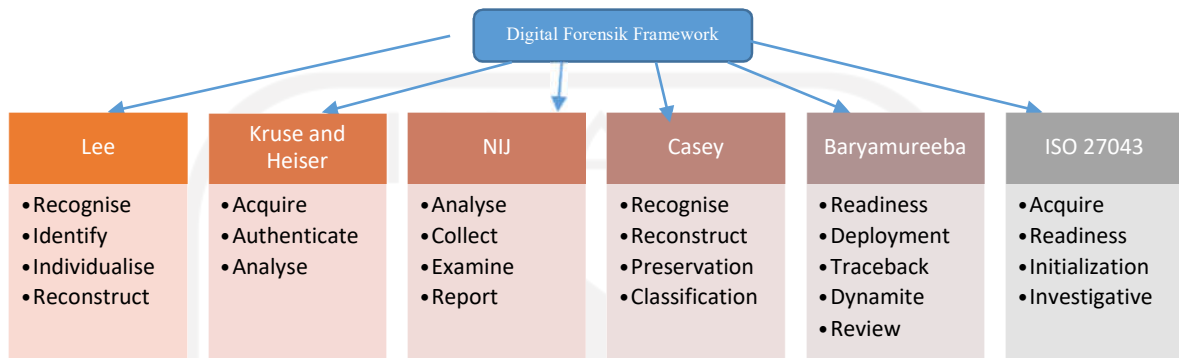
4.3 Identifying and naming concept

Pada tahapan ini data yang terekstraksi sebelumnya akan diurai menjadi konsep konsep yang berkaitan dengan bidang ilmu yang akan diteliti. Antara beberapa data akan memungkinkan konsep yang sama, dan nantinya akan terlihat kesamaan konsep dari beberapa data yang ada. Data yang akan diurai menjadi konsep merupakan framework digital forensik serta tahapan fraud audit. Framework digital forensik yang digunakan pada penelitian ini terdapat 22 referensi seperti yang ditunjukkan pada Gambar 4.1.



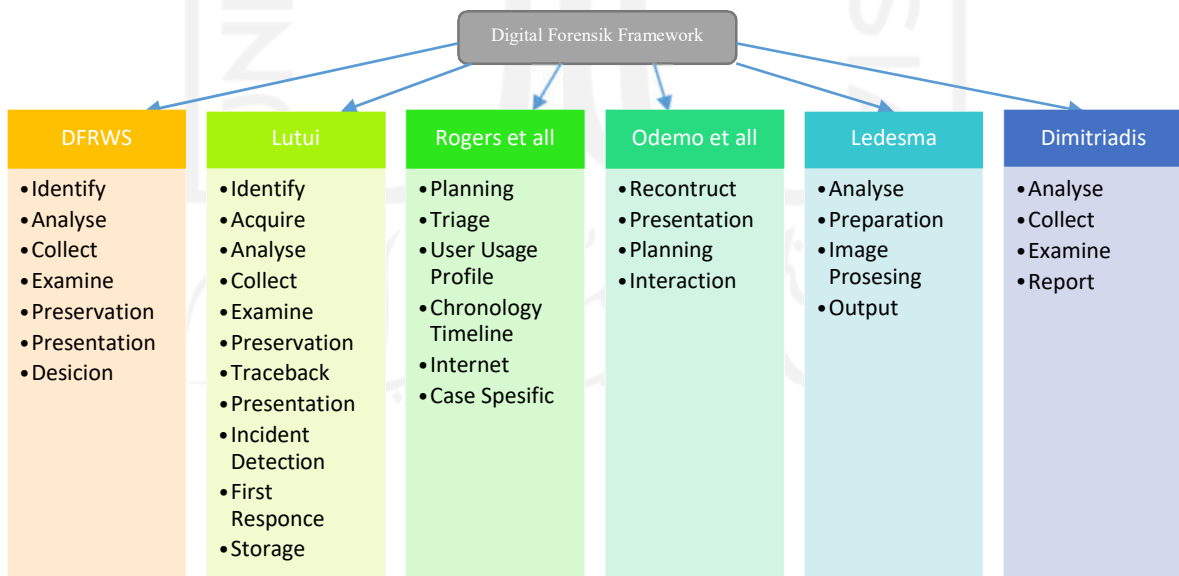
Gambar 4.1 Framework Digital Forensik yang digunakan

Gambar 4.1 menggambarkan 22 framework digital forensik yang akan digunakan sebagai acuan pada penelitian ini. Framework digital forensik yang diambil merupakan framework dari hasil penelitian, maupun yang dibangun oleh standar mutu/organisasi digital forensik. Framework yang dipilih terdiri dari beberapa framework digital forensik secara umum tetapi ada beberapa framework yang diambil untuk kasus device tertentu seperti perangkat IoT, Android, Cloud Services.



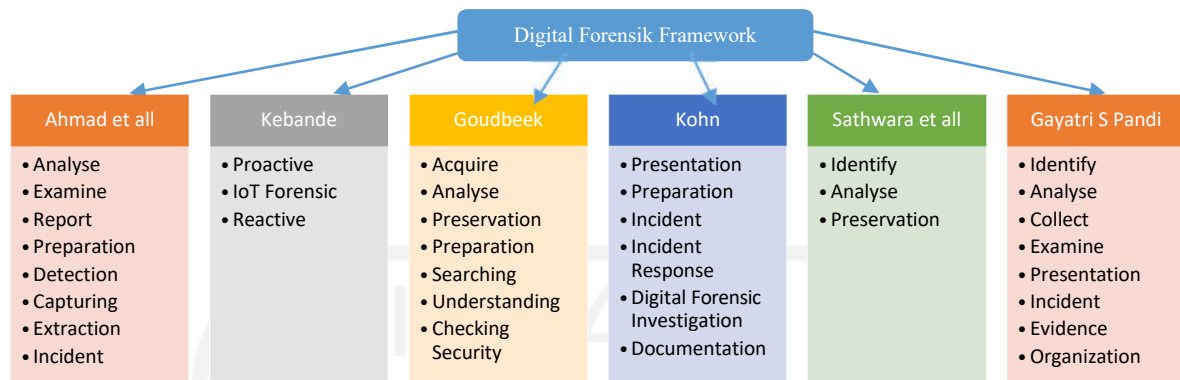
Gambar 4.2 Konsep digital forensic Lee – ISO 27043

Gambar 4.2 menjelaskan secara detail dari framework digital yang telah digambarkan pada Gambar 4.1. ISO 27043 merupakan salah satu framework investigasi digital forensik yang dikembangkan oleh standar mutu, terdapat juga framework yang dibentuk oleh Badan Institusi seperti NIJ.



Gambar 4.3 Konsep digital forensic DFRWS-Dimitriadis

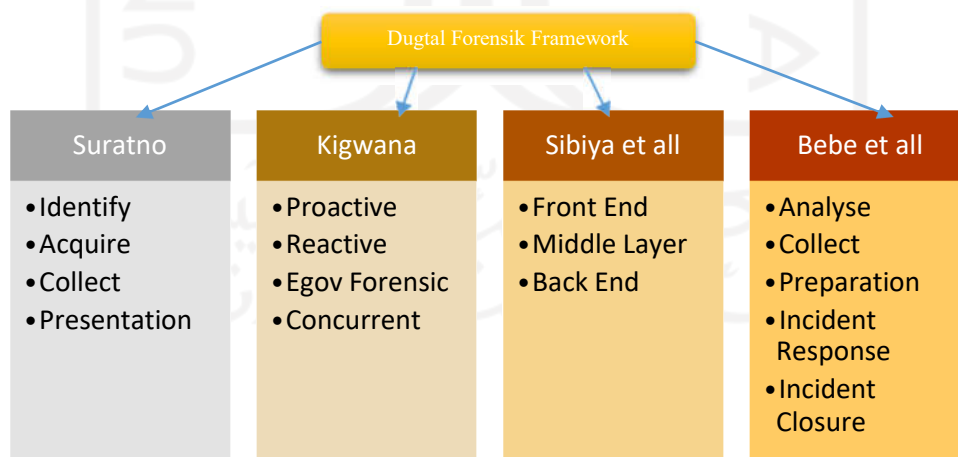
Tujuh framework digital forensic dijabarkan secara detail pada gambar 4.3 dimana terdapat framework digital forensic yang secara khusus digunakan untuk kejahatan yang menggunakan media image, serta ada framework yang dikembangkan oleh DFRWS.



Gambar 4.4 Konsep digital forensic Ahmad-Gayatri

Gambar 4.4 menjabarkan 6 framework digital forensic, beberapa diantara framework tersebut terdapat framework yang digunakan untuk perangkat IoT seperti yang dikembangkan oleh Kebande dimana dalam penelitiannya menyebutkan terdapat tiga tahap yang digunakan untuk proses investigasi IoT forensic yakni tahapan Proactive, IoT Forensic dan Reactive.

Empat framework digital forensic yang tersisa dijabarkan pada gambar 4.5 dimana terdapat beberapa jenis framework digital yang dikembangkan untuk perangkat/system tertentu yakni seperti untuk investigasi di *Cloud Services* dan investigasi forensic dalam *E-Government*.



Gambar 4.5 Konsep digital forensic Suratno-Bebe

Acuan framework yang digunakan pada penelitian ini selanjutnya akan diambil setiap detail tahapan yang kemudian akan dilakukan pendataan dari 22 framework. Setiap

detail tahapan yang memiliki nama yang sama hanya akan ditulis satu saja, sehingga pada identifikasi konsep didapatkan 55 konsep digital forensik.

Tabel 4.3 Konsep Audit Forensik

Concept / Author	Manning	Singleton	Pedneaul	Oyedokun	Chipper	Rozali et all	Saxunova	ICSI India
Recognition and Planning	√	√	√		√		√	√
Collection	√	√					√	
Evaluation	√							
Communication of Result	√							
Predication		√	√			√		
Approach		√						
Report		√	√		√	√		√
Investigative Identifying			√	√				
Computer Assisted Reviews and Document Review				√				
Data Mining				√				
Benford Law				√				
Ratio Analysis				√				
Data Matching				√				
Testing					√	√		
Hipotesis						√		
Data Gathering						√		√
Analysis						√		
Interview						√		
Loss Count						√		
Detecting and analysing potential crime							√	
Interviewing							√	
Finding summarized							√	
Accepting investigation								√
Court proceeding								√

Untuk kategori Audit fraud menggunakan 8 referensi sebagaimana dituliskan pada tabel 4.3 . Pada keenam referensi tersebut dilakukan pendataan dan didapatkan 20 jenis konsep yang berbeda.

4.4 *Deconstructing and categorizing the concepts*

Pada tahap ini akan dilakukan dekonstruksi-konstruksi pada konsep yang telah ada. Dikarenakan ada banyaknya konsep yang memiliki maksud yang sama maka akan dilakukan konstruksi ulang pada konsep tersebut dan selanjutnya mengkategorisasikan sesuai role yang ada. Berikut ini akan diidentifikasi konsep konsep yang sama dan kemudian disederhanakan menjadi satu konsep saja sehingga akan mengurangi redudansi konsep .

Tabel 4.4 Ringkasan konsep data Digital Forensik

No	Nama Konsep	No	Nama Konsep
1	Recognise	31	Interaction
2	Identify	32	Preparation
3	Individualise	33	Image Prosesing
4	Reconstruct	34	Output
5	Acquire	35	Detection
6	Authenticate	36	Capturing
7	Analyse	37	Extraction
8	Collect	38	Proactive
9	Examine	39	IoT Forensic
10	Report	40	Reactive
11	Preservation	41	Searching
12	Classification	42	Understanding
13	Readiness	43	Checking Security Level
14	Deployment	44	Incident
15	Traceback	45	Incident Response
16	Dynamite	46	Digital Forensic Investigation
17	Review	47	Documentation
18	Initialization	48	Evidence
19	Investigative	49	Organization
20	Presentation	50	Egov Forensic
21	Decision	51	Concurrent
22	Incident Detection	52	Front End
23	First Response	53	Middle Layer
24	Storage	54	Back End
25	Planning	55	Incident Closure
26	Triage		
27	User Usage Profile		
28	Chronology Timeline		
29	Internet		
30	Case Spesific		

Identifikasi konsep untuk digital forensik dapat dilihat pada tabel 4.4, pada konsep Framework Investigasi Digital Forensik ditemukan 55 konsep dan disederhanakan menjadi 8 konsep. Konsep yang memiliki makna dan tujuan yang sama dikelompokkan dan disederhanakan menjadi satu konsep sehingga tidak terjadi redudansi konsep

Konsep yang memiliki nama yang sama, atau masih saling berkaitan akan direduksi menjadi satu konsep yang sama. Sedangkan konsep yang tidak memiliki perulangan kata atau makna akan berdiri sendiri. Dari metode yang digunakan tersebut didapatkan konsep untuk digital forensik dan fraud audit dibawah ini.

1. **Readiness**

“Readiness=incident detection=detection=proactive=checking security level=front end=organization”

Konsep Readiness merupakan konsep proaktif untuk menjaga agar tidak terjadi tindak kejahatan pada suatu instansi maupun perusahaan dimana dalam proses ini dapat dibuat suatu peraturan maupun system deteksi pada tindak kejahatan siber.

2. **Incident Response**

“Incident Response =Triage”

Konsep Incident Response ini merupakan tahapan yang penting untuk dilakukan untuk menyelamatkan barang bukti digital pada beberapa kasus tertentu yang memerlukan tindakan secara cepat.

3. **Identification**

“Identify=Recognise=Initialization=First

Response=Planning=Preparation=Review=Case

Spesific=Understanding=Individualise=Reconstruct=Traceback=Incident”

Konsep pertama yakni merupakan tahap identifikasi , pengenalan, persiapan maupun perencanaan dalam investigasi digital forensik. Tahapan ini akan dilaksanakan setelah kejahatan berlangsung dan perlu dilakukan identifikasi dan perencanaan untuk proses investigasi selanjutnya.

4. Collection

“Acquire=Authenticate=Collect=Classification=Deployment=Capturing=Searching=Evidence=Storage=Extraction=Interaction”

Konsep selanjutnya ialah akuisisi dimana merupakan tahapan penting untuk mendapatkan barang bukti digital pada proses investigasi. Proses akuisisi yakni mengumpulkan barang bukti digital yang ada dan membuat “working copy” untuk dianalisis serta dalam tahapan ini perlu dilakukan proses otentikasi agar terjaga keaslian data sehingga dapat dipertanggungjawabkan dipersidangan atau level teratas.

5. Analyse

“Analyse=Examine=Dynamite=Investigative=User Usage Profile=Internet=Chronology Image Prosesing=reactive=IoT Forensic=Digital Forensic Investigation=Back End=Middle Layer=Egov Forensic”

Konsep selanjutnya merupakan analisis, yang dilakukan untuk mengetahui apakah berdasarkan barang bukti yang ada memang telah terjadi tindak kejahatan atau tidak. Konsep analisis ini akan sangat luas dan bergantung pada subjek yang akan dianalisis.

6. Report

“Report =Presentation=Decision=Output”

Konsep selanjutnya adalah pelaporan pada pihak yang berwenang yang selanjutnya dapat diambil keputusan mengenai hasil investigasi .

7. Concurrent

“Preserve=Documentation=Concurrent”

Konsep preserve ini dilakukan untuk menjaga keaslian barang bukti digital dari awal hingga akhir, yang dapat dilakukan dengan dokumentasi maupun proses iterasi untuk menjaga segala proses berjalan sesuai standar dan prosedurnya.

8. Incident Closure

“Incident Closure”

Merupakan konsep untuk melakukan penutupan suatu kasus investigasi tindak kejahatan dan pemusnahan maupun pengembalian barang bukti digital yang telah disita oleh pihak investigator.

Identifikasi konsep untuk audit fraud dapat dilihat pada tabel 4.5 yang terdiri dari 20

konsep dan disederhanakan menjadi 5 konsep. Konsep yang memiliki makna dan tujuan yang sama dikelompokkan dan disederhanakan menjadi satu konsep sehingga tidak terjadi reduksi konsep

Tabel 4.5 Tabel Konsep Audit Forensik

No	Nama Konsep	No	Nama Konsep
1	Recognition and Planning	14	Data Matching
2	Collection	15	Testing
3	Evaluation	16	Hipotesis
4	Communication of Result	17	Data Gathering
5	Predication	18	Analysis
6	Approach	19	Interview
7	Report	20	Loss Count
8	Investigative	21	Detecting and analysing potential crime
9	Identifying	22	Interviewing
10	Computer Assisted Reviews and Document Review	23	Finding summarized
11	Data Mining	24	Accepting investigation
12	Benford Law	25	Court proceeding
13	Ratio Analysis		

1. **Detection**

“Detection=Data Mining=Benford Law=Ratio Analysis=Data Matching=Detecting Plan”

Konsep ini berisi mengenai metode deteksi untuk kejahatan fraud yang dapat dilakukan suatu instansi atau perusahaan untuk mencegah terjadinya fraud yang dapat merugikan instansi maupun perusahaan baik secara materiil maupun non materiil.

2. **Planning**

“Planning=Identification=Predication=Hypothesis=Approach”

Konsep Audit pertama yakni planning yang merupakan konsep yang sama dengan Identification dan Predication dimana semua mengandung makna untuk melakukan identifikasi, perencanaan dan melakukan hipotesis atas kasus fraud yang terjadi.

3. **Collection**

“Collection =Data Gathering”

Konsep selanjutnya yakni pengumpulan barang bukti untuk kasus fraud yang terjadi. Barang bukti untuk kasus fraud dapat berupa dokumen fisik, maupun digital.

4. **Investigation**

“Investigation=Evaluation=Computer Assisterd Reviews and Document

Reviews=Testing=Analysis and Interview=Loss Count=Interviewing”

Konsep investigasi merupakan konsep secara umum yang mencakup semua proses pelaksanaan investigasi fraud baik menggunakan metode interview, analisis dokumen maupun bukti digital.

5. **Report**

“Report=Communication of Result=Finding Summarized=Accepting Investigation=Court Proceeding”

Konsep selanjutnya yakni pelaporan akan hasil investigasi kepada pihak yang berwenang berdasarkan barang bukti dan wawancara yang mendukung, sehingga dapat dibuktikan terjadinya kejahatan fraud dan metodenya.

Untuk dapat memetakan lebih lengkap dapat dilihat pada tabel 4.6 mengenai konsep yang ada pada digital forensik dan audit fraud serta sifat yang ada pada tiap konsep tersebut. Role Ontological merupakan fungsi dimana suatu konsep yang sudah ada, sedang Role Epistemological merupakan bagaimana konsep tersebut seharusnya ada, sedangkan role methodological merupakan bagaimana konsep itu bisa berjalan dengan baik.

Tabel 4.6 Ringkasan sifat konsep

Konsep	Disiplin Ilmu	Sifat Konsep
Detection	Audit Fraud	Ontological
Planning		Ontological
Collection		Ontological
Investigation		Ontological
Report		Ontological
Readiness	Digital Forensik	Epistemological
Identification		Ontological
Collection		Ontological
Analyse		Ontological
Report		Ontological
Concurrent		Methodological
Incident Closure		Ontological
Incident Response		Ontological

4.5 *Integrating concepts*

Tahapan selanjutnya yakni integrasi konsep antara digital forensik dan audit fraud yang pada konsep sebelumnya telah dilakukan penyederhaanaan konsep konsep yang memiliki makna yang hampir sama ataupun dalam lingkup yang sama. Untuk melakukan integrasi konsep dilakukan dengan menghilangkan konsep yang sama, serta memilih konsep yang sesuai dengan kedua bidang tersebut. Untuk mempermudah melakukan integrasi dapat dibuat sebuah tabel untuk melihat konsep yang sama seperti pada tabel 4.7 yang dapat dilihat

adanya beberapa konsep yang sama pada dua bidang tersebut.

Tabel 4.7 Integrasi konsep

Digital Forensik	Audit Fraud	Integrasi Konsep
Readiness	Detection	Readiness
Identification	Planning	Planning
Collection	Collection	Collection
Analyse	Investigation	Analysis
Report	Report	Report
Concurrent		Concurrent
Incident Closure		Incident Closure
Incident Response		Incident Response

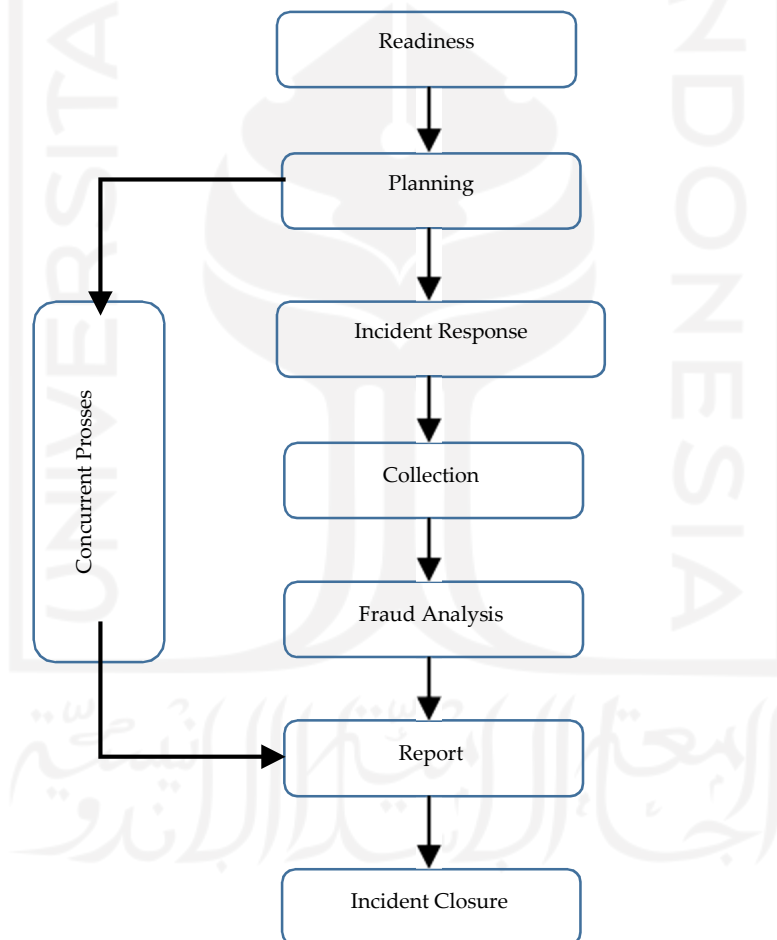
Konsep atau tahapan yang dihasilkan pada integrasi konsep ini akan digunakan seluruhnya pada framework cyber fraud yang akan dikembangkan. Tahapan readiness digunakan sebagai bentuk pencegahan dan antisipasi kejahatan cyber fraud. Readiness dapat mengurangi kerugian instansi apabila deteksi cyber fraud berjalan dengan baik dan prosedur penanganan kasus terbentuk dengan baik. Planning merupakan tahapan penting pada sebuah investigasi kejahatan dimana penyusunan rencana kerja dapat membuat investigasi berjalan dengan efektif dan efisien. Kasus cyber fraud memerlukan perencanaan yang cepat dan tepat sehingga mendapatkan barang bukti digital yang menjadi benda krusial pada investigasi ini. Tahapan pengumpulan barang bukti atau Collection akan tetap digunakan karena tahapan ini juga sangat penting untuk dilakukan, dikarenakan barang bukti digital sangat rawan untuk hilang ataupun rusak maka perlu tenaga ahli yang secara khusus untuk melakukan pengumpulan barang bukti digital. Tahapan Analysis diperlukan pada proses investigasi dikarenakan pada proses ini akan menjadi kunci bagi stakeholder maupun pihak pengadilan dalam mengambil keputusan. Analysis dapat mengungkapkan apakah benar terjadi kejahatan, proses berlangsungnya kejahatan dan pelaku yang melakukan kejahatan ini. Pengambilan keputusan dilakukan setelah tahapan Report dilaksanakan, dimana proses ini merupakan proses pelaporan kasus investigasi kejahatan cyber fraud pada pihak instansi maupun pihak peradilan.

Setelah konsep yang sama diekstraksi, maka framework untuk cyber fraud telah terbentuk dengan adanya penambahan konsep *Incident Response*, *Incident Closure* serta *Concurrent*. Alasan penambahan konsep *Incident Response* dikarenakan banyaknya kasus Cyber Fraud yang membutuhkan proses penanganan pertama agar barang bukti yang dibutuhkan dapat diperoleh sebelum hilang dikarenakan sifat barang bukti digital yang *Volatile*. Penambahan konsep *Concurrent* digunakan untuk menjaga proses investigasi cyber fraud selalu dalam tahap yang sesuai prosedur, apabila ada proses yang terlewat dapat diulangi dari awal sehingga barang bukti digital dapat diperoleh secara baik untuk mempermudah proses investigasi. Konsep *Incident Closure* ditambahkan untuk memperjelas

status investigasi yang telah dilaksanakan.

4.6 Synthesis, Resynthesis and making it all make sense

Tahapan ini merupakan tahapan penyusunan framework cyber fraud berdasarkan integrasi konsep yang telah disebutkan sebelumnya. Dari table 4.7 konsep yang sama dijadikan satu dan ditambahkan konsep lain yang belum tercakup. *Cyber Fraud Framework* yang merupakan hasil kolaborasi hal-hal yang pokok dalam Investigasi Digital Forensik dan Audit Fraud sehingga didapatkan framework seperti Gambar 4.6 yang terdiri dari 8 tahapan dengan 1 proses aktif yang digunakan untuk memastikan barang bukti digital yang didapatkan memang sesuai untuk membuktikan suatu kasus *cyber fraud*.



Gambar 4.6 Framework cyber fraud yang diajukan

Konsep dalam framework tersebut akan dijabarkan lebih lanjut dibawah ini :

1. **Readiness** : Merupakan usaha proaktif yang dilakukan suatu institusi untuk mempersiapkan diri dalam menghadapi kecurangan/fraud yang dilakukan baik secara offline maupun online. Suatu institusi yang memiliki system ini akan mendapatkan trust yang lebih baik dari pelanggan dikarenakan telah memiliki prosedur mitigasi yang dapat memperkecil kerugian yang akan dialami kedepannya. Tahapan ini dinilai sangat penting, dikarenakan banyak laporan kasus fraud tidak dapat tertangani dengan baik dikarenakan kurangnya kesiapan instansi dalam menghadapi kasus fraud.

- Mempersiapkan *fraud detection system* yang sesuai dengan perusahaan

Berbagai macam jenis fraud detection system telah dikembangkan dengan algoritma yang dinilai ampuh untuk mencegah terjadinya fraud yang menimbulkan kerugian yang besar pada perusahaan.

- Mempersiapkan *Cyber Security Incident Management Framework*

Suatu institusi sebaiknya memulai membangun suatu system untuk menanggulangi adanya kejahatan cyber dilingkungannya. Salah satunya dengan membangun *Cyber Security Incident Management Framework* untuk mengurangi biaya kerugian baik materiil maupun non materiil saat terjadi tindak kejahatan.

- Melatih tenaga dalam menghadapi kasus *cyber fraud*

Institusi juga harus memberikan training kepada pegawainya mengenai menanggulangi fraud yang terjadi secara cyber, baik dalam training menggunakan system maupun dalam berkomunikasi dikarenakan salah satu metode cyber crime yang banyak dipakai adalah menggunakan social engineering yang memanfaatkan kelemahan dari sisi manusia.

2. **Planning** : Tahapan ini merupakan tahap pertama yang dilakukan setelah kasus cyber fraud terjadi. Investigator harus melakukan perencanaan mengenai beberapa hal sebelum terjun ke lapangan, hal ini dilakukan untuk menjaga proses investigasi berjalan secara efektif dan efisien. Beberapa hal yang dilakukan yakni :

- Memiliki hipotesis bagaimana fraud itu terjadi

Sebelum melakukan investigasi dilapangan, tim sebaiknya memiliki hipotesis mengenai kejadian cyber fraud ini, perkiraan waktu terjadi

- Memformulasikan jangkauan investigasi

Sebagai bentuk efisiensi tenaga dan waktu, perlu difokuskan jangkauan investigasi dan berkas-berkas apa yang diperlukan untuk mendukung proses investigasi seperti surat izin pengeledahan, maupun surat izin yang lainnya.

- Mendaftar temuan apa saja yang akan dicari

Tim merumuskan potensi barang bukti digital yang dapat membantu proses investigasi

- Mempersiapkan dokumen administrasi

Dokumen pengeledahan, ataupun dokumen lainnya harus dilengkapi serta alat-alat yang dibutuhkan untuk melakukan investigasi.

- Mengumpulkan data-data yang berkaitan dengan kasus cyber fraud

Melakukan tracing apakah pernah ada kasus yang serupa terjadi dapat membantu mempercepat proses investigasi

3. ***Incident Response*** : Tahapan ini dilakukan pada barang bukti digital yang ada pada TKP, investigator sebaiknya segera melakukan pengamanan pertama kepada barang bukti digital karena pada kejahatan cyber fraud data-data yang dibutuhkan sangat memungkinkan bersifat volatile baik pada perangkat laptop, PC, smartphone, maupun pada perangkat lain sehingga tahapan ini sangat penting agar investigator tidak kehilangan barang bukti yang dapat menjadi titik terang dari suatu kasus cyber fraud. Beberapa sub-fase yang dapat dilakukan adalah :

- Melakukan *live acquisition* pada *volatile data*

Dikarenakan tindak kejahatan cyber fraud yang menggunakan perangkat elektronik maka perlu dilakukan live acquisition pada volatile data sehingga data akan aman

- Melakukan pengamanan/*seizure* pada perangkat yang dinilai rawan

Pengamanan barang bukti dilakukan agar barang bukti digital ini dapat dibawa ke laboratorium dan dapat diperiksa oleh petugas forensic. Pengamanan dilakukan sesuai prosedur yang ada.

- Memberikan label pada setiap barang bukti yang sudah diamankan

Tahapan dalam pengamanan selanjutnya yakni memberikan label dan mengemasnya sehingga barang bukti tersebut aman

- Menyimpan barang bukti sesuai SOP sehingga sampai pada laboratorium forensic

Barang bukti yang sudah diamankan selanjutnya disimpan untuk proses selanjutnya. Penyimpanan barang bukti harus sesuai dengan prosedur.

4. **Collection:** Merupakan tahapan pengumpulan barang bukti digital yang berkaitan dengan kasus cyber fraud. Pengumpulan barang bukti ini harus sesuai dengan SOP yang ada pada masing-masing instansi atau kepolisian.

- Memilih barang bukti yang relevan dengan kasus yang diinvestigasi

Barang bukti digital yang telah diamankan pada proses selanjutnya kemudian dilakukan identifikasi apakah barang bukti tersebut relevan dengan kasus yang sedang dihadapi.

- *Confriming*

Barang bukti elektronik yang sudah diamankan juga harus dilakukan konfirmasi apakah sesuai dengan kasus yang diidentifikasi dengan melakukan wawancara kepada saksi maupun terduga

- Melakukan akuisisi dan autentikasi pada hasil akuisisi

Barang bukti selanjutnya diakuisisi untuk proses analisis, akuisisi dilakukan dengan tools yang terpercaya dan selanjutnya dilakukan autentikasi dengan melakukan hashing untuk menjamin integritas barang bukti.

5. **Fraud Analysis :** Merupakan tahapan dimana data dari barang bukti digital diekstrak dan dianalisis menggunakan software/hardware yang memadai. Dalam proses analisis ini harus dilakukan oleh tenaga yang sudah terlatih dan melengkapi dokumen yang ada agar semua proses investigasi lebih *reliable*.

- Melakukan analisis dari barang bukti digital dengan menggunakan software/hardware forensic yang telah terjamin

Tahapan ini yakni memproses dan menganalisa dari hasil akuisisi barang bukti, analisis dilakukan oleh ahli forensic atau tenaga professional lainnya. Proses ini dilakukan sesuai dengan tujuan investigasi untuk mencari barang bukti yang berkaitan dengan *cyber fraud*. Pada tahapan ini akan diketahui apakah benar terjadi kecurangan atau fraud yang dilakukan, dikarenakan pada kasus fraud dengan media digital akan melakukan manipulasi pada data keuangan.

6. **Report :** Tahapan akhir ini disajikan dan dilakukan oleh investigator kepada unit terkait semisal lembaga peradilan, maupun instansi yang menggunakan jasa untuk melakukan investigasi pada kasus cyber fraud.

- Membuat report dari hasil investigasi

Setelah menyelesaikan proses investigasi dan analisis, petugas membuat laporan yang berisi hasil investigasi cyber fraud sesuai dengan prosedur pelaporan yang ada pada masing masing instansi

- Menyampaikan hasil report kepada pihak yang berwenang

Hal terakhir yang dilakukan yakni menyampaikan hasil presentasi ini kepada pihak yang berwenang, dapat berupa pengadilan maupun instansi yang mengalami kerugian karena cyber fraud

7. ***Incident Closure*** : Tahapan ini adalah penutupan dari kasus cyber fraud ini, barang bukti yang ada dapat disimpan sebagai arsip ataupun dapat dilakukan retensi data sesuai dengan kebijakan masing-masing institusi.

8. ***Concurrent*** : Tahap ini merupakan tahapan metodological untuk memastikan bahwa setiap proses berjalan dengan baik, sehingga apabila ada yang dinilai masih kurang sesuai dapat diulangi dari tahapan awal.

4.7 Evaluasi Framework

Evaluasi Framework ini dilakukan dengan memberikan kuesioner/survey dengan Delphi method kepada para praktisi Audit Fraud dan Digital Forensik. Dalam kuesioner ini terdapat 5 pertanyaan yang berkaitan dengan pengembangan framework yang terdiri dari dua bagian dimana 3 pertanyaan pertama berfokus pada perlunya pengembangan framework cyber fraud sedangkan 2 pertanyaan yang lain berfokus pada detail tahapan dari framework yang dikembangkan.

Evaluasi framework menggunakan Delphi method ini digunakan dengan pilot testing yakni dilakukan satu kali saja, sedangkan pada umumnya Delphi method dilaksanakan hingga beberapa putaran sehingga konsensus tercapai. Metode pilot testing ini digunakan untuk menguji survey untuk evaluasi framework, sehingga untuk kedepannya perlu dilakukan survey dengan peserta yang lebih banyak lagi dan dilakukan hingga beberapa putaran sehingga terjadi kesepakatan.

Untuk evaluasi framework *cyber fraud* ini dibantu oleh dua praktisi dari Audit Fraud dan Digital Forensik yakni dari Kementrian Keuangan dan dari PUSFID UII dan satu akademisi dari UII. Dari hasil kuesioner yang didapatkan dari praktisi pertama tidak

memberikan masukan akan pengembangan cyber fraud framework. Praktisi pertama menyatakan bahwa pengembangan cyber fraud ini dibutuhkan dan layak untuk digunakan serta cocok untuk dengan kondisi kejahatan fraud berbasis siber. Serta menyatakan bahwa penamaan konsep atau tahapan sudah sesuai tanpa ada perubahan minor atau mayor.

Hasil kuesioner yang diberikan oleh praktisi kedua lebih memberikan feedback bahwa pengembangan *cyber fraud* framework memang diperlukan tetapi untuk kelayakannya perlu dievaluasi lebih lanjut lagi dan pengembangan framework ini dinilai cocok untuk situasi *cyber fraud*. Ada beberapa perubahan minor yang perlu dilakukan mengenai konsep atau tahapan dalam framework ini agar lebih baik dan diterima.

Praktisi ketiga yang merupakan seorang akademisi menyatakan bahwa framework yang dikembangkan memang dibutuhkan dan layak dikembangkan, konsep yang disajikan dinilai cocok untuk cyber fraud dan pemberian konsep atau perbedaan konsep dapat diterima. Untuk ringkasan hasil kuesioner dari kedua praktisi dapat dilihat pada tabel 4.8

Tabel 4.8 Ringkasan Hasil Kuesioner

No	Pertanyaan	Praktisi 1	Praktisi 2	Akademisi 1
1	Apakah <i>framework</i> yang dikembangkan dibutuhkan di lapangan?	Ya	Ya, Karakteristik <i>cyberfraud</i> di setiap wilayah adalah unik, untuk studi kasus di Indonesia saya rasa perlu dikembangkan framework tersendiri	Ya
2	Apakah <i>framework</i> yang dikembangkan layak digunakan untuk di lapangan?	Ya	Mungkin, Harus dilakukan pengujian secara comprehensive terkait framework tersebut dengan studi kasus/skenario yang dibuat berdasarkan kejadian sebenarnya. Karena ranah fraud menurut saya tidak banyak bersentuhan ke aparat penegak hukum tp lebih ke pada lembaga audit baik government maupun swasta	Ya
3	Apakah konsep/tahapan yang disajikan cocok pada bidang <i>Cyber Fraud</i> ?	Ya	Ya, Sudah ada proses <i>mixing</i> disini untuk menggabungkan 2 buah framework. Perlu ada penjelasan detail bagaimana metode yang digunakan untuk menggabungkan/mensintesis framework ini sehingga framework yang dihasilkan bukan merupakan hasil asumsi dari peneliti	Ya
4	Apakah pemberian konsep/tahapan pada <i>framework</i> dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?	Ya	Perubahan Minor, Menurut saya perlu dilakukan analisis terkait karakteristik kasus fraud yang ada, misal pemanfaatan teknologi dan	Ya

			lain-lain untuk memastikan bahwa framework yang dihasilkan sudah mengakomodir berbagai teknologi tersebut. Misal analisis framework2 yang berhubungan dengan media social	
5	Apakah perbedaan konsep/tahapan pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?	Ya	Perubahan Minor, Sudah disebutkan diatas	Ya (Dalam perbedaan tahapan pada audit forensik, tahap awal adalah pra-planning, bukan detection.)

Dari tabel 4.8 diatas untuk kebutuhan pengembangan framework investigasi *cyber fraud* di lapangan dari ketiga responden menyatakan bahwa semua menyatakan framework ini dibutuhkan untuk dikembangkan namun untuk kelayakan framework perlu dilakukan evaluasi lagi yang merupakan pendapat dari satu praktisi. Penyajian konsep dalam framework yang dikembangkan dinyatakan cocok oleh ketiga responden. Perubahan konsep dalam framework ini dinyatakan tidak perlu oleh kedua responden, tetapi satu responden menyatakan masih membutuhkan evaluasi lagi agar disesuaikan dengan trend teknologi digital yang berkembang. Hasil evaluasi sementara menunjukkan tidak terjadinya konsensus dikarenakan belum terjadinya kesepakatan antar responden seperti pada poin kelayakan framework yang dikembangkan serta poin perlunya perubahan pada framework yang dikembangkan.

Hasil evaluasi dari praktisi diatas merupakan hasil pilot testing untuk Delphi method sehingga diperlukan evaluasi lagi dengan melibatkan lebih banyak peserta. Konsensus dari hasil evaluasi didapatkan setelah dilakukan beberapa kali siklus Delphi method dimana peserta dapat merubah jawaban setelah siklus dilakukan, dan moderator atau peneliti dapat menganalisis hasil dari Delphi method dengan metode kuantitatif. Feedback atau revisi yang diberikan pada responden akan diulang sehingga terjadi kesepakatan mengenai kelayakan dan perubahan pada framework yang dikembangkan, dikarenakan tujuan dari penggunaan Delphi Method adalah mencapai kesepakatan atau consensus terkait framework yang dikembangkan.

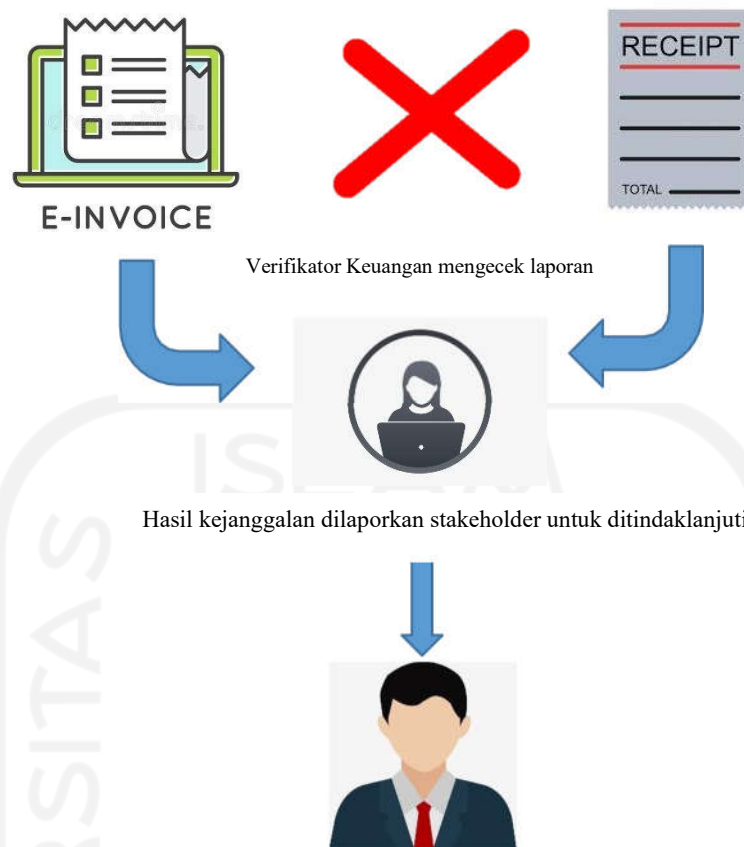
4.8 Simulasi Framework

Framework yang dikembangkan ini selanjutnya akan disimulasikan pada studi kasus *cyber fraud* yakni kasus penggelapan dana dengan mengubah data e-invoice yang berupa PDF pada suatu instansi. Skenario kasus penggelapan dana adalah seorang karyawan dari sebuah instansi pendidikan bernama Universitas Maritim Jaya melakukan sebuah pembelian software dari perusahaan luar negeri. Karyawan dengan inisial ANH ini melakukan komunikasi dengan sales marketing dari perusahaan tersebut dan membuat kesepakatan pembelian software. Prosedur pembelian software yang dilakukan secara online hanya membutuhkan *electronic invoice* yang diberikan kepada karyawan tersebut dan apabila pembayaran telah dilakukan, perusahaan software tersebut akan mengirimkan serial number untuk software tersebut.

Pada skenario kasus ini, karyawan tersebut mengedit dokumen invoice tersebut dan membuat besaran nilai invoice menjadi lebih tinggi, dikarenakan instansi dimana karyawan ini bekerja akan melakukan transfer uang tersebut di rekening karyawan tersebut dan selanjutnya karyawan tersebut yang akan melakukan pembayaran kepada perusahaan penyedia software. Kasus penggelapan dana ini diketahui instansi saat perusahaan penyedia software mengirimkan berkas dokumen asli secara offline dan menjadi temuan pada kasus pengadaan software di instansi tersebut. Kasus penggelapan dana ini disebut kasus cyber fraud dikarenakan tindakan penggelapan dana merupakan salah satu jenis kasus fraud yang menggunakan perangkat digital sebagai media untuk pelaksanaan kasus ini. Proses investigasi kasus ini akan menggunakan framework investigasi kasus cyber yang telah dikembangkan pada penelitian ini.

4.8.1 Readiness

Tahapan ini berisi mengenai bagaimana persiapan institusi Universitas Maritim Jaya dalam menghadapi kasus fraud. Prosedur di Universitas Maritim Jaya untuk menghindari fraud yakni melakukan audit pada laporan keuangan yang dirasa ganjil. Pada kasus ini auditor menemukan kejanggalan pada laporan keuangan pada unit dimana karyawan ANH bekerja, yakni data invoice yang dikumpulkan oleh karyawan dan invoice yang dikirimkan secara offline oleh perusahaan penyedia software ternyata berbeda jumlahnya. Tahapan Readiness pada instansi tersebut digambarkan pada bagan di bawah ini



Gambar 4.7 Tahapan Readiness yang dilakukan instansi UMJ

4.8.2 Planning

Tahapan planning digunakan oleh Stakeholder dengan pembentukan tim investigasi setelah mendapatkan laporan dari pihak verifikator keuangan bahwa ada kecurigaan fraud yang dilakukan. Tim dibentuk untuk mengaudit penggelapan dana sebesar \$2000 USD yang dilakukan oknum karyawan ANH di instansi dia bekerja . Tim berisi kepala auditor dan pembantu pelaksana auditor dari Badan Audit di Universitas Maritim Jaya. Kepala Auditor akan memberikan arahan kepada timnya untuk melakukan penyelidikan yang dimulai dari barang bukti laporan keuangan dan data invoice yang dikirim langsung oleh perusahaan software STATA di Australia. Tim ini sebelum terjun ke lapangan akan melakukan identifikasi kasus, membuat hipotesis dan merencanakan tahapan investigasi.

4.8.3 Incident Response

Incident response atau respon yang diberikan pada kasus pemalsuan data invoice ini dilakukan setelah tahap perencanaan. Tahap yang dilakukan pada incident response ini yakni menunjuk anggota tim yang kompatibel untuk melakukan rencana pengambilan barang bukti

digital, yakni dengan memperkirakan waktu kejadian kejahatan yakni pada Bulan Juli 2020 sesuai dengan tanggal pengajuan invoice ke departemen keuangan. Anggota tim yang ditunjuk selanjutnya mengamankan PC pelaku untuk selanjutnya akan diproses pada tahap pengambilan barang bukti digital. Tahapan ini juga digunakan untuk menentukan prioritas, bahwa mengamankan PC pelaku sangat penting sebelum pelaku melakukan penghapusan data. Tahapan ini tim selanjutnya mengamankan PC Asus All in One V222FAK-BA542T yang digunakan pelaku untuk melakukan manipulasi data.



Gambar 4.8 Barang Bukti PC Asus All in One

4.8.4 Collection

Tahapan Collection dilaksanakan dengan mendapatkan barang bukti digital berupa e-invoice yang ada di karyawan ANH setelah dilakukan investigasi oleh tim. Tim melacak bahwa laporan keuangan di divisi keuangan dan berkas invoice resmi dari STATA berbeda sehingga tim pun memanggil karyawan ANH untuk memberikan e-invoice yang berupa pdf yang digunakan ANH untuk membuat laporan keuangan dimana invoice tersebut masih disimpan sebagai bukti audit tahunan instansi. Invoice tersebut disimpan dengan nama InvoiceUMJ.pdf.

4.8.5 Fraud Analysis

Analisis fraud dimulai dengan menganalisis keaslian dokumen e-invoice yang didapatkan pada proses collection. Sebuah dokumen invoice dengan nama InvoiceUMJ dianalisis dengan dua tools yakni exiftools dan pdftool.py. Exiftool digunakan untuk memeriksa metadata pada InvoiceUMJ.pdf, pemeriksaan metadata dari exiftool ini

```
C:\Users\user\Desktop\exiftool(-k).exe
ExifTool Version Number      : 12.22
File Name                    : InvoiceUMJ.pdf
Directory                   : C:/Users/user/Desktop
File Size                    : 784 KiB
File Modification Date/Time  : 2020:07:25 08:08:34+07:00
File Access Date/Time       : 2020:07:25 08:09:16+07:00
File Creation Date/Time     : 2020:07:24 05:05:12+07:00
File Permissions             : -rw-rw-rw-
File Type                    : PDF
File Type Extension         : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.4
Linearized                   : No
Page Count                   : 1
XMP Toolkit                  : 3.1-701
Producer                    : Microsoft® Word 2016
Modify Date                  : 2020:07:25 08:08:34+07:00
Title                       : InvoiceUMJ
Creator                     : sdas.ltd
Creator Tool                 : Microsoft® Word 2016
Create Date                  : 2020:07:24 08:05:12+10:00
Document ID                  : uuid:59373C1B-E243-4301-B5A7-1749E8C24159
Instance ID                  : uuid:59373C1B-E243-4301-B5A7-1749E8C24159
Language                     : en-US
Tagged PDF                   : Yes
Author                      : sdas.ltd
-- press ENTER --
```

Gambar 4.9 Rincian meta data file menggunakan exiftool

Pada gambar 4.9 menggambarkan meta data dari InvoiceUMJ.pdf yang terdiri dari *create date* tertulis tanggal 24 Juli 2020 pada pukul 08:05:12 GMT+10 dikarenakan pembuatan dokumen ada di Australia yakni perusahaan tempat software tersebut sedangkan tanggal *modify date* tertulis tanggal 25 Juli 2020 pukul 08:08:34 GMT+7 sehingga dari data ini dapat diketahui terjadinya perubahan data pada file tersebut, tetapi dengan menggunakan satu tools ini kurang dapat membuktikan bahwa dokumen ini telah dimodifikasi. Tools yang dapat digunakan untuk mendeteksi rekayasa pada dokumen PDF adalah pdftool.py yang merupakan tools berbasis python dengan memeriksa *incremental update* pada dokumen PDF.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop>pdftool.py iu InvoiceUMJ.pdf
File: InvoiceUMJ.pdf
1: objects= 136 length= 614472 difference= 614472 MD5= b433154db657050dcaa155aa8767ab81
2: objects= 12 length= 803168 difference= 188696 MD5= 8587b7297589b9f89be9e721887ce0b3

C:\Users\user\Desktop>
```

Gambar 4.10 incremental update dari InvoiceUMJ.pdf

Gambar 4.10 pdftool.py mendeteksi terdapat *incremental update* pada dokumen InvoiceUMJ.pdf seperti yang ditunjukkan pada poin 2 yang memiliki object 12 dengan length 803168.

```

000C4090: 31 20 30 30 30 30 20 6E 0D 0A 32 32 31 20 31 1 00000 n..221 1
000C40A0: 0D 0A 30 30 30 30 38 30 31 30 39 33 20 30 30 30 ..0000801093 000
000C40B0: 30 30 20 0E 0D 0A 74 72 61 69 6C 65 72 0D 0A 3C 00 n..trailer..<
000C40C0: 3C 2F 49 44 20 5B 3C 31 42 33 43 33 37 35 39 34 </ID [<1B3C37594
000C40D0: 33 45 32 30 31 34 33 42 35 41 37 31 37 34 39 45 3E20143B5A71749E
000C40E0: 38 43 32 34 31 35 39 3E 20 3C 39 41 30 30 44 42 8C24159> <9A00DB
000C40F0: 33 42 43 35 30 42 46 46 33 45 45 45 37 37 30 43 3BC50BFF3EEE770C
000C4100: 39 31 33 32 30 34 33 30 45 30 3E 5D 0D 0A 2F 52 91320430E0>]../R
000C4110: 6F 6F 74 20 31 20 30 20 52 0D 0A 2F 49 6E 66 6F oot 1 0 R../Info
000C4120: 20 32 30 20 30 20 52 0D 0A 2F 53 69 7A 65 20 32 20 0 R../Size 2
000C4130: 32 32 0D 0A 2F 50 72 65 76 20 36 31 31 35 37 34 22../Prev 611574
000C4140: 0D 0A 3E 3E 0D 0A 73 74 61 72 74 78 72 65 66 0D ...>...startxref.
000C4150: 0A 38 30 32 37 31 35 0D 0A 25 25 45 4F 46 0D 0A .802715..%%EOF..

C:\Users\user\Desktop>pdftool.py iu -s 2 InvoiceUMJ.pdf

```

Gambar 4.11 select incremental update dari InvoiceUMJ.pdf

Untuk mengetahui nilai dari incremental update pada file InvoiceUMJ.pdf memerlukan perintah `pdftool.py iu -s 2 InvoiceUMJ.pdf` seperti pada gambar 4.11, lalu tools ini akan memberikan hasil dari perubahan atau manipulasi data yang dilakukan pada file invoice. Dari perintah ini akan diketahui dua sintak EOF yang menandakan bahwa file pdf tersebut telah dirubah.

```

A string with comments to be included in the log file
--ignoreprocessingerrors
Ignore errors during file processing

This tool also accepts flag arguments (#f#), read the man page (-m) for more
info.

C:\Users\user\Desktop>pdftool.py iu -s 1 -d InvoiceUMJ.pdf

```

Gambar 4.12 perintah dump dari file InvoiceUMJ.pdf

Pada poin 1 seperti yang digambarkan pada Gambar 4.10 merupakan file asli , dan pada poin 2 merupakan perubahan yang dilakukan pada file pdf. Perintah dump file untuk mengembalikan file asli yang belum dirubah menggunakan `pdftool.py iu -s 1 d InvoiceUMJ.pdf` seperti yang digambarkan pada Gambar 4.12.

```

0000028007 00000 n
0000028293 00000 n
0000225775 00000 n
0000227322 00000 n
0000227670 00000 n
0000451914 00000 n
0000453461 00000 n
0000453489 00000 n
0000519876 00000 n
0000521423 00000 n
0000521724 00000 n
0000534895 00000 n
0000536442 00000 n
0000536486 00000 n
0000536576 00000 n
0000536604 00000 n
0000603955 00000 n
0000605502 00000 n
0000608176 00000 n
trailer
<</Size 137/Root 1 0 R/Info 20 0 R/ID[<1B3C375943E20143B5A71749E8C24159><1B3C375943E20143B5A717
49E8C24159>] >>
startxref
611574
%%EOF
C:\Users\user\Desktop>

```

Gambar 4.13 hasil dump file InvoiceUMJ.pdf

Gambar 4.13 memperlihatkan hasil dump dari file pdf yang asli, dimana hasil dump merupakan sintak pdf yang apabila dilihat secara biasa akan kesulitan untuk dibaca. Untuk membaca hasil dump dapat dicopy pada text editor tetapi untuk cara mudahnya menggunakan perintah pdftool.py iu -s 1 -d -o recoveredInvoiceUMJ.pdf InvoiceUMJ.pdf seperti gambar 4.14

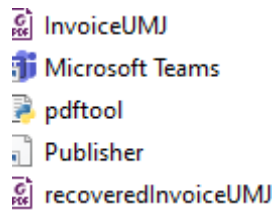
```

C:\Windows\System32\cmd.exe
0000225775 00000 n
0000227322 00000 n
0000227670 00000 n
0000451914 00000 n
0000453461 00000 n
0000453489 00000 n
0000519876 00000 n
0000521423 00000 n
0000521724 00000 n
0000534895 00000 n
0000536442 00000 n
0000536486 00000 n
0000536576 00000 n
0000536604 00000 n
0000603955 00000 n
0000605502 00000 n
0000608176 00000 n
trailer
<</Size 137/Root 1 0 R/Info 20 0 R/ID[<1B3C375943E20143B5A71749E8C24159><1B3C375943E20143B5A717
49E8C24159>] >>
startxref
611574
%%EOF
C:\Users\user\Desktop>pdftool.py iu -s 1 -d -o recoveredInvoiceUMJ.pdf InvoiceUMJ.pdf
C:\Users\user\Desktop>

```

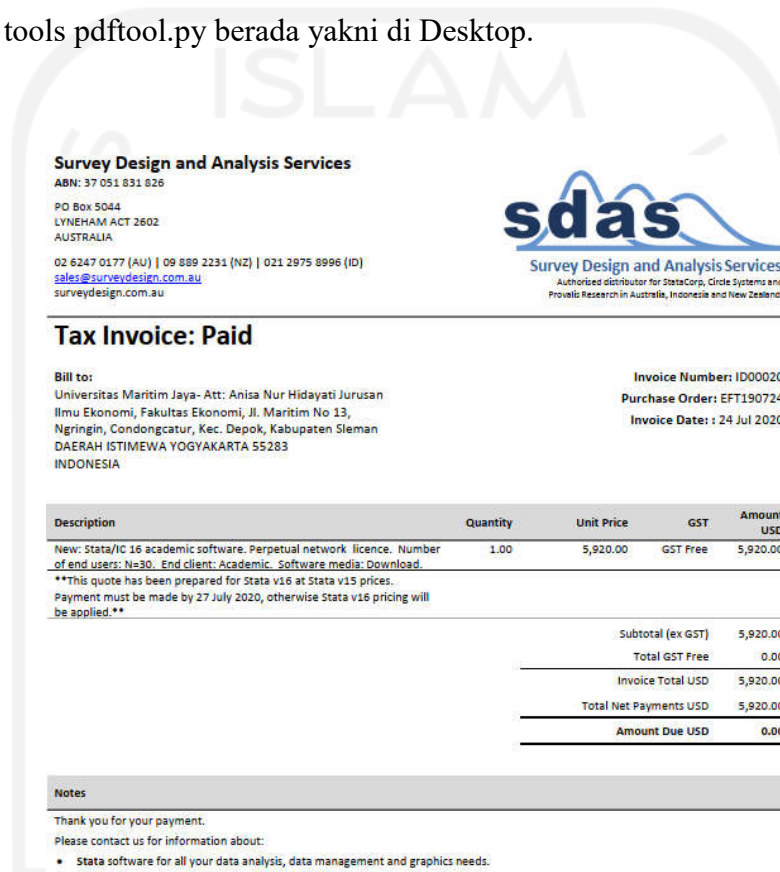
Gambar 4.14 Menyimpan hasil dump menjadi recoveredInvoiceUMJ.pdf

Pada gambar 4.14 menunjukan bahwa tools pdftool.py memberikan fitur untuk membuat suatu file pdf yang berisi dari dump file asli yang belum dimanipulasi.



Gambar 4.15 hasil dump di explorer

Pada gambar 4.15 menunjukkan hasil file yang telah dibuat oleh tool pdftool.py untuk dump file dari file asli InvoiceUMJ.pdf. Hasil ekstraksi file pdf berada pada lokasi yang sama dimana tools pdftool.py berada yakni di Desktop.



Gambar 4.16 file recoveredInvoiceUMJ.pdf

Gambar 4.16 menunjukkan file asli dari InvoiceUMJ.pdf dimana terdapat perbedaan dengan file InvoiceUMJ.pdf pada gambar 4.17 dimana nilai harga berbeda \$2000 Dollar Amerika. Dari kedua file tersebut dapat disimpulkan terjadi manipulasi laporan keuangan yang dilakukan oleh tersangka dengan mengganti nominal invoice menjadi \$7.920 dari \$5.920.

Survey Design and Analysis Services

ABN: 37 051 831 826

PO Box 5044
LYNEHAM ACT 2602
AUSTRALIA

02 6247 0177 (AU) | 09 889 2231 (NZ) | 021 2975 8996 (ID)

sales@surveydesign.com.au
surveydesign.com.au**Tax Invoice: Paid****Bill to:**Universitas Maritim Jaya- Att: Anisa Nur Hidayati Jurusan
Ilmu Ekonomi, Fakultas Ekonomi, Jl. Maritim No 13,
Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman
DAERAH ISTIMEWA YOGYAKARTA 55283
INDONESIA

Invoice Number: ID00020

Purchase Order: EFT190724

Invoice Date: 24 Jul 2020

Description	Quantity	Unit Price	GST	Amount USD
New: Stata/IC 16 academic software. Perpetual network licence. Number of end users: N=30. End client: Academic. Software media: Download.	1.00	7,920.00	GST Free	7,920.00
This quote has been prepared for Stata v16 at Stata v15 prices. Payment must be made by 27 July 2020, otherwise Stata v16 pricing will be applied.				
Subtotal (ex GST)				7,920.00
Total GST Free				0.00
Invoice Total USD				7,920.00
Total Net Payments USD				7,920.00
Amount Due USD				0.00

Notes

Thank you for your payment.

Please contact us for information about:

- Stata software for all your data analysis, data management and graphics needs.
- Stata Press books and Stata NetCourse online training courses to support your use of Stata.
- Stat/Transfer for fast, easy and accurate transfer of data between data applications.
- QDA Miner and Wordstat for qualitative, content and text-mining analysis.

Gambar 4.17 File InvoiceUMJ.pdf yang berisi manipulasi data

Hal tersebut membuktikan bahwa terdapat perubahan / modifikasi yang dilakukan pada invoice yang berbentuk PDF dan untuk mengetahui bagian mana yang dimodifikasi dapat dilakukan dengan tools ini . Tools ini juga dapat digunakan untuk mengembalikan file PDF menjadi asli seperti sebelum dimodifikasi atau sebelum adanya *incremental updates*. Hasil perbandingan file PDF yang dimodifikasi dengan file PDF asli ditunjukkan pada gambar 4.5 dimana terjadi perubahan penambahan jumlah dari semula 5,920 dollar menjadi 7,920 dollar dimana file PDF yang asli ternyata sama dengan file yang dikirim secara offline oleh pihak STATA. Tahapan ini membuktikan terjadinya penyalahgunaan laporan keuangan dan modifikasi laporan untuk keuntungan pribadi karyawan tersebut.

4.8.6 Report

Kasus penggelapan uang menggunakan metode manipulasi laporan keuangan akan dibuat laporan oleh tim yang bertugas dan selanjutnya akan dilaporkan kepada instansi pendidikan tersebut. Laporan kasus penggelapan ini dinyatakan bahwa memang karyawan ANH telah melakukan tindakan penggelapan uang dengan memanipulasi laporan e-invoice atau cyber fraud dan merugikan Universitas Maju Mundur sebesar 2000 dollar US.

4.8.7 Incident Closure

Penutupan kasus audit penggelapan uang ini dilakukan sesuai kebijakan setiap instansi, dimana kasus ini dapat dibawa ke pengadilan atau diselesaikan secara kekeluargaan. Kasus ini ditutup secara kekeluargaan dimana karyawan ANH diminta untuk mengembalikan uang sebesar 2000 dollar US, mendapatkan SP serta mendapatkan beberapa sanksi administrasi yang lain dikarenakan perbuatan karyawan yang merugikan instansi.

4.8.8 Concurrent Proseses

Concurrent proses pada kasus ini dilakukan dengan mendokumentasi semua kegiatan sesuai dengan SOP pada instansi mulai dari tahap Planning hingga tahapan Incident Closure. Hal ini dilakukan seperti apabila barang bukti digital yang dianalisis ternyata bukan barang bukti yang asli maka proses Collection dapat diulangi lagi dan mencari bukti Invoice yang Asli.



BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Dari penelitian ini dapat disimpulkan tiga hal yakni :

1. Pengembangan Cyber Fraud Framework ini berdasarkan dari Metode Jabareen dengan menggunakan 6 fase yakni *Mapping the selected data source, extensive reading and categorizing of the selected data, Identifiyin and naming object, Deconstructing and categorizing the concept, Integrating concept, Synthesis, resynthesis and make it all sense*. Terdapat 8 tahapan dalam cyber fraud framework ini yakni : *Forensic Readiness, Planning , Incident Response, Collection, Analysis, Report, Incident Closure* dengan 1 proses *Concurrent*.
2. Evaluasi framework ini dilakukan dengan Delphi method yakni dengan memberikan kuesioner kepada para praktisi baik dibidang audit fraud maupun bidang digital forensik serta akademisi secara umum menyatakan bahwa pengembangan framework investigasi memang diperlukan tetapi tingkat kelayakan dan apakah framework yang dikembangkan sudah cukup masih belum memenuhi konsensus, sehingga diperlukan evaluasi dengan responden yang lebih banyak dengan beberapa putaran survey.
3. Implementasi framework untuk kasus *cyber fraud* dapat dilakukan, akan tetapi apabila kasus *cyber fraud* dilakukan terlalu lama, barang bukti digital dapat hilang sehingga dalam tahapan readiness harus ditentukan SOP dari instansi yang bersangkutan untuk mencegah dampak lebih buruk dari tindakan fraud apalagi yang dilakukan oleh pegawai internal.

5.2 Saran

Untuk penelitian kedepannya, penulis memberikan beberapa saran yang berkaitan dengan penelitian ini yakni ,

1. Melakukan pengujian secara lebih komprehensif kepada praktisi di lembaga audit negara maupun swasta sehingga mendapatkan umpan balik untuk mengembangkan framework sehingga didapatkan consensus bahwa framework yang dikembangkan sudah layak digunakan

2. Menambahkan beberapa aspek untuk kejahatan fraud yang menggunakan teknologi terbaru, sehingga framework dapat digunakan secara umum untuk kasus-kasus terbaru.



Daftar Pustaka

- Abduh, M., Wirahadikusumah, R. D., & Messah, Y. (2018). Framework Development Methodology for Sustainable Procurement of Construction Works in Indonesia. *MATEC Web of Conferences*, 203. <https://doi.org/10.1051/matecconf/201820302014>
- Accenture. (2018). *Unmask Digital Fraud*.
- Adom, D., & Hussain, Emad.Kamil. and Joe, A. . A. (2018). THEORETICAL AND CONCEPTUAL FRAMEWORK : MANDATORY INGREDIENTS THEORETICAL AND CONCEPTUAL FRAMEWORK : MANDATORY INGREDIENTS Engineering Dickson Adom * Emad Kamil Hussein. *International Journal of Scientific Research*, 7(1), 93–98.
<https://www.researchgate.net/publication/322204158%0ATHEORETICAL>
- Afra, S., & Alhajj, R. (2019). Integrated framework for criminal network extraction from Web. *Journal of Information Science*. <https://doi.org/10.1177/0165551519888606>
- Ahmad, S., Saad, N. L., Zulkifli, Z., & Nasaruddin, S. H. (2016). Proposed network forensic framework for analyzing IaaS cloud computing environment. 2015 *International Symposium on Mathematical Sciences and Computing Research, ISMSC 2015 - Proceedings*, 2015, 144–149. <https://doi.org/10.1109/ISMSC.2015.7594043>
- Ajayi, E. F. . (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(August), 1–12.
<https://doi.org/10.5897/JIIS2015.0089>
- 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>
- Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. *National Institute of Justice*, 7(2), 95–111.
<https://doi.org/10.3408/jasti.7.95>
- Bacon, C. J., & Fitzgerald, B. (2001). A Systemic Framework for the Field of Information Systems. *Data Base for Advances in Information Systems*, 32(2), 46–67.
<https://doi.org/10.1145/506732.506738>
- Cusack, B., & Ahokovi, T. (2016). Improving forensic software tool performance in detecting fraud for financial statements. *Proceedings of the 14th Australian Digital Forensics Conference, ADF 2016, December*, 17–24.
<https://doi.org/10.4225/75/58a4f9b604efd>
- Dickson, A., Adu-Agyem, J., & Emad Kamil, H. (2018). Theoretical and conceptual framework: mandatory ingredients of a quality research. *International Journal of*

Scientific Research, 7(1), 438–441.

- Dimitriadis, A., Ivezić, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5(December 2019), 100015. <https://doi.org/10.1016/j.array.2019.100015>
- Durtischi, C. (2001). Fraud 101: Techniques and Strategies for Detection. In *The Accounting Review* (Vol. 76, Issue 4).
- Eizenberg, E., & Jabareen, Y. (2017). Social sustainability: A new conceptual framework. *Sustainability (Switzerland)*, 9(1). <https://doi.org/10.3390/su9010068>
- Federal Bureau of Investigation. (2019). 2019 Internet Crime Report. *Federal Bureau of Investigation - Internet Crime Complaint Center*, 1–28. https://pdf.ic3.gov/2019_IC3Report.pdf
- Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime*, 14(2), 190–207. <https://doi.org/10.1108/13590790710742672>
- Goodison, S. E., Davis, R. C., & Jackson, B. A. (n.d.). *Digital Evidence and the US Criminal Justice System*.
- Goudbeek, A., Choo, K. K. R., & Le-Khac, N. A. (2018). A Forensic Investigation Framework for Smart Home Environment. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 1446–1451. <https://doi.org/10.1109/TrustCom/BigDataSE.2018.00201>
- Haddadi, A., Johansen, A., & Andersen, B. (2016). A Conceptual Framework to Enhance Value Creation in Construction Projects. *Procedia Computer Science*, 100(1877), 565–573. <https://doi.org/10.1016/j.procs.2016.09.196>
- Harbawi, M., & Varol, A. (2017). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*. <https://doi.org/10.1109/ISDFS.2017.7916508>
- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008–1015. <https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>
- Hayes, B., Jeandesboz, J., Ragazzi, F., Simon, S., & Mitsilegas, V. (2015). The law enforcement challenges of cybercrime: are we really playing catch-up? *European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs*, November. <https://doi.org/10.1017/CBO9781107415324.004>
- Howard, R. (2009). *Cyber Fraud: Tactics, Techniques and Procedures*.

- Htun, N. L., & Thwin, M. M. S. (2017). Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation. *The International Journal of Engineering and Science*, 6(01), 82–92. <https://doi.org/10.9790/1813-0601028292>
- Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4), 49–62. <https://doi.org/10.1177/160940690900800406>
- Khadijah, S., Mohd, T., Adil, Z., & Talib, B. (2013). *Standard Operating Procedure of Digital Evidence Collection*. July. <http://www.cybercsi.my/download/SOP OF DIGITAL EVIDENCE COLLECTION.pdf>
- Kigwana, I., Kebande, V. R., & Venter, H. S. (2017). A proposed digital forensic investigation framework for an eGovernment structure for Uganda. *2017 IST-Africa Week Conference, IST-Africa 2017, August 2018*. <https://doi.org/10.23919/ISTAFRICA.2017.8102348>
- Kohn, M. D. (2012). *Integrated Digital Forensic Process Model*. November.
- Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Generation Computer Systems*, 110, 91–106. <https://doi.org/10.1016/j.future.2020.03.042>
- KPMG Australia. (2019). *Global Banking Fraud Survey 2019*. May. <https://home.kpmg/au/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html>
- Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, 120, 13–25. <https://doi.org/10.1016/j.future.2021.02.016>
- Loo, R. (2002). The Delphi method: A powerful tool for strategic management. *Policing*, 25(4), 762–769. <https://doi.org/10.1108/13639510210450677>
- Manning, G. A. (2005). *Financial Investigation and Forensic Accounting*. <http://ia600302.us.archive.org/29/items/gov.ntis.ava21336vnb1/ava21336vnb1.pdf%5Cnpapers3://publication/uuid/C84C9BBD-F394-42B5-A13C-232326E7623F>
- Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *Procedia Computer Science*, 85(Cms), 149–154. <https://doi.org/10.1016/j.procs.2016.05.202>
- Material, S. (2019). *Study Material Professional Programme Forensic Audit*.
- Megan, E. (2019). Crime in England and Wales: year ending March 2019. *Office for National Statistics, March 2019*, 1–24. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crime>

- Microsoft. (2020). *Online Fraud : Your Guide to Prevention, Detection, Recovery*.
- Murdock, D. H., & Murdock, D. H. (2018). Association of Certified Fraud Examiners (ACFE). *Auditor Essentials*, 7–10. <https://doi.org/10.1201/9781315178141-3>
- National Forensic Science Technology Center. (2014). A Simplified Guide To Digital Evidence. *National Forensic Science Technology Center*.
- Nawang, N. I. (2017). Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia. *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017, August 1996*, 13–18. <https://doi.org/10.1109/Anti-Cybercrime.2017.7905255>
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information and Management*, 42(1), 15–29. <https://doi.org/10.1016/j.im.2003.11.002>
- Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, 76(July), 130–157. <https://doi.org/10.1016/j.engappai.2018.07.008>
- Sathwara, S., Dutta, N., & Pricop, E. (2018). IoT Forensic, A digital investigation framework for IoT systems Snehal. *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), June*, 1–9. <https://doi.org/10.1145/3230833.3233257>
- Saxunova, D. (2012). INVESTIGATION OF SUSPECTED FRAUD. *International Journal of Business and Management Studies*, 1.
- Sharma, P., Arora, D., & Sakthivel, T. (2020). Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications. *Procedia Computer Science*, 167(2019), 907–917. <https://doi.org/10.1016/j.procs.2020.03.390>
- Smutny, Z., & Veber, J. (2015). Standard ISO 27037 : 2012 and Collection of Digital Evidence : Experience in the In : 14th European Conference on Cyber Warfare & Security , Standard ISO 27037 : 2012 and Collection of Digital Evidence : Experience in the Czech Republic. *14th European Conference on Cyber Warfare & Security, July 2015*.
- Valjarevic, A., Venter, H., & Petrovic, R. (2017). ISO/IEC 27043:2015 - Role and application. *24th Telecommunications Forum, TELFOR 2016*. <https://doi.org/10.1109/TELFOR.2016.7818718>

LAMPIRAN A

INSTRUMEN PENELITIAN

INSTRUMEN KUISIONER PENYUSUNAN FRAMEWORK *CYBER FRAUD*

Kuisisioner berikut dibuat menggunakan delphi method. Delphi method merupakan salah satu metode yang cukup populer digunakan pada penelitian Sistem Informasi. Metode delphi survey merupakan survey yang dilakukan pada seorang ahli dan menyediakan variasi sesuai dengan tujuan penelitian. Metode ini juga dapat digunakan untuk menyatukan pendapat tentang identifikasi kendala pada permasalahan yang akan diteliti (Abduh et al., 2018).

Terdapat dua jenis aplikasi delphi method yakni untuk forecasting dan identifikasi masalah, serta untuk menguji konsep/pengembangan framework (Okoli & Pawlowski, 2004).

Untuk survey mengenai pengembangan framework akan menggunakan instrument penelitian yang dikembangkan oleh Bacon (Bacon & Fitzgerald, 2001) yang terdiri dari 6 pertanyaan dengan tiga indikator jawaban seperti pada Tabel 1.

Tabel 1. Instrumen kuisisioner

No	Pertanyaan	Jawaban		
		Ya	Tidak	Mungkin
1	Apakah framework yang dikembangkan dibutuhkan di lapangan?			
2	Apakah framework yang dikembangkan layak digunakan untuk di lapangan?			
3	Apakah informasi yang disajikan adalah tema yang cocok pada bidang tersebut?			
No	Pertanyaan	Jawaban		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pengelompokan area utama pada framework dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?			
5	Apakah perbedaan karakter pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			
6	Apakah perbedaan kompetensi pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			

Untuk survey dari para ahli mengenai perkembangan cyber fraud framework akan ada sedikit modifikasi instrument seperti yang ditunjukkan pada Tabel 2.

Tabel 2. Modifikasi Instrumen kuisisioner

No	Pertanyaan	Jawaban		
		Ya	Tidak	Mungkin

1	Apakah framework yang dikembangkan dibutuhkan di lapangan?			
2	Apakah framework yang dikembangkan layak digunakan untuk lapangan?			
3	Apakah konsep/tahapan yang disajikan cocok pada bidang <i>Cyber Fraud</i> ?			
No	Pertanyaan	Jawaban		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pemberian konsep/tahapan pada framework dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?			
5	Apakah perbedaan konsep/tahapan pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?			



HASIL KUESIONER DARI PRAKTISI

Praktisi Kementerian Keuangan

KUISIONER PENYUSUNAN *FRAMEWORK CYBER FRAUD*

Assalamu'alaikum Wr. Wb.

Yth **Bapak/Ibu Responden** yang saya hormati,

Perkenalkan nama saya Anisa Nur Hidayati NIM 18917106, mahasiswa Magister Teknik Informatika Universitas Islam Indonesia. Saya ingin memohon bantuan Bapak/Ibu untuk memberikan masukan terkait penelitian tesis saya yang berjudul “Pengembangan konseptual *framework* untuk *cyber fraud investigation*“ dimana masukan Bapak/Ibu sebagai praktisi Audit Forensik maupun Digital Forensik akan sangat membantu dalam proses penelitian ini. Berikut yang ditunjukkan tabel 1 merupakan kuesioner yang dapat Bapak./Ibu isi terkait pengembangan *framework* untuk *cyber fraud investigation* yang telah saya lampirkan dihalaman kedua.

Tabel 1. Kuisisioner Pengembangan *Cyber Fraud Framework*

No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Tidak	Mungkin
1	Apakah <i>framework</i> yang dikembangkan dibutuhkan di lapangan?	X		
2	Apakah <i>framework</i> yang dikembangkan layak digunakan untuk di lapangan?	X		
3	Apakah konsep/tahapan yang disajikan cocok pada bidang <i>Cyber Fraud</i> ?	X		
No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pemberian konsep/tahapan pada <i>framework</i> dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?	X		
5	Apakah perbedaan konsep/tahapan pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?	X		

Atas segala bantuan dan partisipasi yang Bapak/Ibu berikan, saya mengucapkan terima kasih. Semoga segala kebbaikannya mendapatkan balasan yang lebih baik dari Allah SWT dan hasil dari penelitian ini bisa bermanfaat bagi orang banyak.

HASIL KUESIONER DARI PRAKTISI PUSFID

KUISIONER PENYUSUNAN *FRAMEWORK CYBER FRAUD*

Assalamu'alaikum Wr. Wb.

Bapak **Fietyata Yudha, S.Kom., M.Kom** yang saya hormati,

Perkenalkan nama saya Anisa Nur Hidayati NIM 18917106, mahasiswa Magister Teknik Informatika Universitas Islam Indonesia. Saya ingin memohon bantuan Bapak untuk memberikan masukan terkait penelitian tesis saya yang berjudul “ Pengembangan konseptual *framework* untuk *cyber fraud investigation*“ dimana masukan Bapak sebagai praktisi Digital Forensik akan sangat membantu dalam proses penelitian ini.

Berikut yang ditunjukkan tabel 1 merupakan kuesioner yang dapat Bapak isi terkait pengembangan *framework* untuk *cyber fraud investigation* yang telah saya lampirkan di halaman kedua.

Tabel 1. Kuisisioner Pengembangan *Cyber Fraud Framework*

No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Tidak	Mungkin
1	Apakah <i>framework</i> yang dikembangkan dibutuhkan di lapangan?	Karakteristik cyberfraud di setiap wilayah adalah unik, untuk studi kasus di Indonesia saya rasa perlu dikembangkan <i>framework</i> tersebut		
2	Apakah <i>framework</i> yang dikembangkan layak digunakan untuk di lapangan?			Harus dilakukan pengujian secara comprehensive terkait <i>framework</i> tersebut dengan studi kasus/scenario yang dibuat berdasarkan kejadian sebenarnya. Karena ranah fraud menurut saya tidak banyak bersentuhan ke APH tp lebih ke pada lembaga audit baik government maupun swasta
3	Apakah konsep/tahapan yang disajikan cocok pada bidang <i>Cyber Fraud</i> ?	Sudah ada proses mixing disini		

		untuk menggabungkan 2 buah framework. Perlu ada penjelasan detail bagaimana metode yang digunakan untuk menggabungkan/ mensintesis framework ini sehingga framework yang dihasilkan bukan merupakan hasil asumsi dari peneliti		
No	Pertanyaan	Jawaban(dengan alasan)		
		Ya	Perubahan Minor	Perubahan Mayor
4	Apakah pemberian konsep/tahapan pada <i>framework</i> dapat diterima sebagaimana adanya (ya); atau perubahan apa yang dibutuhkan?		Menurut saya perlu dilakukan analisis terkait karakteristik kasus fraud yang ada, misal pemanfaatan teknologi dan lain-lain untuk memastikan bahwa framework yang dihasilkan sudah mengakomodir berbagai teknologi tersebut. Misal analisis framework2 yang berhubungan dengan media sosial	
5	Apakah perbedaan konsep/tahapan pada bidang tersebut dapat diterima (ya); atau apa perubahan dibutuhkan?		SDA	

Atas segala bantuan dan partisipasi yang Bapak berikan, saya mengucapkan terima kasih. Semoga segala kebbaikannya mendapatkan balasan yang lebih baik dari Allah SWT dan hasil dari penelitian ini bisa bermanfaat bagi orang banyak.
Wassalamu'alaikum Wr. Wb.



LAMPIRAN B

Data yang digunakan untuk kategorisasi data

Nama artikel	Nama Pengarang	Sumber Data	Kategori
Cyberfraud and the implications for effective risk-based responses: themes from UK research	Levi, Michael Doig, Alan Gundur, Rajeev Wall, David Williams, Matthew	Artikel Jurnal	Audit Fraud
Spreading dynamics of SVFR online fraud information model on heterogeneous networks	Hou, Jingrui Chi, Ming Li, Tao Guan, Zhi Hong Luo, Kai Zhang, Ding Xue	Artikel Jurnal	Audit Fraud
A multidisciplinary digital forensic investigation process model	Lutui, Raymond	Artikel Jurnal	Digital Forensik
Online frauds: Learning from victims why they fall for these scams	Button, Mark Nicholls, Carol Mc Naughton Kerr, Jane Owen, Rachael	Artikel Jurnal	Audit Fraud
Teknik Audit Investigatif Dalam Pengungkapan Money Laundering Berdasarkan Perspektif Akuntan Forensik	Dewi Yuniarti Rozali, Rozmita	Artikel Jurnal	Audit Fraud
INTERNATIONAL STANDARD ISO / IEC 27043: Information technology — Security techniques — Incident investigation principles and processes	ISO	Dokumen ISO	Digital Forensik
INTEGRATING FORENSIC INVESTIGATION TECHNIQUES INTO Group Head of Internal Audit	Gerry Chipper	Artikel Jurnal	Audit Fraud
Computer Forensics Field Triage Process Model	Rogers, Marcus Goldman, James Mislán, Rick Wedge, Timothy Debrotá, Steve	Artikel Jurnal	Digital Forensik

Nama artikel	Nama Pengarang	Sumber Data	Kategori
Forensic Accounting Investigation Techniques: Any Rationalization?	Oyedokun, Godwin Emmanuel	Artikel Jurnal	Audit Fraud
Exploring the cybercrime investigation framework of ATM Heist from ISO/IEC 27043:2015	Kao, Da Yu	Artikel Jurnal	Digital Forensik
A New Approach of Digital Forensic Model for Digital Forensic Investigation	O, Inikpi Chris, Dr David, Dr	Artikel Jurnal	Digital Forensik
A PROPOSED FRAMEWORK FOR FORENSIC IMAGE ENHANCEMENT	Enst, Mler Anab, Reklamcilik Tez, Doktora Dan, L U	Artikel Jurnal	Digital Forensik
D4I - Digital forensics framework for reviewing and investigating cyber attacks	Dimitriadis, Athanasios Ivezic, Nenad Kulvatunyou, Boonserm Mavridis, Ioannis	Artikel Jurnal	Digital Forensik
Proposed network forensic framework for analyzing IaaS cloud computing environment	Ahmad, Samsiah Saad, Nor Liza Zulkifli, Zalikha Nasaruddin, Siti Hajar	Artikel Jurnal	Digital Forensik
A generic digital forensic investigation framework for Internet of Things (IoT)	Kebande, Victor R. Ray, Indrakshi	Artikel Jurnal	Digital Forensik
A Forensic Investigation Framework for Smart Home Environment	Goudbeek, Arnoud Choo, Kim Kwang Raymond Le-Khac, Nhien An	Artikel Jurnal	Digital Forensik
Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody	Prayudi, Yudi Ashari, Ahmad K Priyambodo, Tri	Artikel Jurnal	Digital Forensik
Mapping process of digital forensic investigation framework	Selamat, Siti Rahayu Yusof, Robiah Sahib, Shahrin	Artikel Jurnal	Digital Forensik
Framework for a Digital Forensic Investigation.	Kohn, Michael Olivier, Martin Eloff, Jan	Artikel Jurnal	Digital Forensik
Digital Forensic Framework for a Cloud Environment	Sibiya, George Venter, Hein S Fogwill, Thomas	Artikel Jurnal	Digital Forensik
Cloud Forensic Frameworks , Challenges ,	Pandi, Gayatri S	Artikel Jurnal	Digital Forensik

Nama artikel	Nama Pengarang	Sumber Data	Kategori
State of Art and Future Directions			
A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics	Khanafseh, Mohammed Qatawneh, Mohammad Almobaideen, Wesam	Artikel Jurnal	Digital Forensik
First Respond Framework Untuk Forensik CCTV	Suratno, Danang Mulyadipa Riadi, Imam Prayudi, Yudi	Artikel Jurnal	Digital Forensik
Fraud 101: Techniques and Strategies for Detection	Durtischi, Cindy	Buku	Audit Fraud
Fraud Auditing and Forensic Accounting	Singleton, Tommie W Singleton, Aaron J	Buku	Audit Fraud
Over half of fraud incidents in England and Wales are now cyber-related	Hedley, Daniel Llp, Mitchell	Artikel Jurnal	Audit Fraud
Computer forensics in IT audit and credit card fraud investigation - For USB devices	Verma, Saurabh Singh, Abhishek Singh, Divakar Laxmi, Vijay	Artikel Jurnal	Digital Forensik
Cyber Fraud: Tactics, Techniques and Procedures	Howard, Rick	Buku	Audit Fraud
Financial Investigation and Forensic Accounting	Manning, George A	Buku	Audit Fraud
A hierarchical, objectives-based framework for the digital investigations process	Beebe, Nicole Lang Clark, Jan Guynes	Artikel Jurnal	Digital Forensik
IoT Forensic, A digital investigation framework for IoT systems Snehil	Sathwara, Snehil Dutta, Nitul Pricop, Emil	Artikel Jurnal	Digital Forensik
A proposed digital forensic investigation framework for an eGovernment structure for Uganda	Kigwana, Ivans Kebande, Victor R. Venter, H. S.	Artikel Jurnal	Digital Forensik