IMPLEMENTASI BPMN UNTUK MEMBANGUN MODEL BISNIS FORENSIKA DIGITAL

Nyata Nopiansah

1411050106

Fakultas Bisnis dan Komputer

nyata.1411050106@mail.darmajaya.ac.id

ABSTRAKS

Model bisnis adalah sebuah konseptual untuk menggambarkan aktifitas dan menangkap nilai yang ada. Salah satu metode yang dapat digunakan untuk membuat model bisnis adalah BPMN. Dalam BPMN terdapat Business Proces Diagram (BPD) yang berfungsi untuk pemodelan bisnis berdasarkan proses. Tantangan muncul ketika mencoba mengkaitkan antara BPMN dengan konsep yang berbeda, yaitu forensika digital. Sebuah proses dalam mengumpulkan data, melakukan pemeriksaan, menganalisis, hingga didapatkan bukti yang dapat dipertanggungjawabkan untuk menyelesaikan sebuah peristiwa. Melalui pendekatan penelitian desain dapat ditemukan penghubung antara BPMN dengan forensika digital, yaitu adanya interaksi yang terjadi selama sebuah proses berlangsung. Dengan memodelkan proses forensik digital menggunakan BPMN dengan sub-model orchestration dan collaboration ditemukan dua kondisi. Pertama, diketahui interaksi yang terjadi dari dan ke proses yang berlangsung. Kedua, dapat diketahui interaksi antara aktor dengan aktifitas yang dilakukan selama proses berlangsung. Sehingga BPMN ini dapat diterapkan untuk pengembangan framework investigasi forensika digital dengan berfokus pada interaksi dan proses.

1. PENDAHULUAN

Komputer dapat dijadikan instrument untuk melakukan sebuah kejahatan. Jenis kejahatan komputer menurut Bainbridge (1993) yang disebutkan oleh Sutiyoso (2015) adalah memasukkan instruksi yang tidak sah ke dalam komputer, perubahan data, perusakan data, komputer digunakan sebagai alat bantu kejahatan tradisional, dan akses tidak sah terhadap komputer. Sedangkan kejahatan yang memanfaatkan teknologi internet dikenal dengan *cybercrime*. Kejahatan siber telah menjadi bagian dari kehidupan sehari-hari. Serangan ini bisa terjadi terhadap kepentingan bisnis atau bahkan negara dengan target *smartphone*, penipuan media sosial, dan kerentanan terhadap IoT (*Internet of Things*) yang dijadikan sebagai taktik penyerang dan motivasi. Penyerangan ini antara lain; *e-mail phishing*, *e-mail malware*, *Crypto-Ransomware*, dan Bots (Symantec, 2016).

Perkembangan kejahatan harus diimbangi dengan cara penyelesaian yang benar. Oleh sebab itu, berkembang pula ilmu forensik komputer atau forensik digital. Secara sederhana, forensik digital adalah keseluruhan proses dalam mengambil, memulihkan, menyimpan, memeriksa informasi atau dokumen elektronik yang terdapat dalam sistem elektronik atau media penyimpanan, berdasarkan cara dan dengan alat yang dapat dipertanggungjawabkan secara ilmiah untuk kepentingan pembuktian (Raditio, 2014: 94). Sedangkan dalam melakukan forensik digital terdapat tahapan dasar yang yang dikemukakan oleh NIST (2006) yaitu *Collection, Examination, Analysis, Reporting*. NIST (*National Institute of Standards and Technology*) Amerika Serikat yang bertanggungjawab untuk mengembangkan standard dan pedoman, termasuk di dalamnya persyaratan minimum untuk menyediakan keamanan informasi

yang memadai (Kent, Chevalier, Grance, & Dang, 2006).

Panduan yang dikembangkan oleh NIST dijadikan titik awal dalam melakukan proses forensik digital sesuai dengan hukum dan peraturan yang berlaku di setiap organisasi atau negara. Dalam melakukan tahapan forensik digital dibutuhkan model atau *framework* sebagai acuan pelaksanaannya. Namun, hingga saat ini belum terdapat standar model forensik digital yang dapat digunakan sebagai acuan bagi semua instansi atau organisasi. Hal ini karena setiap peneliti, organisasi, atau instansi dapat mengembangkan modelnya sendiri (Prayudi, Ashari, & K Priyambodo, 2015). Selanjutnya, Prayudi, Ashari, dan Priyambodo (2014) pernah melakukan penelitian tentang *chain of custody* berdasarkan model bisnis. Model yang dikembangkan adalah *Digital Evidence Cabinets* (DEC) yang terdiri tiga komponen, yaitu manajemen bukti digital, *digital evidence bags with tag*, dan akses kontrol. Sehingga bukti digital tidak disimpan dalam komputer penyidik, namun disimpan dalam sistem penyimpanan terpusat. DEC diharapkan dapat menjaga integritas serta kredibilitas bukti digital. Peneliti yang sama mengembangkan DEC ke dalam *Digital*

2. KONSEP MODEL BPMN

Model bisnis merupakan sebuah konseptual, bukan keuangan. Konsep model bisnis ini tidak memiliki landasan teoritis di bidang ekonomi atau studi bisnis. Model bisnis menggambarkan arsitektur penciptaan nilai, pengiriman, dan mekanisme pekerjaan (Teece, 2010). Dalam model bisnis juga memuat tentang proses bisnis yang dapat ditentukan dengan BPMN. Menurut Object Management Group seperti yang dikutip oleh Rosing, White, Cummins, & Man (2015) BPMN merupakan standar untuk pemodelan proses bisnis yang menyediakan notasi grafis untuk menentukan proses bisnis yang terjadi dalam Business Process Diagram (BPD). BPMN menyediakan cara untuk berkomunikasi tentang proses bisnis bagi personil manajemen, analisis bisnis, dan pengembang sehingga memudahkan untuk mendefinisikan dan menganalisis proses bisnis umum maupun pribadi. Terdapat 3 kategori elemen utama dari BPMN, yaitu; *flow objects*, *connecting objects*, *swimlanes*

Forensics Business Model berdasarkan pada mekanisme yang terjadi selama proses investigasi. Model terdiri dari tiga bagian, yaitu penanganan bukti digital yang berkaitan dengan orang atau pelaku, bagian penyimpanan dan dokumentasi (*chain of custody*) untuk akses bukti digital, dan bagian dari kegiatan utama forensik digital, yaitu; eksplorasi, analisis, dan presentasi temuan. Terdapat keterkaitan antara orang, bukti digital, dan proses yang terjadi. Penggunaan model bisnis tersebut disebabkan adanya penafsiran yang beragam dari kegiatan forensik digital di lapangan dan kegiatan penanganan bukti digital dengan mempertimbangkan interaksi dari semua objek yang terlibat (Prayudi et al., 2015). Pendekatan model bisnis dapat menerangkan orang yang terlibat, peran dari orangnya, dan interaksi yang terjadi antara orang dengan proses forensik digital sehingga menjadikan pemahaman tahapan forensik digital lebih utuh (Prayudi et al., 2015). Model forensik digital tersebut sudah dikembangkan berdasarkan model bisnis, akan tetapi belum menggunakan metode standar dalam pemodelannya, dan salah satu metode yang dapat diterapkan adalah BPMN.

(Object Management Group (OMG), 2016). BPMN dirancang untuk pemodelan proses bisnis dan menciptakan bisnis proses *end-to-end*. Terdapat 3 sub-model dalam BPMN (Von Rosing, Von Scheel, & Scheer, 2014), yaitu:

- a. Proses (*orchestration*) termasuk di dalamnya;
  - Proses Bisnis *Private non-executable (internal)*, Model yang digunakan untuk organisasi tertentu. Proses bisnis ini dimodelkan untuk dieksekusi menurut eksekusi semantik BPMN.
  - Proses Bisnis *Private executable (internal)*, Proses pribadi (organisasi tertentu) yang dimodelkan untuk mendokumentasikan perilaku proses pada tingkat *modeler*.
  - Proses Bisnis Publik (*public process*), Model yang digunakan untuk menggambarkan interaksi ke dan dari proses lain atau

participant. Proses publik dapat dimodelkan secara terpisah atau dimodelkan dalam kolaborasi untuk menunjukkan arah aliran dari sebuah pesan.

- b. Koreografi (*choreography*), Merupakan kegiatan interaksi yang mewakili satu set atau lebih dari pertukaran pesan yang melibatkan dua atau lebih *participants*.
- c. Kolaborasi (*collaboration*), Model yang menggambarkan interaksi antara dua atau lebih entitas bisnis. Dalam model ini biasanya terdiri dari dua *pools* atau lebih yang mewakili *participant* dari kolaborasi tersebut. Pertukaran pesan antar *participant* ditunjukkan dengan arus pesan yang menghubungkan antara dua *pools* atau objek di dalamnya. Kolaborasi dapat berupa gabungan dari dua atau lebih proses *public* atau *private*. Diantara *pools* dimungkinkan untuk

ditampilkan elemen koreografi karena hal ini membagi

antara dua arus pesan antar *pools*.

Kolaborasi dapat berisi kombinasi *pools*, proses, dan koreografi. BPMN bukan digunakan untuk model data, akan tetapi untuk menunjukkan aliran data atau pesan serta

asosiasi artefak data kegiatan. Aturan bisnis, laporan, tabel keputusan, dan dukungan pengambilan keputusan tidak termasuk dalam BPMN. Ruang lingkup BPMN tidak memberikan kemampuan untuk pemodelan enterprise, manajemen kinerja, dan arsitektur enterprise. (Rosing et al., 2015). Secara singkat, BPMN ini sebuah metode yang digunakan untuk menggambarkan proses bisnis dalam bentuk diagram yang menyerupai flowchart sehingga mudah dipahami oleh semua bagian yang terlibat di dalam proses bisnis dengan penjelasan aktifitas yang dilakukan menggunakan kata kerja.

3. ALUR UMUM PROSES FORENSIKA DIGITAL

Bagian ini menjelaskan tentang forensika digital. Tujuan umum forensik yang dikemukakan oleh Kent, Chevalier, Grance, & Dang (2006) adalah untuk mendapatkan pemahaman dari suatu peristiwa dengan cara menemukan dan menganalisa fakta-fakta yang terkait dengan peristiwa tersebut. Ketergantungan dunia dengan teknologi menjadikan forensik digital mempunyai peran penting (Sammons, 2014). Kejahatan yang terjadi akan meninggalkan barang bukti, berupa bukti elektronik maupun bukti digital (Raditio, 2014). Barang bukti tersebut harus memenuhi lima karakteristik penting, yaitu; *Admissible, Authentic, Complete, Reliable, Believable* (Richter, Kuntze, & Rudolph, 2010). Menurut Sammons (2014) terdapat prinsip-prinsip umum yang perlu diterapkan untuk mendukung seluruh proses forensik, yaitu:

- a. Mempertahankan bukti asli
- b. Melakukan dokumentasi secara lengkap, rinci, dan menyeluruh atas apa yang telah dilakukan. Dokumentasi ini dapat berupa foto, catatan tertulis, sketsa, dan video. Catatan dalam dokumentasi harus memuat rincian tentang siapa, apa, di

mana, kapan, dan bagaimana dari segala yang didokumentasikan.

- c. *Chain of Custody*, merupakan bagian dari dokumentasi berupa serangkaian pencatatan yang dimulai dari awal pengumpulan bukti hingga kasus resmi ditutup. Kunci dari *chain of custody* ini adalah keamanan dari penyimpanan barang bukti. Sehingga bukti tidak dapat diubah, dicuri, atau dirusak.
- d. Validasi, memastikan bahwa alat, teknik, prosedur yang dilakukan tepat dan memberikan hasil yang konsisten serta dapat diandalkan.
- e. *Quality assurance*, Jaminan kualitas atas keakuratan hasil yang diperoleh dari proses yang dilakukan.

Jejak yang ada dari lingkungan digital dapat berupa *log file, key registry*.

Forensika digital merupakan penerapan ilmu pengetahuan yang digunakan untuk identifikasi, pengumpulan, pemeriksaan, dan melakukan analisis data dengan tetap menjaga integritas informasi dan *chain of custody* (Kent et al., 2006). Penjelasan proses forensik digital menurut NIST (2006) adalah sebagai berikut:

- a. *Collection*, merupakan tahap pertama yang harus dilakukan untuk mengidentifikasi sumber data yang

relevan. Cara mendapatkan data harus mengikuti pedoman dan prosedur supaya integritas data tetap terjaga. Pelabelan dan pencatatan termasuk dalam tahap ini.

- b. *Examination*, tahap pemeriksaan, pengolahan data yang telah dikumpulkan dengan mengkombinasikan metode manual dan otomatis. Dalam tahap ini harus tetap menjaga integritas data yang diperoleh.
- c. *Analysis*, tahapan melakukan analisis hasil pemeriksaan (*examination*) dengan menggunakan metode yang benar secara teknik dan hukum yang berlaku untuk memperoleh informasi. Dalam melakukan analisis harus dibuat salinan file supaya data asli yang menjadi barang bukti tidak rusak. Menyalin file ini dapat dilakukan dengan dua teknik, yaitu; *logical backup* dan *bit stream imaging*. Teknik dengan *Logical backup* tidak termasuk dalam menyalin file yang

telah dihapus atau residual data yang di simpan di dalam *slack space*. Teknik *bit stream imaging* akan menghasilkan salinan media asli bit-to-bit, termasuk *free space* dan *slack space*, untuk menyalin *disk-to-disk* atau *disk-to-file*. (Kent et al., 2006).

- d. *Reporting*, berupa tahap laporan hasil analisis yang memuat tindakan, prosedur, alat yang digunakan, menentukan tindakan lain jika diperlukan, dan memberikan rekomendasi untuk perbaikan kebijakan dari proses forensik yang dilakukan. Tahap ini sangat bervariasi, tergantung dari situasi yang sedang dialami. Secara singkat, forensik digital merupakan bagian dari investigasi untuk menyelesaikan sebuah kasus, baik berupa kasus *cybercrime*, *computer crime*, ataupun *computer-related crime* untuk mengungkap bukti dari kejahatan tersebut dengan tetap mempertahankan integritas bukti yang diperoleh.

4. PENGEMBANGAN DESAIN BPMN

Penelitian ini menggunakan paradigma *design science research* atau penelitian desain. Penelitian ilmu desain sangat relevan untuk penelitian *Information System* (IS) karena membahas dua isu utama, berupa peran artefak IT dalam penelitian IS (Weber, 1987; Orlikowski & benbasat & Zmud, 2003) dan kurangnya relevansi professional dalam penelitian IS (Benbasat & Zmud, 1999; Hirschheim & Klein 2003) seperti yang dikutip dalam (Antonelli, Mathew, Hevner, Chatterjee, & Series, 2010). Desain sebagai penelitian meliputi gagasan untuk melakukan desain inovatif yang menghasilkan kontribusi berupa pengetahuan. Bentuk dari pengetahuan tersebut berupa konstruksi, model, metode, dan *instantiations* (Maret & Smith, 1995) dikutip oleh Antonelli, Mathew, Hevner, Chatterjee & Series (2010). Hasil penelitian desain akan mencakup penambahan atau ekstensi untuk teori asli dan metode yang dilakukan selama penelitian, artefak baru; yaitu produk desain dan proses. Penelitian desain harus memberikan

kontribusi pengetahuan, bukan hanya berupa desain rutin berdasarkan penerapan proses. Penelitian desain mempunyai tujuh pedoman, yaitu; desain sebagai artefak, relevansi masalah, desain evaluasi, kontribusi penelitian, ketegasan peneitian, desain sebagai penelusuran proses, dan komunikasi penelitian. (Antonelli et al., 2010). Metodologi penelitian menggunakan *Design Science Research Methodology* (DSRM) (Peppers, Tuunanen, & Rothenberger, 2008) yang ditampilkan di dalam Gambar 1, dengan pembuatan alur model terinspirasi dari Fathul & Sein (2013).

Gambar 1. Metodologi Penelitian Desain

BPMN (*Business Process Model and Notation*) merupakan metode yang

digunakan untuk menjelaskan proses bisnis dalam bentuk *flowchart*, namun dengan

notasi khusus. Sedangkan forensik digital merupakan bagian investigasi kasus yang terdiri dari empat proses dasar. BPMN dan forensik digital mempunyai kesamaan yang berorientasi pada proses. Diperlukan cara yang tepat untuk menghubungkan BPMN dengan forensika digital, yaitu dengan melakukan desain dan pengembangan dari artefak tersebut. Seperti yang dikatakan oleh Peffers, Tuunanen, & Rothenberger (2008) bahwa kegiatan ini meliputi

penentuan fungsi yang diinginkan dari artefak dan arsitektur yang kemudian menciptakan aktual artefak. Langkah pertama dari desain dan pengembangan ini adalah mengulas elemen-elemen yang terdapat di dalam BPMN. Dalam tulisan ini hanya memaparkan elemen yang dapat dikaitkan dengan forensika digital. Keterangan mengenai elemen-elemen tersebut dapat dilihat pada Tabel 1 (Rosing et al., 2015).

Tabel 1. Elemen Business Process Diagram Dalam BPMN

No.	Kategori elemen	Nama elemen	Bentuk elemen	Fungsi
1.	Flow Objects	Activities		Untuk menunjukkan pekerjaan atau aktifitas yang dilakukan. Aktifitas ini dapat berdiri sendiri atau membentuk gabungan. Terdiri dari <i>task</i> dan <i>sub-process</i>
		Gateway		Untuk mengontrol percabangan atau penggabungan dari <i>sequence flow</i> dengan tujuan menentukan keputusan yang akan dilakukan dalam sebuah proses. <i>Gateway</i> mempunyai kontrol perilaku yang berbeda.
		Event		Suatu hal yang terjadi selama proses berlangsung. <i>Event</i> mempengaruhi aliran proses yang mempunyai penyebab (<i>trigger</i>) dan hasil.
		Trigger		Jenis-jenis <i>Trigger</i> .
2.	Connecting Objects			Untuk menghubungkan <i>flow objects</i> dengan membentuk aliran proses, dengan posisi arah anak panah menunjukkan arah proses
3.	Data Objects			Sebagai input atau ouput untuk proses kegiatan, dapat mewakili benda tunggal atau kelompok. <i>Data Store</i> , terjadinya proses membaca dan menulis data, contoh: database, lemari arsip
4.	Artefacts			<i>Artefactss text annotation</i> untuk menambahkan informasi dalam model proses. <i>Group</i> , untuk pengelompokan kategori yang sama. <i>Artefacts</i> tidak mempengaruhi aliran proses.
5.	Swimlanes			<i>Pool</i> merupakan representasi dari <i>participant</i> dalam model kolaborasi. <i>Lane</i> , sub-bagian dari pool. <i>Swimlanes</i> ini untuk mengatur <i>flow objects</i> dalam kategori beragam yang mempunyai fungsi serupa. Dapat dibentuk secara <i>horizontal</i> atau <i>vertical</i>

langkah berikutnya adalah melakukan pemodelan. Untuk melakukan pemodelan ini diawali dengan membuat *start event*, elemen

flow objects yang berupa lingkaran. Gunakan *connecting objects* yang berupa *sequence flow* untuk menghubungkan *start event*

dengan *activities*. Elemen *activities* ini bagian dari *flow object* yang berbentuk persegi tanpa siku, terdiri dari berbagai elemen *task* dengan fungsi yang berbeda untuk digunakan sesuai dengan kondisi. Setiap proses yang terjadi dapat memiliki sub-proses yang berisi aktifitas lain, yang berupa penjabaran dari proses utama. Untuk membuat percabangan aliran atau keputusan dimodelkan dengan *gateway*. Semua aliran proses yang terjadi diakhiri dengan elemen *end event*. Pemodelan yang kompleks dapat menggunakan jenis model kolaborasi (*collaboration*), sebuah pemodelan yang menggunakan *swimlanes*. Di dalam *swimlanes* ini terdiri dari *pools* dan *lane* untuk menunjukkan *participant*. Selanjutnya, pemodelan menggunakan *business process diagram* ini dapat dikembangkan sesuai dengan kebutuhan. Seperti yang dikemukakan oleh Rosing, White, Cummins, & Man (2015) bahwa BPMN memiliki fleksibilitas untuk pengembangan semua contoh proses bisnis.

Langkah selanjutnya adalah mengidentifikasi proses yang terjadi dalam forensik digital. Empat tahapan dasar telah dijelaskan dibagian alur umum proses forensik digital, Gambar 2 berikut ini merupakan skema dari

tahapan forensik digital tersebut (Kent et al., 2006).

Gambar 2. Proses Forensik

Proses forensik yang dikemukakan oleh NIST tersebut dikembangkan dari sudut pandang IT bukan dari penegak hukum. Sebuah proses yang dilakukan untuk mendapatkan data dari media yang kemudian diolah untuk memperoleh informasi sehingga dapat dijadikan bukti. Istilah bukti ini mempunyai arti luas dan spesifik yang dilihat dari perspektif hukum. Bukti dari perspektif hukum berarti suatu hal yang digunakan dalam pengadilan. Proses forensik tersebut dapat digunakan oleh analis forensik sistem, jaringan, administrator keamanan, dan para peneliti untuk pengembangan *framework* investigasi forensik digital yang sesuai dengan kebutuhan. Model yang dikembangkan mempunyai prinsip dasar yang sama dari proses dasar forensik dengan aktifitas yang berbeda-beda, seperti yang ditunjukkan dalam Tabel 2.

Tabel 2. Aktifitas Setiap Proses Forensik Digital

No.	Proses forensik digital	Aktifitas	Keterangan
1.	Collection (Pengumpulan Data)	• Mengidentifikasi kemungkinan sumber data	Contoh sumber data : media penyimpanan internal dan eksternal, perangkat digital portable, aktifitas jaringan, dan sistem operasi
		• Mendapatkan, Mengumpulkan data	• Melakukan akuisisi data • Memperoleh data volatile maupun non-volatile • Verifikasi integritas data (nilai hash, MD5 atau SHA-1) dari data asli dan hasil akuisisi (salinan data)
		• Pertimbangan respon insiden	Mengisolasi sistem yang bersangkutan, memutuskan jaringan kabel, mencabut listrik, memastikan host, meningkatkan keamanan fisik
2.	Examination (Pemeriksaan)	• Memeriksa kemungkinan enkripsi data, kompresi data, dan mekanisme akses kontrol • Mengekstraksi potongan informasi yang relevan dengan data yang diperoleh	• Mengidentifikasi file data yang berisi informasi menarik

Menggunakan bantuan alat
forensik (*forensics toolkit*)

3.	Analysis (Analisis)	Analisis forensik bertugas mempelajari dan menganalisis data untuk mendapatkan Kesimpulan Mengidentifikasi orang, tempat, • kegiatan, acara dan mengkaitkan antar elemen tersebut sehingga dicapai sebuah Kesimpulan	Dapat menggunakan bantuan alat forensik (<i>forensics toolkit</i>)
4.	Reporting (Pelaporan)	• Melakukan proses penyusunan dan penyajian informasi yang dihasilkan dari tahap analisis dengan mempertimbangkan penjelasan alternatif, pertimbangan informan (contoh: penegak hukum), dan menindaklanjuti informasi.	

Sebuah proses forensik digital terkait dengan manusia, pengguna, *user*, atau aktor, yaitu subjek yang melakukan sebuah kegiatan. Dalam elemen BPD Tabel 1 tersebut juga telah dijabarkan tentang elemen *activities* yang berfungsi untuk mendeskripsikan aktifitas atau kegiatan yang dilakukan. Penjabaran aktifitas dalam

elemen *activities* harus menggunakan kata kerja. Aktifitas dapat dilakukan dengan bantuan sistem atau tanpa sistem. Dalam forensik digital terdapat aktor yang terlibat dalam proses forensik, baik secara langsung maupun tidak langsung, yang ditunjukkan dalam Tabel 3 sebagai berikut;

Tabel 3. Aktor yang Terlibat Dalam Forensik Digital

No.	NIST (2006)	Ćosić & Ćosić (2012)		
1.	Penyidik (Investigator)	Responden Pertama	Penegak Hukum	Tersangka
2.	Profesional IT	Investigator Forensik	Petugas Polisi	Orang yang melewati TKP
3.	Incident Handlers	Saksi Ahli Pengadilan	Korban	

Aktor-aktor tersebut mempunyai tugas yang berbeda dalam proses forensik digital. Dalam model bisnis forensik digital yang pernah diteliti oleh Prayudi, Ashari, dan Priyambodo (2014) menyebutkan bahwa orang yang terlibat dalam kegiatan forensik digital adalah responden pertama, petugas, dan penegak hukum. Dalam hal tersebut investigator forensik dapat menjadi bagian dari penegak hukum. Responden pertama dan *incident handlers* mempunyai peran yang

sama. Menjadi orang yang pertama kali menangani sebuah peristiwa. Penemuan peristiwa dilanjutkan dengan pencarian sumber data. Pemeriksaan dapat dilakukan oleh investigator forensik, penegak hukum, polisi dan dibantu oleh profesional IT. Investigator forensik juga dapat berperan sebagai analis forensik. Tetapi peran ini juga dapat dipegang khusus oleh analis forensik. Bahkan, investigator forensik ini juga menjadi penanggungjawab dalam penyajian dan pelaporan mengenai bukti

yang diperoleh. Setiap ahli forensik harus mempunyai keahlian yang beragam. Hal ini berguna untuk ketepatan dalam penyelesaian peristiwa yang terjadi.

5. HASIL DAN DISKUSI

Empat tahap forensik digital tersebut apabila dikaitkan dengan BPMN dapat dimodelkan berdasarkan proses dan interaksi yang terjadi. Untuk pemodelannya menggunakan sub-model *process* atau *orchestration* dan sub-model *collaboration*. Sub-model *orchestration* dipilih karena dapat memodelkan interaksi yang terjadi dalam setiap tahap forensik digital. Pemodelan dapat dilihat pada Gambar 3. Terlihat elemen *sub-process activities* yang digunakan untuk menerangkan empat tahap dasar dari forensik digital. Pemodelan diawali dengan penggunaan *star event* sebagai tanda dimulainya proses forensik digital. Untuk menunjukkan arah proses digunakan elemen *sequence flow*, yang berupa garis dengan anak panah di ujungnya. Arah anak panah menunjukkan aktifitas lanjutan yang akan dilakukan. *Sequence flow* ini digunakan untuk menunjukkan aliran proses dari elemen *start event* menuju ke elemen *sub-process* pertama, yaitu tahap pengumpulan data. Pemilihan untuk menggunakan elemen *sub-process* ini karena dari tahap utama forensik digital tersebut masih terdapat aktifitas lain yang harus dilakukan. Dalam elemen *sub-process* terdapat tanda plus (+) dibagian bawah, hal ini menunjukkan bentuk penyederhanaan dari aktifitas-aktifitas yang ada di dalam tahap pengumpulan data tersebut. Aktifitas dapat diuraikan untuk menunjukkan rincian dari tahap pengumpulan data. Akan tetapi, rincian aktifitas tersebut tidak dijelaskan dalam

Korban, tersangka, dan orang yang melewati TKP (tempat kejadian perkara) menjadi aktor yang terlibat secara tidak langsung dalam proses forensik digital.

pemodelan. Karena tujuan dari pemodelan ini hanya untuk melihat keterkaitan forensik digital dengan BPMN, bukan untuk pengembangan *framework* forensik digital.

Tahap berikutnya adalah pemeriksaan yang juga menggunakan elemen *sub-process*. Untuk menunjukkan aliran proses antara elemen *sub-process* dengan *sub-process* juga digunakan *sequence flow*. Dilanjutkan dengan tahap analisis yang juga menggunakan elemen yang sama. Elemen *sequence flow* juga digunakan untuk menunjukkan arah dari elemen *sub-process* analisis ke elemen *gateway*, yang digunakan untuk menentukan keputusan yang akan dilakukan selanjutnya dari tahap yang sedang berlangsung. Apabila data yang sudah dikumpulkan dan dianalisis tetapi belum mencukupi, maka proses forensik digital akan kembali ke tahap pengumpulan data untuk mencari data pendukung. Untuk menunjukkan aliran dari elemen *gateway* menuju ke elemen *sub-process* pengumpulan data juga digunakan *sequence flow*. Setelah dilakukan analisis dan data sudah mencukupi untuk memperoleh informasi, maka dilanjutkan menuju tahap pelaporan yang juga menggunakan elemen yang sama. Untuk mengakhiri proses forensik digital ini digunakan elemen *end event* yang berbentuk lingkaran dengan garis tebal. Dalam menunjukkan aliran dari *sub-process* pelaporan menuju ke *end event* proses forensik digital juga digunakan *sequence flow*.

Gambar 3. Pemodelan Proses Forensik Digital dengan BPMN Sub-Model *Orchestration*

Pengembangan model selanjutnya menggunakan sub-model *collaboration*. Sub-model ini dipilih karena mampu

mengambarkan interaksi yang terjadi antara entitas-entitas yang ada dalam forensik digital. Pemodelan dilakukan

dengan membuat aktor yang terlibat dalam forensik digital menjadi *participant* dalam *pool* yang berbeda. Digunakan aktor yang terlibat secara langsung dalam proses tersebut. Sehingga didapatkan pemodelan dengan sub-model *collaboration* di Gambar 4. Pemodelan ini dapat menjelaskan interaksi yang terjadi antara aktor dan aktifitas yang dilakukan selama proses forensik digital berlangsung. Dalam hal ini aktor berperan sebagai subjek, yang melakukan aktifitas dalam aliran proses. Untuk pengembangan model, peran sebagai subjek ini tidak harus manusia, tetapi juga dapat benda, aturan, informasi, data, organisasi, atau sistem.

Pemodelan dengan sub-model *collaboration* ini dibagi menjadi dua *pool*, yaitu responden pertama dan investigator forensik. Setiap *pool* mewakili *participant* yang berperan menjadi aktor yang terlibat langsung dalam proses forensik digital. *Start event* proses digital forensik dimulai dari responden pertama yang melakukan tahap pengumpulan data (*collection*). Hal ini menunjukkan interaksi yang terjadi antara aktor dan aktifitas yang dilakukan. Elemen *activities* yang digunakan dalam *pool* ini adalah elemen *task* tanpa kondisi khusus. Sehingga dapat menyesuaikan aktifitas yang dilakukan dalam proses forensik digital. Dalam tahap pengumpulan data terdiri dari dua aktifitas, yaitu menemukan sumber data dan melakukan akuisisi dari data yang telah ditemukan. Kedua proses ini terpisah dan berada dalam elemen *activities* yang berbeda.

Penunjukkan arah aliran proses yang terjadi dari kedua *activities* tersebut menggunakan *sequence flow*, sama seperti yang digunakan dalam elemen *sub-process*. Untuk memperjelas bahwa dua elemen *task* tersebut merupakan satu kesatuan tahap pengumpulan data, maka digunakan elemen *group* yang termasuk dalam elemen *artefacts*. Group ini berfungsi untuk mengkategorikan aktifitas yang serupa. Penggunaan group ini tidak mempengaruhi aliran proses dari *sequence flow*. Setelah akuisisi data diselesaikan maka langkah berikutnya adalah memeriksa data hasil akuisisi untuk mendapatkan informasi yang relevan dengan peristiwa yang sedang

ditangani. Kedua proses tersebut merupakan bagian dari tahap pemeriksaan (*examination*) yang dilakukan oleh investigator forensik. Karena investigator forensik ini berada dalam *pool* yang berbeda maka aliran proses selanjutnya menggunakan elemen *message flow*.

Elemen *message flow* ini digunakan untuk menunjukkan aliran pesan dari *participant* responden pertama menuju *participant* investigator forensik. Kedua *participant* tersebut diwakili dengan *pool* dalam sebuah pemodelan. Dari elemen *task* akuisisi data *participant* responden pertama dikirimkan menuju *participant* investigator forensik untuk melakukan aktifitas pemeriksaan hasil akuisisi data. Setelah mendapatkan informasi yang sesuai dengan fakta yang terjadi, maka proses dilanjutkan ke tahap analisis. Pemodelan tahap ini juga menggunakan elemen yang sama, yaitu elemen *activities* berupa *task* tanpa kondisi tertentu dengan *sequence flow* sebagai penunjuk arah aliran proses. Dalam tahap ini dilakukan peninjauan informasi yang diperoleh.

Untuk menentukan proses yang akan dilakukan berikutnya digunakan elemen *gateway* yang berfungsi sebagai penentu keputusan. Apabila data yang diperlukan belum mencukupi, maka proses akan kembali ke tahap pengumpulan data. Kedua elemen tersebut juga berada dalam *pool* yang berbeda, sehingga untuk menunjukkan aliran prosesnya digunakan *message flow* untuk menyampaikan pesan yang berupa membutuhkan data pendukung lain. Apabila data sudah mencukupi untuk dijadikan bukti maka proses dilakukan menuju tahap pelaporan yang berupa penyajian dan penyampaian informasi yang diperoleh untuk menyelesaikan kasus atau peristiwa yang terjadi. Saat proses forensik digital telah diselesaikan, maka ditunjukkan dengan *end event* yang ditunjukkan dengan aliran proses menggunakan *sequence flow*. Elemen yang digunakan untuk pemodelan dalam Gambar 3 dan Gambar 4 hampir sama. Perbedaan terletak dalam penggunaan penunjukkan aliran proses. Apabila aliran proses terjadi dalam satu *pool* yang sama, maka digunakan *sequence flow*. Jika aliran proses berada dalam *pool* yang berbeda digunakan *message*

flow, yang berupa garis putus-putus dengan berikutnya.
arah anak panah sebagai tujuan proses

Gambar 4. Pemodelan Proses Forensik Digital dengan BPMN Sub-Model Collaboration

Pemodelan Gambar 3 dan Gambar 4 menerangkan hubungan antara BPMN dengan tahap dasar dari forensik digital. Pemodelan Gambar 3 menjelaskan tentang proses yang terjadi dalam setiap tahap yang terjadi dalam forensik digital. Sedangkan, Gambar 4 menerangkan tentang interaksi antara aktor (*participant*) dengan aktifitas yang dilakukan selama proses forensik digital. Dengan didapatnya kedua model tersebut membuktikan bahwa *Business Process Diagram* (BDP) dari BPMN dapat diterapkan untuk pemodelan dalam forensika digital. Temuan ini dapat

dikembangkan untuk pengembangan *framework* investigasi forensik digital yang disesuaikan dengan kebutuhan, hukum, dan peraturan yang berlaku.

Langkah selanjutnya berupa demonstrasi dari temuan artefak yang akan diterapkan pada *framework* Model Bisnis Digital Forensik yang dikembangkan oleh Prayudi, Ashari, dan Priyambodo (2014) di Gambar 5. Model forensik digital ini sudah menggunakan pendekatan bisnis, akan tetapi belum menerapkan metode BPMN. Oleh sebab itu, dalam tulisan ini akan digunakan sebagai contoh demonstrasi.

Gambar 5. Model Bisnis Forensik Digital Tanpa BPMN

Model Bisnis Forensik Digital pada Gambar 6 didesain menggunakan metode BPMN dengan sub-model *collaboration*. Dalam pemodelannya dilakukan penambahan beberapa aktifitas untuk memperjelas proses

yang terjadi tanpa mengurangi atau meniadakan esensi dari Model Bisnis Forensik Digital tersebut. Dalam model ini terdiri dari empat *pool* yang merupakan representasi dari *participant* yang terdiri dari

orang (aktor), bukti digital, *digital evidence cabinets* (sistem penyimpanan bukti digital), dan *frameworks* atau kerangka kerja pengolahan data. Bagian *pool* untuk orang terdiri dari tiga *lane*, yaitu petugas, responden pertama, dan investigator atau penegak hukum. *Lane* ini merupakan sub-bagian dari *pool* yang digunakan untuk mengkategorikan jenis dari aktor atau orang yang berkaitan dalam proses tersebut. *Start event* proses forensik digital dimulai dari responden pertama yang dimulai dengan aktifitas memeriksa dan mengamankan tempat kejadian perkara. Proses selanjutnya adalah mencari sumber data. Dalam model ini sumber data terbagi menjadi dua, yaitu bisa mendapatkan sumber data secara *offline* maupun *online*. Untuk menentukan sumber data ini dilakukan pencabangan keputusan menggunakan gateway. Elemen yang digunakan dalam model ini sama dengan elemen yang digunakan untuk membuat model di Gambar 4 dengan penambahan beberapa elemen untuk lebih memperjelas proses yang terjadi. Saat pencarian data memilih sumber *offline*, maka akan ditemukan bukti digital elektronik yang selanjutnya disimpan dalam tas bukti. Aliran proses ini berada dalam satu *pool* yang sama, namun berada di dalam *lane* yang berbeda. Untuk menunjukkan aliran proses dari *lane* yang berbeda, namun masih berada dalam satu *pool* ini digunakan *sequence flow*. Selanjutnya dari bukti elektronik yang didapat di simpan dalam rak bukti fisik yang ditangani oleh petugas. Apabila sumber data yang dicari berbentuk *online*, maka proses selanjutnya adalah melakukan akuisisi secara langsung. Proses akuisisi ini juga dilakukan dalam pencarian sumber data *offline*. Sub-bagian dari *pool* orang yang lainnya adalah investigator atau penegak hukum yang bertanggungjawab dalam melakukan pemeriksaan. Investigator ini dapat mengakses *digital evidence cabinets* atau mengakses bukti digital yang diperoleh. Semua proses akhir dari *pool* orang dengan ketiga *lane* tersebut menuju ke bagian *pool* bukti digital. Untuk menunjukkan aliran dalam proses ini digunakan *message flow*. Karena untuk menghubungkan antara elemen

activities dengan *pool* hanya dapat menggunakan *message flow*. Dalam *pool* bukti digital ini tidak terjadi aktifitas di dalamnya. Sebab *pool* ini hanya digunakan untuk menunjukkan interaksi yang terjadi antara orang dan komponen lain yang terlibat dalam Model Bisnis Forensik Digital. Bagian dari *lane* investigator atau penegak hukum ketika memilih untuk mengakses *digital evidence cabinets*, maka akan meneruskan prosesnya untuk masuk ke akses kontrol dari sistem penyimpanan buktidigital tersebut. Aktifitas yang terjadi di dalam *pool* "*digital evidence cabinets*" ini dimodelkan dengan elemen *activities* dengan aliran proses menggunakan *sequence flow*. Bagian akhir dari aktifitas dalam *pool* ini adalah menyimpan data yang didasarkan dari *chain of custody* ke dalam penyimpanan bukti digital yang dimodelkan dengan elemen *data store*. Di dalam *data store* ini akan terjadi proses untuk menyimpan dan membaca data. Kedua elemen dihubungkan menggunakan *association* dengan kondisi anak panah berada di kedua ujungnya. Hal ini menunjukkan arah aliran berada di kedua elemen. Selanjutnya, terdapat aliran proses dari *pool* bukti digital menuju ke elemen *activities* dari eksplorasi. Untuk menunjukkan aliran dari *pool* menuju *flow objects* berupa *activities* juga digunakan *message flow*. Bahkan *message flow* ini juga digunakan untuk menunjukkan aliran dari *pool* atau *lane* menuju ke *pool*. Hal ini dapat dilihat dari *lane* investigator atau penegak hukum menuju ke *pool framework*. Dalam *pool framework* ini terdapat proses yang dilakukan untuk mengolah data, yang dimulai dari tahap eksplorasi bukti yang diperoleh dilanjutkan dengan analisis dan diakhiri dengan pelaporan atau presentasi. Aktifitas dalam *pool framework* ini dilakukan oleh investigator atau penegak hukum. *End event* dari proses forensik digital ini berada di dalam *pool framework*. Karena penyelesaian dari tahap forensik digital ini adalah melaporkan dan mempresentasikan informasi yang diperoleh, sehingga dapat dijadikan bukti untuk menyelesaikan sebuah kasus atau peristiwa

6. KESIMPULAN

Hasil desain menggunakan sub-model *orchestration* dan *collaboration* dari empat tahap dasar forensik digital dengan BPMN membuktikan bahwa diagram bisnis terdapat keterkaitan dan dapat diaplikasikan untuk membangun model forensik digital. Walaupun kedua hal tersebut bukan berada dalam lingkungan yang sama. Akan tetapi, dua hal tersebut dapat disatukan untuk membentuk sebuah model yang dapat menjelaskan interaksi antara proses yang satu dengan proses yang lain. Selanjutnya, juga berguna untuk menjelaskan interaksi yang terjadi antara aktor atau subjek dengan aktifitas yang dilakukan selama proses forensik berlangsung. Pemodelan dengan BPMN dapat menjelaskan komponen-komponen yang terkait dalam proses forensik

digital. Temuan ini juga bersifat umum untuk forensika digital. Sehingga, BPMN dapat dikembangkan untuk *framework mobile forensics*, *network forensics*, bahkan *database forensics*.

Tulisan ini mempunyai batasan, yaitu tidak membahas tentang pembuatan *framework* forensik digital. Hanya menerapkan BPMN pada *framework* yang telah dikembangkan oleh peneliti sebelumnya sebagai langkah demonstrasi dari temuan artefak. Selain itu, desain dan pengembangan artefak tidak dilakukan pada sub-model *choreography*. Sehingga keterbatasan ini dapat dijadikan penelitian di masa depan. Selain itu, dapat dilakukan untuk pengembangan *framework* investigasi forensik digital dengan metode BPMN.

DAFTAR PUSTAKA

- Antonelli, P., Mathew, R., Hevner, A., Chatterjee, S., & Series, I. (2010). Design Science Research in Information Systems, 9–23.
- Ćosić, J., & Ćosić, Z. (2012). Chain of Custody and Life Cycle of Digital Evidence. *Computer Technology and Application*, 3(2012), 126–129.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, (August), 800–886.
- Object Management Group (OMG). (2016). BPMN Specification - Business Process Model and Notation. Retrieved February 2, 2017 from www.bpmn.org/
- Peffer, K. E. N., Tuunanen, T., & Rothenberger, M. A. (2008). A Design Science Research Methodology for Information Systems Research, 24(3), 45–77.
- Prayudi, Y., Ashari, A., & K Priyambodo, T. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1–8.
- Prayudi, Y., Luthfi, A., & Pratama, A. M. R. (2014). Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody. *Cybermatika ITB*, 2(2), 36–43.
- Raditio, R. 2014. *Aspek Hukum Transaksi Elektronik Perikatan, Pembuktian, dan Penyelesaian Sengketa*. Yogyakarta. Graha Ilmu.
- Richter, J., Kuntze, N., & Rudolph, C. (2010). Securing digital evidence. *5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010*, (September), 119–130.
- Rosing, M. Von, White, S., Cummins, F., & Man, H. De. (2015). *Business Process Model and Notation-BPMN. The Complete Business Process Handbook*. Elsevier Inc.
- Sammons, J. (2014). Digital Forensics. *Introduction to Information Security*, 275–302.
- Sutiyoso, B. 2015. *Manajemen, Etika & Hukum Teknologi Informasi*. Yogyakarta. UII Press.
- Symantec. (2016). *Symantec's Internet Security Threat Report*.
- Teece, D. J. (2010). Business models, business strategy and innovation. *Long Range Planning*, 43(2–3), 172–194.
- Von Rosing, M., Von Scheel, H., & Scheer, A. W. (2014). *The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM* (Vol. 1).