DIGITAL FORENISCS READINESS UNDERSTANDING AND SIMPLE IMPLEMETATION

Ewaldo Simon Hiras, Teguh Hariyono, Rizka Muliana, Dano Norama Dista, Ian Nurseto
Direktorat Penegakan Hukum Direktorat Jenderal Pajak Kementerian Keuangan
subditfbb@pajak.go.id

Mei 2020

Abstract

This research introduces the concept of digital forensic readiness through academic principles and frameworks. The research began with an academic definition of digital forensic readiness and a glance at the forerunners in various countries and the costs and benefits of its application. Furthermore, based on these academic principles and frameworks practical steps can be formulated that can be directly applied to improve information security posture by focusing on the digital forensic readiness of an organization

Keywords: digital forensic, digital forensic readiness, cost and benefit, implementation

Abstrak

Penelitian ini mengenalkan konsep *digital forensic readiness* melalui prinsip dan kerangka akademis. Penelitian ini dimulai dengan definisi akademis *digital forensic readiness* dan selayang pandang penerepan di berbagai negara serta *cost and benefit* penerapannya. Lebih jauh, berdasarkan prinsip dan kerangka akademis tersebut dirumuskan langkah praktis yang dapat langsung diterapkan untuk memperbaiki postur keamanan informasi dengan berfokus pada *digital forensic readiness* dari sebuah organisasi

Kata kunci: forensik digital*, digital forensic readiness,* biaya dan manfaat, implementasi

I. PENDAHULUAN

Pada era revolusi industri 4.0 yang terjadi sekarang, data digital menjadi suatu kebutuhan yang penting bagi semua entitas. Pada bulan April 2020 tercatat hampir 4,57 milyar atau 60 persen penduduk di dunia aktif menggunakan data digital (J.Clement, 2020). Dunia tanpa data digital adalah sesuatu yang tidak dapat dibayangkan sekarang sehingga entitas perlu memiliki kemampuan untuk memanajemen data digitalnya dengan tepat dan aman sesuai dengan ketentuan yang berlaku untuk mencapai tujuan.

Pentingnya data digital dan besarnya manfaat yang diberikan kepada suatu entitas tentu memunculkan suatu risiko. Tidak sedikit perusahaan yang gulung tikar atau dituntutnya pemerintah di suatu negara karena data digital. Kasus yang terjadi pada HMRC (*Her Majesty's Revenue and Customs*) di UK dimana terjadi peretasan 25 juta data wajib pajak membuat Pemerintah mereformasi besar-besaran *information security*. Di Indonesia sendiri, tidak lama ini telah terjadi kasus peretasan data digital beberapa *market place* terbesar di Indonesia seperti Bukalapak dan Tokopedia. Penting menyadari bahwa selain data digital memberikan manfaat, data digital juga mengandung risiko didalamnya yang harus dikelola dalam manajemen keamanan siber.

Pelaku peretasan atau penyalahgunaan data digital dapat dijatuhi hukuman sesuai aturan yang berlaku. Namun yang menjadi *bottleneck* adalah menemukan siapa pelakunya dan membuktikannya. Grobler (2007) menggambarkan rendahnya tingkat kesuksesan penegakan hukum dalam konteks keamanan siber melalui survey di Amerika Serikat pada tahun 2006 dimana hanya terdapat 25% insiden siber yang dilanjutkan dengan proses litigasi, sedangkan 70% hanya dilakukan *patching* pada sistem informasi yang terpengaruh. Grobler berpendapat rendahnya tingkat penegakan hukum pada sebuah insiden siber, salah satunya, disebabkan oleh rendahnya kapabilitas untuk memanfaatkan bukti berupa data digital atau biasa kita sebut dengan kemampuan *digital forensic*.

Kegiatan *digital forensic* sering terletak setelah kejadian atau *post incident* yang dilaksanakan setelah insiden terjadi dan seringkali digunakan dalam *root cause analysis* untuk menemukan *root cause* dari sebuah insiden siber, ataupun kejadian lain yang melibatkan data digital. Tingginya penggunaan data digital dan tingginya pertumbuhan jumlah insiden siber yang terjadi serta rendahnya tingkat keberhasilan penegakan hukum pada sebuah insiden siber disebabkan rendahnya kemampuan *digital forensics.* Tan (2001) memperkenalkan *digital forensic readiness framework* untuk memaksimalkan penggunaan data digital demi meningkatkan keberhasilan *digital forensic investigation* dan meminimalkan biaya *digital forensic investigation* apabila terjadi insiden.

Pentingnya *digital forensic readiness* selain memaksimalkan fungsi dan meminimalkan biaya dari *digital forensic investigation, digital forensic readiness* juga merupakan bagian yang tidak terpisahkan dari konsep keamanan sistem informasi (Grobler, 2007). Berbagai negara menyarankan untuk menerapkan *digital forensic readiness* untuk keamanan sistem informasi, bahkan di UK diwajibkan sebagai *mandatory requirement* suatu entitas (S. Park et al., 2018). Indonesia mulai menerbitkan aturan terkait data digital seperti Undang-Undang ITE, Peraturan Pemerintah Penyelenggaraan Sistem dan Transaksi Elektronik, dan Rancangan UU Perlindungan Data Pribadi yang menyebutkan bahwa perlunya menyelenggarakan keamanan sistem informasi terkait data digital yang dimiliki entitas. Oleh karena itu,

pentingnya memahami *digital forensic readiness* selain untuk keamanan sistem informasi juga untuk mematuhi ketentuan yang berlaku.

II. TINJAUAN PUSTAKA

Secara umum, *digital forensic readiness* merupakan kesiapan dari sebuah entitas untuk memanfaatkan data digital yang dimilikinya ketika dibutuhkan. Walaupun tidak secara gamblang disebutkan dengan menggunakan istilah *forensic readiness*, konsep kesiapan menggunakan data digital telah beberapa kali disebutkan dalam beberapa penelitian. Tan (2001) salah satu yang paling pertama menggunakan istilah *digital forensic readiness*, menggambarkan bahwa *digital forensic readiness* memiliki dua tujuan utama, yaitu memaksimalkan penggunaan data digital dan meminimalkan biaya investigasi digital forensik apabila terjadi insiden.

Yasinsac dan Manzano (2002) menyebutkan bahwa sebuah institusi yang bergantung kepada data digital, ataupun *network* harus memiliki perhatian yang seimbang antara *security* dan kapabilitas digital forensik. Lebih jauh Yasinsac dan Manzano menggambarkan beberapa skenario yang dapat berujung pada insiden siber, dan langkah-langkah untuk memaksimalkan penggunaan data digital apabila insiden siber dalam skenario tersebut terjadi. Walaupun tidak secara gamblang menyebutkan kebijakan tersebut sebagai *forensic readiness*, namun secara konsep merupakan hal yang serupa dengan *digital forensic readiness*.

Carrier dan Spafford (2003) menggunakan istilah *readiness phases* dalam model investigasi forensik yang dikemukakan. *Readiness phases* menyebutkan perlunya kesiapan operasional dan infrastruktur dalam mendukung sebuah investigasi forensik. Kesiapan operasional lebih mengarah kepada kesiapan sebuah organisasi dalam melaksanakan operasi atau kegiatan digital forensik (ketersediaan peralatan, personil, dan sebagainya). Kesiapan infrastruktur yang disampaikan Carrier dan Spafford, menggambarkan ketersediaan data digital untuk dapat dimanfaatkan dalam *digital forensic investigation*.

Endicott-Popovsky et al. (2007) memiliki konsep *network forensic readiness* dengan definisi memaksimalkan kemampuan suatu lingkungan untuk mengumpulkan bukti digital yang kredibel sembari meminimalkan biaya *incident response*. Secara sederhana, *digital forensic readiness* adalah konsep untuk mendukung *digital forensic investigation*.

Grobler (2007) secara lebih gamblang mendefinisikan *digital forensic readiness*, sebagai bagian yang tidak terpisahkan dari konsep keamanan sistem informasi. Grobler membagi forensik digital menjadi reaktif dan proaktif. Forensik digital reaktif adalah *digital forensic investigation* yaitu penggunaan sains dan teknologi dalam investigasi untuk *preservation, identification, extraction, documentation, analysis and interpretation* media komputer yang disimpan secara digital untuk pembuktian dan rekonstruksi tindak pidana kriminal di pengadilan. Sementara *digital forensic readiness* merupakan forensik digital proaktif yang didefinisikan sebagai keyakinan atas keseluruhan proses bisnis atas data digital yang dimiliki untuk dimanfaatkan demi menjamin kesuksesan *digital forensic investigation* pada insiden siber.

Trenwith (2013) menyoroti penggunaan *digital forensic investigation* pada lingkungan *cloud*. Beberapa persoalan yang utamanya ditemukan dalam konteks *digital forensic investigation* pada lingkungan *cloud* antara lain yurisdiksi dan ketersediaan akses data. Ketersediaan akses data digital, menurut Trenwith, dapat diatasi dengan *digital forensic readiness* khususnya sentralisasi log. Sentralisasi log menjamin ketersediaan akses data ketika terjadi insiden, sehingga tidak lagi menjadi hambatan dalam melakukan digital forensik.

III. PEMBAHASAN

A. Selayang Pandang *Digital Forensic Readiness* di UK, US, EU, South Korea, dan Indonesia

Pada bagian ini kita akan membicarakan tentang latar belakang, ketentuan perlindungan data digital, dan *legal requirement* yang mendasari penerapan *digital forensic readiness* di berbagai negara

The United Kingdom (UK)

Sejak tahun 1900an UK sudah mengimplementasikan sistem keamanan informasi melalui Security Policy Framework (SPF). Namun semenjak terjadinya insiden kebocoran data 25 juta wajib pajak dari HMRC (Her Majesty's Revenue and Customs) pada tahun 2007, UK mewajibkan *digital forensic readiness* sebagai standar minimum keamanan sistem informasi untuk semua instansi pemerintahan melalui HMG Security Policy Framework.

Sementara untuk sektor swasta, UK mengimplematasikan *digital forenisc readiness* sebagai *best practice* keamanan sistem informasi. UK menyadari betapa pentingnya *digital forensic readiness* untuk keamanan sistem informasi dan kesuksesan forensik digital.

The United States (US)

US belum memiliki satu aturan tunggal yang komprehensif sebagai dasar ketentuan perlindungan data digital. Berbagai macam aturan terkait perlindungan data digital diatur oleh berbagai ketentuam seperti SOX terkait keuangan, HIPPA terkait kesehatan, HITECH terkait kesehatan teknologi dan informasi. Pemerintah federal US sendiri juga sudah mengimplenyasikan sanksi apabila terjadi pelanggaran penggunaan data digital (Zurich, 2010) terbukti berbagai kasus sukses memaksa perusahaan yang mengalami kebocoran data untuk membayar kompensasi seperti kasus kebocoran data perusahaan Sony (Tsotsis, 2014). Tidak semua insiden kebocoran data ditindaklajuti dengan denda apabila dapat dibuktikan melalui *digital forenics investigation* bahwa perusahaan tidak bersalah.

US telah mulai mengintegrasikan *digital forensic readiness* dengan keamanan sistem informasi untuk mencegah terjadinya penyalahgunaan data digital. Ketentuan tersebut dituangkan melalui *guidance* yang dibuat oleh NIST, dan SOX section 404 dan 802. Melihat dukungan dari pemerintah US terkait forensik digital, tinggal menunggu waktu *digital forensic readiness* ditetapkan menjadi standar minimum keamanan sistem informasi di US seperti yang dilakukan di UK.

European Union (EU)

Berdasarkan Genaral Data Protection Regulation (GDPR) mulai tahun 2018 entitas tertentu perlu mengimplementasikan sistem perlindungan data digital, apabila tidak patuh maka akan didenda sebesar 10juta Euro dan apabila merupakan entitas tertentu maka dapat didenda mencapai 20juta Euro. Oleh karena itu di EU, pemenuhan *digital forensic readiness* menjadi prioritas karena tertuang sebagai persyaratan minimal dalam GDPR pasal 32 terkait forensik digital dalam sistem keamanan informasi.

South Korea

South Korea merupakan negara dengan koneksi internet tercepat dengan lalu lintas data digital yang luar biasa besar. Insiden kebocoran data yang terjadi pada perusahaan LG pada tahun 2004 membuat publik marah karena kebocoran data tersebut dalam selang waktu yang tidak terlalu lama dengan kebocoran data LG sebelumnya. Desakan publik kepada pemerintah yang menuntut untuk meningkatkan regulasi perlindungan data pribadi beserta denda yang menyertai membuat berbagai aturan diterbitkan untuk meningkatkan keamanan

sistem informasi berikut *digital forensic readiness* untuk membantu kesuksesan penegakan hukum apabila terjadi kebocoran data. Aturan tersebut mengikat berbagai perusahaan terutama perusahaan Payment Card Industry (PCI).

Indonesia

Indonesia merupakan salah satu negara pengguna internet terbesar di dunia, hampir 64 persen penduduknya menggunakan internet, lalu lintas data digital di negara inipun sangat tinggi. Tingginya data digital di Indonesia tentu memunculkan risiko penyalahgunaan data digital. Tercatat pada awal tahun 2020 terjadi berbagai insiden pencurian data digital oleh para hacker dari beberapa market place ternama seperti tokopedia, bukalapak, dan bhinneka.

Regulasi terkait perlindungan data digital sebenarnya sudah diatur sejak tahun 2012 melalui Peraturan Pemerintah (PP) Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang kemudian diubah melalui PP nomor 71 Tahun 2019 tentang PSTE dimana pada pasal 11 mewajibkan penyelenggara sistem elektronik menjamin keamanan informasi dan komunikasi data digital, apabila tidak menjalankan maka pada pasal 100 perusahaan dapat dikenakan sanksi administratif dan denda berdasarkan Undang-Undang. Senada dengan Permen Kominfo nomor 20 tahun 2016 yang mewajibkan penyelenggara sistem elektronik untuk menjaga kerahasiaan data pribadi, apabila terbukti gagal maka akan dikenaik sanksi administratif dan denda juga berdasarkan Undang-Undang. Undang-Undang tersebut sampai dengan jurnal ini dibuat masih dalam tahap Rancangan Undang-Undang tentang Perlindungan Data Pribadi.

Berdasarkan hal tersebut bahwa sudah terdapat regulasi yang mengatur tentang perlidungan data pribadi termasuk data digital yang dikelola oleh penyelenggara sistem elektronik melalui kewajiban penjaminan keamanan sistem informasi beserta sanksi dan denda yang menyertai apabila melanggar atau gagal menyelenggarakannya. Hal tersebut menjadi penting untuk diketahui karena setidaknya sudah terdapat regulasi apabila terjadi insiden.

Arah regulasi perlindungan data pribadi sudah seperti perkembangan berbagai negara sehingga dipandang perlu untuk *sounding* terkait *digital forensics readiness* di Indonesia. Di US apabila dapat dibuktikan melalui *digital forensics investigation* kalau kebocoran data digital disebabkan bukan karena lemahnya keamanan sistem informasi, maka insiden tersebut ditindaklajuti melalui *patching.* Oleh karena itu, pentingnya *digital forensics readiness* untuk meningkatkan keberhasilan forensik digital dalam insiden siber. Harapan kedepan *digital forensics readiness* dapat ditetapkan sebagai standar minimum untuk keamanan sistem informasi seperti yang dilakukan di UK ataupun di EU dan South Korea yang wajib untuk entitas tertentu.

B. Cost and Benefit

Pentingnya *digital forensic readiness* dikemukakan oleh Rowlingsons (2004), dengan menyoroti sisi *cost* dan *benefit*-nya, ketersediaan data digital dari permulaan penanganan insiden yang menjamin kegiatan investigasi dapat dilaksanakan secara proporsional dengan ukuran insidennya. *Digital forensic readiness* juga dapat meminimalkan biaya (dan waktu) pada pelaksanaan investigasi digital forensik. Lebih jauh, Rowlingsons juga menggarisbawahi *digital forensic readiness* yang dapat menjamin ketersediaan data digital juga memastikan proses bisnis dapat terus berjalan tanpa perlu terganggu oleh kegiatan *digital forensics investigation*. Rownlingsons juga menambahkan *digital forensic readiness* dapat berfungsi sebagai *detterent effect* bagi pihak internal.

1. Cost

Reddy dan Venter (2013) mengungkapkan bahwa *cost* (biaya) merupakan aspek penting dari *digital forensics readiness* karena manajemen forensik digital biasanya bekerja dengan anggaran terbatas. Anggaran tersebut digunakan relatif terhadap risiko. Dengan kata lain, semakin besar risiko maka semakin besar anggaran yang digunakan. Prioritas pertama dalam penggunaan anggaran adalah pada risiko dalam hal terdapat potensi kerugian dan paling dimitigasi dalam penggunaan bukti digital (Rowlingson, 2004).

Rowlingson juga menjelaskan bahwa biaya penerapan *digital forensic readiness* mungkin tinggi, terutama dalam organisasi dengan proses manajemen keamanan sistem informasi yang belum matang. Namun, biaya tersebut dapat dikurangi secara signifikan jika organisasi telah melakukan penilaian risiko yang komprehensif, menerapkan rencana kesinambungan bisnis, dan telah memberikan materi terkait integrasi *digital forensic readiness* dengan keamanan sistem informasi pada setiap bagian ke dalam pelatihan staff.

2. Benefit

Digital forensics readiness jelas memberikan benefit yang besar kepada organisasi, dari berbagai benefit yang ditawarkan, berikut tiga benefit utama *digital forenisc readiness*

Enhance Digital Forensics Investigation

Tan (2001) menjelaskan bahwa *digital forensic readiness* memiliki dua tujuan utama yaitu memaksimalkan penggunaan data digital dan meminimalkan biaya investigasi digital forensik apabila terjadi insiden. Senada dengan Grobler (2007) yang menjelaskan bahwa *digital forensic readiness* merupakan bentuk forensik digital proaktif yang memberikan keyakinan atas keseluruhan proses bisnis baik dari manajemen puncak sampai detail teknis sistem infotmasi dimana data digital yang dimiliki dapat dimanfaatkan untuk menjamin kesuksesan *digital forensic investigation* pada insiden siber yang terjadi.

Improve Information Security

Grobler (2007) menjelaskan bahwa *digital forensic readiness* merupakan bagian yang tidak terpisahkan dari konsep *information security*. Grobler membagi hubungan forensik digital dengan *information security* menjadi reaktif dan proaktif. *Digital forensic investigation* merupakan forensik digital reaktif karena dilakukan setelah terjadi insiden terhadap *information security.* Sementara *digital forensic readiness* merupakan forensik digital proaktif yang senantiasa terintegrasi dengan *information security*.

Melihat berbagai penuntutan terkait kejadian siber di US, Grobler menjelaskan bahwa arsitektur *information security* di US pada umumnya masih belum cukup untuk mensukseskan penuntutan di pengadilan karena lemahnya bukti digital dan prosedur yang kurang dapat dipercaya dari *digital forensic investigation* sehingga entitas tidak dapat membuktikan bahwa sebenarnya *information security* sudah efektif dan efisien. Penerapan *digital forensic readiness* memberikan *guidelines* untuk mengintegrasikan digital forensik dengan *information security* pada setiap tahap seperti *legal guidance* dalam logging data dan memonitor aktivitas pengguna sistem meggunakan *information security* sehingga secara langsung *digital forensic readiness* memberikan peningkatan kualitas dari *information security* suatu entitas.

Penerapan *digital forensic readiness* melalui integrasi *information security* memberikan kesiapan kepada entitas apabila terjadi insiden siber sehingga *digital forensics investigation* yang dilakukan dapat mengumpulkan bukti yang cukup dan handal dengan biaya minimal tanpa mengganggu proses bisnis secara keseluruhan.

Legal Requirement

Salah satu tujuan utama suatu entitas menerapkan *digital forensic readiness* adalah kewajiban dari suatu ketentuan atau *legal requirement.* Kewajiban penerapan *digital forensic readiness* di UK menjadi prioritas karena merupakan suatu persyaratan yang tertuang pada HMG Security Policy FrameworkUK pasal 37 yang mewajibkan *digital forensic readiness* sebagai standar minimum keamanan sistem informasi untuk semua instansi pemerintahan. Kemudian di EU melalui General Data Protection Regulation (GDPR) nomor 32 dimana entitas perlu mengimplementasikan digital forensik kedalam sistem perlindungan data digital, apabila tidak patuh maka akan didenda. South Korea juga mewajibkan *digital forensic readiness* untuk industri tertentu seperti *Payment Card Industry* (PCI).

Indonesia sudah mulai menerbitkan regulasi yang mengatur tentang perlidungan data pribadi dan kewajiban penjaminan keamanan sistem informasi beserta sanksi dan denda yang menyertai apabila melanggar atau gagal menyelenggarakannya. Rancangan Undang-Undang Perlindungan Data Pribadi juga sudah ada yang mengatur sanksi dan denda didalamnya. Arah regulasi sudah seperti perkembangan berbagai negara sehingga dipandang perlu untuk *sounding* terkait *digital forensics readiness* karena melalui keberhasilan *digital forensics investigation* dapat meningkatkan kualitas pengambilan putusan hukum ketika terjadi sengketa inseden siber. Harapan kedepan *digital forensics readiness* dapat ditetapkan sebagai standar minimum untuk keamanan sistem informasi seperti yang dilakukan di UK ataupun di EU dan South Korea yang wajib untuk entitas tertentu.

IV. STUDI KASUS

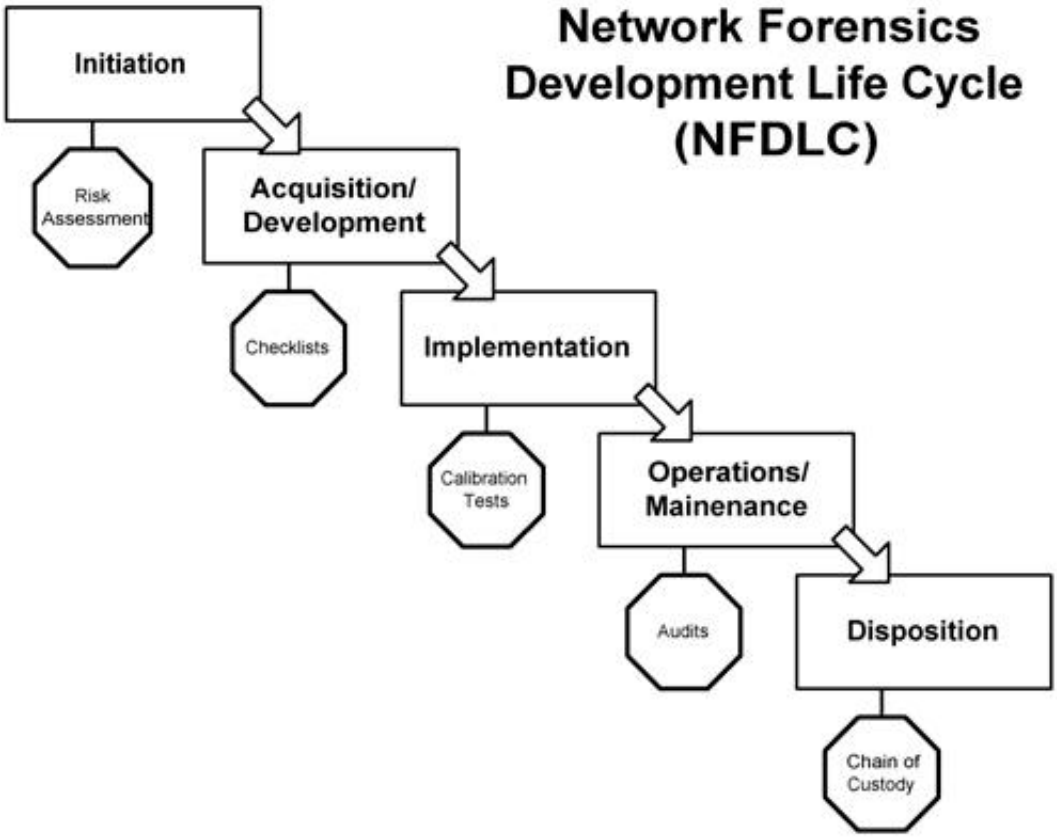
SIMPLE PRACTISES IN IMPLEMENTING DIGITAL FORENSIC READINESS

Pada bagian ini setelah membahas berbagai macam literatur dan penerapan *digital forensic readiness* di berbagai negara di bagian sebelumnya, berikut bagaimana konsep dan langkah yang harus ditempuh untuk menerapkan *digital forensic readiness.*

Digital Forensic Readiness Principle

Endicott-Popovsky et al. (2007) mengadaptasi 4R *Strategies of Accountable Systems* sebagai suatu kebijakan untuk menerapkan *digital forensic readiness* yang harus diadopsi oleh organisaisi dalam hal terjadi peningkatan penuntutan kejahatan siber. 4R yaitu *Resistance* (kemampuan untuk mengusir serangan)*, Recognition* (kemampuan untuk medeteksi serangan atau penyelidikan dan kemampuan untuk bereaksi/beradaptasi selama serangan)*, Recovery* (memberikan layanan penting selama serangan dan mengembalikan layanan setelah serangan)*,* dan *Redress* (kemampuan untuk meminta pertanggungjawaban penyusup di pengadilan dan kemampuan untuk membalas serangan).

Mengadopsi model strategi 4R memberikan dasar konseptual untuk mengembangkan kebijakan jaminan informasi yang mencakup forensik digital. Implikasinya, hal tersebut memperluas tugas dari jaringan pengamanan untuk memasukkan identifikasi persyaratan forensik digital ketika mengembangkan prosedur, praktik, dan mekanisme sistem informasi. Untuk mencapai hal ini, Endicott-Popovsky et al. (2007) menawarkan metodologi *life cycle* untuk menanamkan forensik dalam sistem jaringan sebagaimana pada gambar 1 di bawah ini.

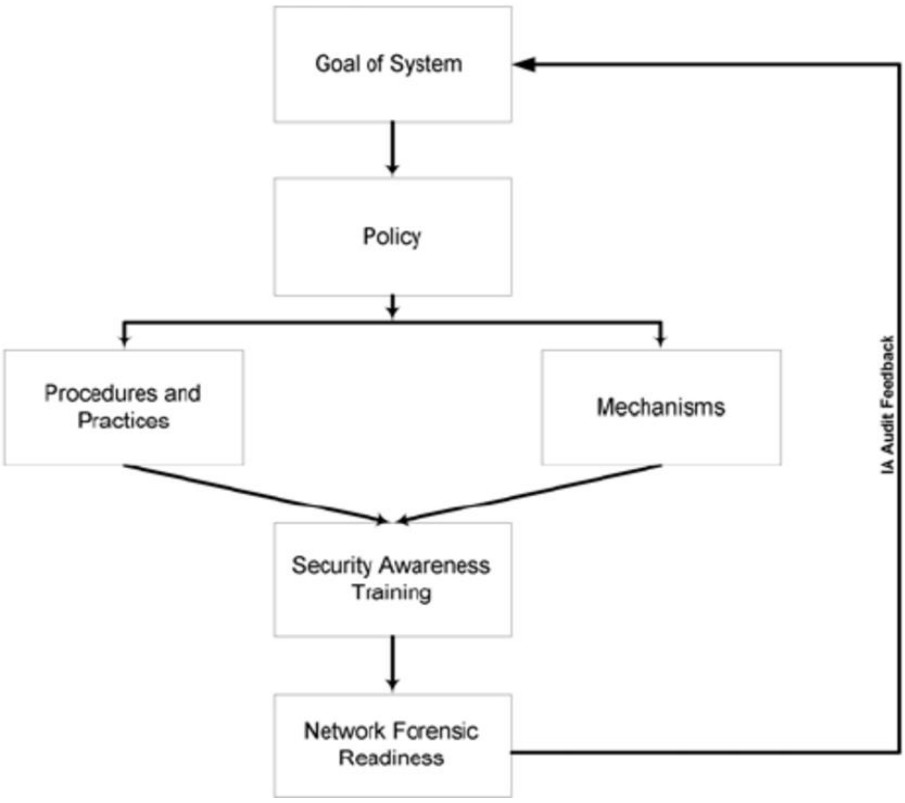


Gambar 1 NFDLC (Endicott-Popovsky et al., 2007)

1. *Initiation Phase*: menentukan aspek jaraingan apa yang akan menjamin perlindungan forensik digital (*premilinary risk assessment*).
2. *Acquisition/Development Phase*: mematuhi *Rules of Evidence* dalam persyaratan sistem dan menerapkan daftar forensik yang dipublikasikan.
3. *Implementation Phase*: melakukan pengujian awal dan melakukan uji jaringan/verifikasi mekanisme/kalibrasi.
4. *Operations/Maintenance Phase*: melakukan audit verifikasi/kalibrasi.
5. *Disposition Phase*: menggabungkan prosedur *chain of custody / preservation procedures*.

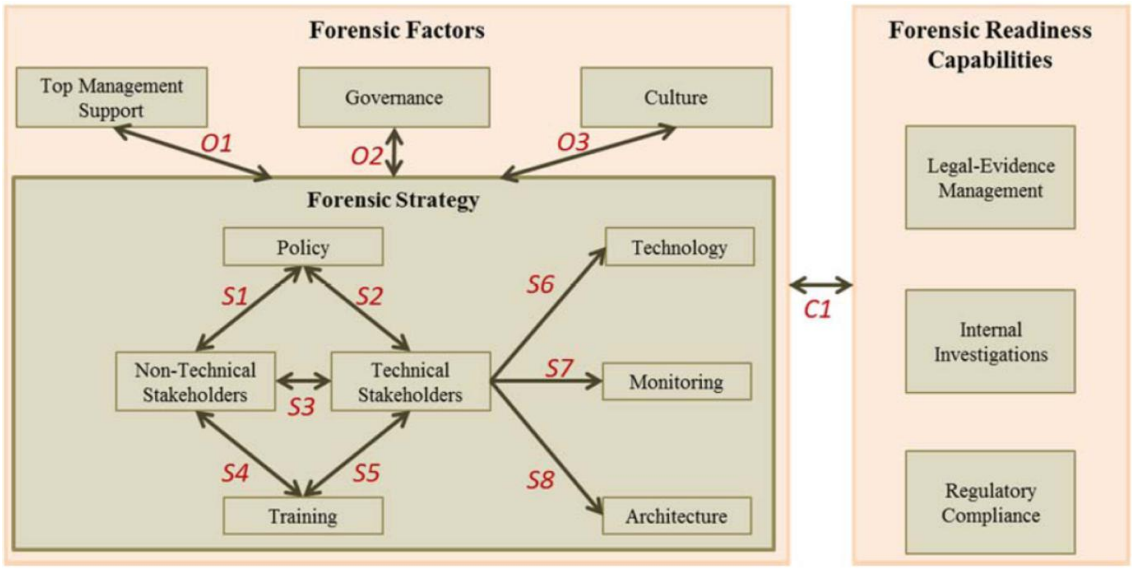
Digital Forensic Readiness Framework

Framework adalah sebuah struktur konseptual dasar yang digunakan untuk memecahkan sebuah permasalahan atau isu-isu kompleks (Daqiqil, 2011). Endicott-Popovsky et al. (2007) merumuskan suatu konseptual *framework* yang dapat menanamkan forensik digital di suatu perusahaan. *Framework* tersebut diawali dengan adanya *system goal* yang dimiliki perusahaan. *System goal* tersebut diartikan sebagai kemampuan perusahaan untuk menuntut penjahat siber sembari mengurangi biaya yang saat ini dikeluarkan untuk penyelidikan forensik digital. *System goal* tersebut mendorong *policies* (kebijakan), *procedures* (prosedur), *practices* (praktik), *mechanisms* (mekanisme), dan *awareness training* dalam pelaksanaannya. Berikut gambar *framework* tersebut.



Gambar 2 *Digital Forensics Readiness Framework* (Endicott-Popovsky et al., 2007)

Framework di atas bertujuan untuk mengarahkan pengembangan kebijakan manajemen yang tepat untuk seluruh aspek forensik, misalnya dukungan untuk menemukan bukti. Kebijakan-kebijakan tersebut kemudian dimplementasikan melalui prosedur/praktik dan/atau mekanisme yang sesuai dan selanjutnya dapat memberikan dasar *security awareness training* secara menyeluruh di perusahaan. Hal tersebut merupakan mekanisme untuk menyebarluaskan kebijakan keamanan dan instruksi bagaimana penerapannya dengan menghasilkan *network forensic readiness*. Kemudian sebagai mekanisme umpan balik, audit IA mengkomunikasikan efektivitas berbagai elemen pendukung kepada pembuat keputusan yang memiliki kewenangan untuk melakukan penyesuaian dengan tepat dan sesuai kebutuhan.



Gambar 3 *Digital Forensics Readiness Framework* (Elyas et al., 2014)

Berbeda dengan Endicott-Popovsky et al. (2007), Elyas et al. (2014) menyajikan *digital forensic readiness framework* pada organisasi terdiri dari dua bagian yaitu *forensic readiness capabilities* dan *forensic factors*. Kedua bagian tersebut saling bekerja sama untuk mencapai kesiapan forensic sebagaimana terlihat pada Gambar 3.

Tiga *forensic readiness capabilities* yang harus dimiliki oleh suatu organisasi yaitu:

a. *Regulatory Compliance*: kemampuan organisasi untuk menunjukkan kepatuhan terhadap hukum dan peraturan (memanfaatkan bukti digital dalam konteks kesiapan forensik).
b. *Internal Investigation*: kemampuan organisasi untuk menghasilkan bukti untuk memfasilitasi penyelidikan digital internal.
c. *Legal-Evidence Management*: kemampuan organisasi untuk menghasilkan bukti yang dapat digunakan dalam proses hukum.

Selain itu, terdapat sebelas faktor utama yang diidentifkasi mempengaruhi dan berkontribusi terhadap kesiapan forensik suatu oraganisasi. Terdapat tujuh faktor yang sangat penting dalam menyusun strategi forensik (*non-technical stakeholders, technical stakeholders, technology, monitoring, architecture, policy,* dan *training*) dan tiga faktor organisasi di luar program forensik yang mempengaruhi pengembangan dan implementasi strategi forensik (*forensic culture, top management support,* and *governance*). Berikut penjelasan mengenai kesebelas faktor tersebut.

a. *Forensic Strategy*: Rencana yang dapat ditindaklanjuti yang dirancang untuk mencapai kesiapan forensik dalam suatu organisasi.
b. *Non-Technical Stakeholders*: Individu dan/atau pihak tertentu, internal atau eksternal organisasi, yang tidak terlibat dalam pelaksanaan atau dukungan program forensik organisasi.
c. *Technical Stakeholders*: Individu dan/atau pihak tertentu, internal atau eksternal organisasi, yang terlibat dalam program forensik organisasi.
d. *Technology*: Perangkat lunak dan/atau perangkat keras yang mungkin diperlukan dalam program forensik.
e. *System Monitoring*: Memantau sistem (apabila terjadi anomali) untuk mendeteksi insiden secara tepat waktu.
f. *System Architecture*: Desain sistem untuk memaksimalkan potensi forensiknya.
g. *Policy*: Seperangkat prinsip tertulis yang dirancang untuk memandu dan memanipulasi perilaku dalam organisasi untuk tujuan forensik.
h. *Training*: Proses mendidik para pegawai tentang peran dan tanggung jawab mereka terhadap program forensik.
i. *Culture*: Seperangkat nilai-nilai, kepercayaan, asumsi, dan praktik yang membentuk dan mengarahkan sikap dan perilaku para pegawai ke arah kesiapan forensik.
j. *Top Management Support*: Dukungan kesiapan forensik oleh manajemen senior suatu organisasi.
k. *Governance*: Implementasi proses dan struktur dalam organisasi yang memungkinkan kegiatan forensik.

A Ten Step Process for Digital Forensic Readiness

Robert Rowlingson (2004) menjelaskan secara lebih detail bagaimana cara mencapai *digital forensic readiness* melalui *"A Ten Step Process for Forensic Readiness"* berikut

1. Tentukan proses bisnis yang membutuhkan bukti digital.

   Langkah pertama dalam *digital forensic readiness* adalah menentukan tujuan pengumpulan bukti digital. Alasannya adalah untuk mengetahui risiko dan dampaknya pada bisnis dari berbagai jenis sengketa, mengetahui ancaman terhadap bisnis, dan bagian

dari proses bisnis yang rentan. Tujuannya adalah untuk memahami proses bisnis mana dalam suatu organisasi/perusahaan yang memerlukan bukti digital.

2. Identifikasi sumber dan jenis bukti digital

Langkah kedua dalam *digital forensic readiness* bagi organisasi adalah untuk mengetahui sumber bukti yang dimiliki yang dapat dihasilkan oleh sistem dan untuk mengetahui apa yang saat ini terjadi berdasarkan data bukti yang ada. Log komputer dapat berasal dari banyak sumber (Melia, 2002). Tujuan dari langkah ini adalah untuk mengumpulkan bukti yang mungkin tersedia dari berbagai perangkat elektronik dan aplikasi yang digunakan.

3. Tentukan Persyaratan Pengumpulan Bukti

Tujuan dari langkah ini adalah untuk menghasilkan kesepakatan persyaratan pengumpulan bukti antara pihak yang bertanggung jawab untuk mengelola risiko bisnis dengan pihak yang menjalankan dan memantau sistem informasi. Persyaratan pengumpulan bukti dimoderasi oleh analisis *cost and benefit* pengumpulan bukti.

4. Menetapkan cara yang aman pengumpulan bukti yang sah secara hukum

Pada titik ini organisasi mengetahui totalitas bukti yang tersedia dan telah memutuskan cara yang dapat dilakukan untuk mengatasi risiko perusahaan sesuai anggaran yang direncanakan. Dengan memahami persyaratan pengumpulan bukti, langkah selanjutnya adalah memastikan bahwa bukti dikumpulkan dari sumber yang relevan dan dijaga keasliannya dengan melakukan pemeriksaan pendahuluan untuk memastikan bukti dapat dikumpulkan secara legal dan tanpa mengganggu proses bisnis.

Tinjauan hukum diperlukan untuk memastikan bahwa persyaratan pengumpulan bukti dapat dipenuhi dengan cara yang direncanakan. Misalnya, apakah itu melibatkan pemantauan email pribadi atau data pribadi lainnya. Di beberapa negara, beberapa atau semua kegiatan ini mungkin ilegal. Hukum yang relevan, di bidang perlindungan data, privasi, dan hak asasi manusia, mau tidak mau akan membatasi apa yang sebenarnya bisa dikumpulkan.

5. Menetapkan kebijakan penanganan dan penyimpanan bukti yang aman

Tujuan dari langkah ini adalah untuk mengamankan bukti untuk jangka panjang setelah dikumpulkan dan untuk memfasilitasi pengambilannya jika diperlukan. Hal ini menyangkut penyimpanan informasi jangka panjang yang mungkin diperlukan untuk bukti di kemudian hari. Kebijakan penyimpanan yang aman dan penanganan bukti terdiri dari langkah-langkah keamanan untuk memastikan keaslian data dan juga prosedur untuk menunjukkan bahwa integritas bukti dipertahankan setiap kali digunakan, dipindahkan, atau dikombinasikan dengan bukti baru.

6. Memastikan monitoring dan audit untuk mendeteksi dan mencegah insiden yang signifikan

Manajer bertanggung jawab untuk menjelaskan kepada pihak yang memonitoring terkait data apa yang ingin dicegah dan tindakan untuk mendeteksinya (*prevent and detection analysis*). Kebijakan "kecurigaan" yang ditetapkan membantu staf bagian monitoring memahami pemicu kecurigaan, kepada siapa melaporkan kecurigaan itu, apakah monitoring yang lebih tinggi diperlukan, dan apakah langkah-langkah keamanan tambahan harus diambil sebagai tindakan pencegahan.

Apa yang sebenarnya harus dimonitoring dan apa yang dianggap mencurigakan akan bervariasi sesuai waktu. Kebijakan kecurigaan perlu diperbarui ketika proses bisnis baru diimplementasikan, dan hubungan bisnis baru perlu dilindungi. Kebijakan tersebut

juga dipengaruhi oleh intelijen perusahaan dari ancaman yang berkembang dan modus operandi yang harus diperhatikan oleh organisasi.

7. Tentukan keadaan seperti apa yang perlu dilakukan investigasi

   Setiap peristiwa mencurigakan yang ditemukan di langkah 6 perlu ditinjau kembali. Tujuan langkah ini adalah untuk memutuskan langkah apa yang akan diambil atas kejadian yang mencurigakan dengan menetapkan kriteria penilaian pendahuluan atas dampak bisnis yang dapat dijadikan sebagai dasar untuk melakukan investigasi seperti adanya bukti dan kemungkinan potensi yang dapat merugikan organisasi.

8. Melatih staf untuk memahami bukti digital dan hukum

   Berbagai staf dapat terlibat dalam insiden keamanan komputer. Tujuan dari langkah ini adalah untuk memastikan bahwa pelatihan yang tepat dikembangkan untuk mempersiapkan staf untuk berperan sebelum, selama, dan setelah suatu insiden. Penting juga untuk memastikan bahwa setiap staf berkompeten untuk melakukan peran apa pun yang terkait dengan penanganan dan pelestarian bukti.

   Pelatihan juga diperlukan untuk memahami hubungan dan komunikasi yang diperlukan dengan organisasi eksternal yang mungkin terlibat seperti: Kepolisian, Kejaksaan, auditor internal atau eksternal, Otoritas Jasa Keuangan, Bank Indonesia, Pelanggan, pemasok, Pihak Media baik cetak maupun elektronik, dll.

9. Sajikan sebuah kasus berbasis bukti yang menggambarkan insiden dan dampaknya.

   Tujuan investigasi bukan hanya untuk menemukan pelakunya atau memperbaiki kerusakan. Investigasi harus memberikan jawaban atas pertanyaan dari berbagai pihak dan menunjukkan mengapa jawaban itu kredibel. Pertanyaan seperti siapa, apa, mengapa, kapan, di mana, dan bagaimana. Kredibilitas disediakan oleh bukti dan argumen logis. Tujuan langkah ini adalah untuk menghasilkan kebijakan yang menjelaskan bagaimana kasus berbasis bukti harus dikumpulkan. Bukti digital bisa sulit dibaca dan dipahami oleh orang awam. Dengan demikian, *file* kasus harus menunjukkan cara menyajikan bukti yang baik, misalnya menggunakan alat visualisasi dan analisis garis waktu dari insiden atau peristiwa yang mengarah padanya (Stephenson, 2003).

10. Pastikan tinjauan hukum untuk memfasilitasi tindakan dalam menanggapi suatu insiden

    Pada titik-titik tertentu selama pengumpulan *file* suatu insiden perlu ditinjau dari sudut pandang hukum dan mendapatkan nasehat hukum atas setiap tindakan. Penasehat hukum harus dapat memberi nasehat terkait kasus dan memberi saran terkait tindakan yang harus diambil. Setiap tindakan formal perlu diperhitungkan terkait biaya dan kemungkinan akhir yang baik bagi perusahaan.

Simple Implementation of Digital Forensic Readiness

Endicott-Popovsky et. al (2007) melalui *Theoretical Framework for Organizational Netfork Forensic Readiness*, menjabarkan sebuah *conceptual framework* bagi *Forensic Readiness*. Di dalam *framework* tersebut, Endicott-Popovsky et. al. mengidentifikasi tiga komponen bagi keberhasilan penerapan, yaitu *procedures and practice*s, *mechanism*, serta *training*. Salah satu tulisan yang dapat menjadi rujukan dalam merancang langkah-langkah praktis sebagai bagian dari *procedures and practice*s adalah *A Ten Step Process for Forensic Readiness* milik Rowlingsons (2004), bab ini akan memaparkan langkah-langkah dimaksud, sekaligus mencoba menjembatani teori yang sebelumnya telah dijabarkan melalui *framework* dengan praktek melalui penjabaran penerapan praktis dari *Digital Forensic Readiness*.

Rowlingsons (2004) menjabarkan sepuluh langkahnya dengan penentuan ruang lingkup dari *Digital Forensic Readiness*, yaitu dengan menentukan proses bisnis yang menghasilkan bukti digital serta identifikasi sumber digital yang tersedia. Hal ini senada dengan yang dikemukakan Endicott-Popovsky et. al. (2007) dalam tahapan awalan dari *Information System Development Life Cycle* (ISDLC), dan lebih jauh pada *Network Forensic Development Life Cycle* (NFDLC). Pada tahapan inisiasi ISDLC mensyaratkan dilakukannya asesmen resiko awalan, dan NFDLC menambahkan prosedur penentuan aset information yang menjadi fokus DFR. Secara umum tahapan awalan ini dilakukan dengan melakukan asesmen terhadap sumber data digital yang dimiliki (atau dapat dimiliki) sebuah organisasi.

Mengetahui sumber data digital yang dapat digunakan, maka Rowlingsons (2004) juga menjabarkan perlunya ditentukan syarat pengumpulan bukti, cara pengumpulan bukti yang aman dan sah di muka hukum serta kebijakan penanganan dan penyimpanan bukti yang aman. Terdapat dua soal besar yang patut menjadi perhatian pada langkah-langkah ini, yaitu efektifitas dan efisiensi.

Efektifitas berbicara mengenai bagaimana sumber data digital mampu dikumpulkan secara aman dan sah secara hukum sehingga dapat digunakan di muka pengadilan. Efektifitas, sejatinya adalah kegiatan pokok dari forensik digital sendiri. Carrier dan Spafford dalam *Getting Physicial with Digital Investigation Process* menjabarkan beberapa fase untuk menjamin efektifitas pengumpulan sumber data digital yaitu *Operations Readiness Phase* dan *Infrastructure Readiness Phase*. *Operations Readiness Phase* meliputi kegiatan pelatihan personil (yang juga termasuk dalam sepuluh langkah Rowlingsons), sedangkan *Infrastructure Readiness Phase* menjabarkan bahwa sumber data digital, selain personil, juga perlu dipersiapkan. Carrier dan Spafford menjabarkan beberapa teknik, antara lain menjamin keseragaman timestamp, serta penggunaan penyimpanan *server log* tersentralisasi dalam menjaga integritas data.

Efisiensi, berbeda dengan efektifitas, berfokus bagaimana kegiatan DFR mampu melahirkan alur kerja forensik digital yang berbiaya rendah serta tidak memakan banyak waktu. Tan (2001) dalam *Forensic Readiness*, menyampaikan penanganan *log* yang tersentralisasi diperlukan, selain untuk menjaga integritas data, juga untuk memudahkan proses akuisisi dan analisis forensik digital sehingga mengurangi *downtime* dan akhirnya menurunkan *cost*. Selain itu, sentralisasi *log* juga efisien dalam penggunaan biaya karena mengurangi perangkat yang digunakan dalam penanganan berbagai macam *log* yang berbeda.

Selain langkah-langkah tersebut, Rowlingsons (2004) juga menyampaikan beberapa langkah tambahan yang meliputi target pemantauan, pelatihan, serta Langkah-langkah yang terkait aspek hukum seperti penentuan batasan investigasi dan tinjauan hukum.

Sepuluh langkah Rowlingsons (2004) sendiri diidentifikasi pula oleh Trenwith (2013) di *Digital Forensic Readiness in the Cloud*. Trenwith menyimpulkan beberapa hal yang perlu dimiliki guna memastikan *Digital Forensic Readiness* diterapkan secara lengkap. Menurut Trenwith diperlukan *Communication Channel, Encryption, Compression, Authentication/Integrity proof, and Timestamping*. Secara garis besar serupa dengan Rownlingsons (2014), Trenwith menyempurnakan langkah-langkah Rowlingson dengan *Encryption* dan *Authentication/Integrity Proof*.

Hal-hal ini, seperti yang telah kita bahas sebelumnya, perlu diejawantahkan menjadi beberapa langkah praktis. Usulan langkah praktis tersebut, antara lain meliputi, penggunaan perangkat log dan pengiriman log yang memiliki kapabilitas *log* tersentralisasi, penggunaan pengiriman log terenkripsi, autentifikasi log, serta penggunaan perangkat yang memiliki

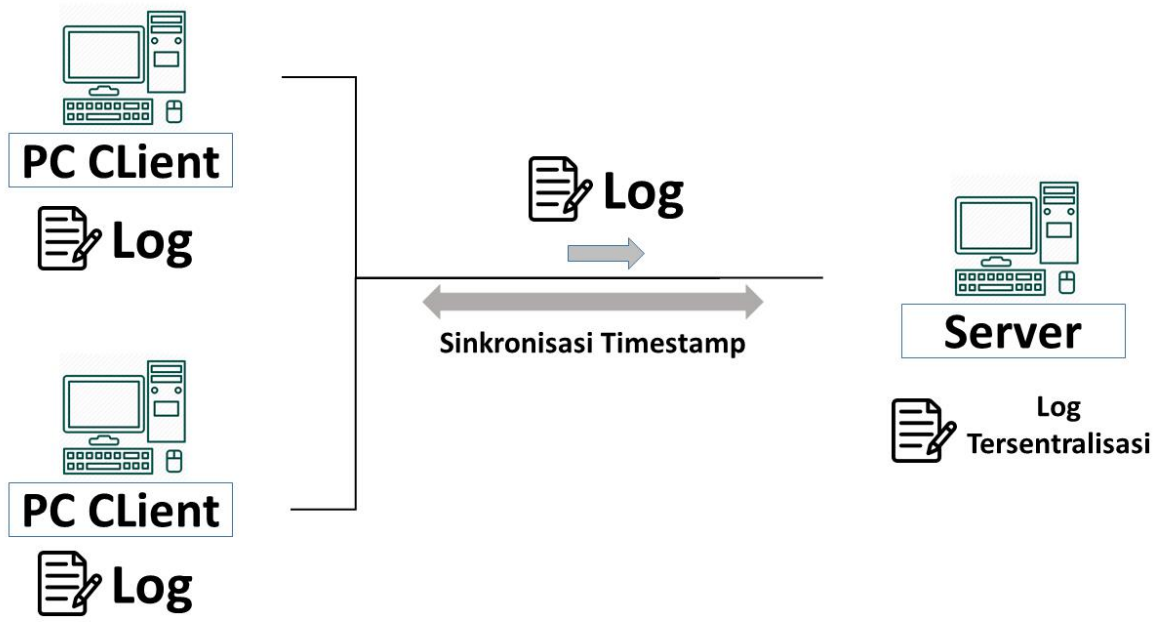
kapabilitas *timestamping*. Berikut aplikasi yang perlu digunakan untuk menerapkan secara sederhana *Digital Forensic Readiness*

Jenis Aplikasi	Kriteria	Contoh Aplikasi
Pencatat *log*	format log umum atau opensource	windows event, Linux log
log shipper	gratis atau murah mendukung enkripsi tersentralisasi	syslog-ng, rsyslog, winlogbeat, filebeat, fluentd, logstash
timestamp	-	NTP, HTP

Sedangkan infrastruktur dan sumber daya yang dibutuhkan untuk penerapan *Digital Forensic Readiness* secara sederhana adalah sebagai berikut:

1. Perangkat / komputer *client*
2. Perangkat / komputer *server*
3. Jaringan
4. SDM (Petugas yang telah dilatih untuk melakukan konfigurasi, monitoring, dan *troubleshooting*)

Skema yang akan digunakan adalah sebagai berikut:



Pembahasan:

1. DFR mengacu pada kesiapan sebuah sistem untuk dilakukan audit secara forensik. Oleh karena itu dibutuhkan sistem yang memiliki rekam jejak terhadap segala macam proses yang terjadi pada tiap-tiap perangkat di suatu perkantoran.
2. Informasi yang dapat terekam pada *log* meliputi riwayat *user login, timestamp, network*, aplikasi, dan lain-lain

3. Aplikasi pencatat log diperlukan untuk melakukan perekaman secara otomatis terhadap setiap perangkat. Pada sistem operasi Windows, aplikasi pencatat *log* telah terinstall secara *default* dengan nama Windows Event Viewer. Namun untuk keperluan kustomisasi proses apa saja yang akan dicatat, kita dapat menggunakan aplikasi tambahan seperti Sysmon.
4. Untuk kemudahan audit, dibutuhkan perangkat yang berfungsi untuk menampung seluruh *log* dari setiap client. Perangkat tersebut disebut *Log Server*. *Log Server* ini juga akan mencatat setiap proses yang terjadi pada perangkatnya sendiri.
5. *PC Client* perlu dilakukan konfigurasi agar secara otomatis mengirimkan rekaman *log* ke *Log Serve*r melalui jaringan. Syslog merupakan protokol standar yang dapat diimplementasikan untuk melakukan pengiriman *log* dalam suatu jaringan.
6. Untuk memastikan bahwa *Serve*r dan *Client* menggunakan format dan zona waktu (*timestamp*) yang sama, maka dibutuhkan protokol yang dapat mensikronisasi waktu semisal Network Time Protocol (NTP), HTTP Time Protocol (HTP), dan lain-lain.
7. Setelah semuanya terkonfigurasi, diperlukan SDM yang terlatih untuk melakukan *monitoring* dan *troubleshooting* agar menjamin keberlangsungan sistem.
8. Apabila dilakukan audit, maka auditor dapat dengan mudah melakukan penelusuran rekam jejak yang telah tercatat pada Perangkat *Log Server*, bahkan ketika ada PC Client yang mati/rusak/hilang karena *log* dari *client* telah tersentralisasi pada *Log Server*.

V. KESIMPULAN

Peningkatan penggunaan dan penyimpanan data digital tentunya akan semakin tinggi seiring dengan peningkatan penggunaan teknologi informasi. Perlindungan terhadap data digital yang disimpan (atau digunakan) oleh sebuah organisasi, akan menjadi sebuah kebutuhan bagi sebuah organisasi. Hal ini timbul dari *legal requirement* maupun kebutuhan untuk meminimalisir biaya yang terjadi dari sebuah investigasi atas insiden.

Tulisan ini telah menyajikan beberapa prinsip, teori, dan kerangka kerja seputar *digital forensic readiness*. Sebuah konsep yang sudah cukup lama dirumuskan, namun memiliki implementasi yang masih terbatas. Hal ini terjadi dikarenakan sebagian besar organisasi dan praktisi masih berfokus pada tahapan perencanaan keamanan informasi, serta berusaha mencegah terjadinya insiden, sehingga kerap melupakan apa yang perlu dilakukan seandainya insiden terjadi. Prinsip, teori, dan kerangka kerja tersebut kemudian digunakan untuk merumuskan sebuah prosedur sederhana sehingga diharapkan penerapannya pun dapat dengan mudah dilakukan.

Saran

Implementasi *Digital Forensic Readiness* (DFR) oleh Unit Kerja Kementerian Keuangan seperti Direktorat Jenderal Pajak atau Organisasi dapat memberikan manfaat secara nyata. DFR dapat memudahkan investigasi internal karena aktivitas yang dilakukan melalui perangkat elektronik kantor dapat termonitor sehingga dapat diketahui dengan bukti digital yang memadai. Investigasi yang dilakukan pun jauh lebih efisien dan efektif tanpa harus mengecek satu per satu aset teknologi informasi yang dimiliki. Pada akhirnya biaya yang dibutuhkan/dikeluarkan jadi lebih sedikit, waktu yang dibutuhkan juga semakin sedikit, dan tidak mengganggu kegiatan sehari-hari kantor/perusahaan. Monitoring terhadap aktivitas penggunaan perangkat elektronik kantor dapat dilakukan tanpa menunggu adanya laporan atau pengaduan dari suatu pihak sehingga insiden internal dapat terdeteksi sejak dini.

Selain itu, DFR juga mampu menjadi alat yang digunakan apabila terdapat insiden yang disebabkan serangan siber yang dilakukan pihak luar. Hal tersebut menjadi salah satu

alternatif mitigasi risiko yang dapat dilakukan oleh suatu organisasi. Perusahaan/organisasi lainnya dapat mengimplementasikan DFR sesuai dengan kebutuhan perusahaan/organisasi masing-masing karena memiliki karakteristik, jenis usaha, ruang lingkup usaha, skala usaha, dan gaya kepemimpinan yang berbeda antara perusahaan/organisasi yang satu dengan yang lainnya. Secara khusus, bagi DJP atau Unit Esselon 1 lain di bawah Kemenkeu yang melakukan kegiatan forensik digital kepada Wajib Pajak/perusahaan/organisasi lainnya, impelentasi DFR oleh perusahaan/organisasi lainnya memudahkan dalam melakukan kegiatan forensik digital untuk mengetahui aktivitas usaha yang sebenarnya dari perusahaan/organisasi lainnya tersebut.

Keterbatasan

Demi menjaga agar kegiatan *digital forensic readiness* ini berbiaya rendah, maka keseluruhan aplikasi yang disarankan adalah aplikasi *open source* yang gratis. Beberapa aplikasi yang disarankan tersebut memiliki level konfigurasi yang cukup tinggi agar dapat bekerja optimal. Sistem untuk mewujudkan *digital forensic readiness* yang disarankan dalam tulisan ini dibuat tanpa mempertimbangkan secara spesifik proses bisnis yang dilakukan. Sistem untuk mewujudkan *digital forensic readiness* yang disarankan menggunakan asumsi bahwa Sebagian besar proses bisnis mampu tercatat dalam sistem operasi. Terdapat kemungkinan proses bisnis yang berbeda sehingga yang tercatat dalam sistem operasi tidak cukup lengkap. contohnya sebagian besar aplikasi yang digunakan adalah web based, maka sebagian besar kegiatan *user* tidak akan terekam melalui log operating system.

Penelitian Selanjutnya

Seperti yang telah disampaikan sebelumnya, tulisan ini tidak secara rinci mempertimbangkan proses bisnis dalam merancang sistem yang disarankan. Penelitian selanjutnya dapat memilih proses bisnis yang secara khusus membutuhkan *digital forensic readiness* sehingga dapat turut dipertimbangkan dalam perancangan sistem. Kekurangan dari system yang dirancang dengan memasukkan proses bisnis dalam pertimbangan perancangan sistem *digital forensic readiness,* maka sistem yang dirancang akan sangat spesifik dan sulit diterapkan pada proses bisnis yang berbeda, namun akan sangat mudah diimplementasikan untuk proses bisnis tersebut.

Sebagian besar sistem yang disarankan berangkat dari beberapa teori, namun keseluruhannya tidak mempertimbangkan data hasil dari sistem *digital forensic ready* tidak bergantung pada aplikasi yang akan digunakan untuk melakukan pengolahan. Sehingga keseluruhan sistem yang dirancang berorientasi pada aplikasi *open source*, sehingga dapat diolah oleh berbagai macam aplikasi. Sebuah organisasi yang lebih mapan, tentunya memiliki *environment* pengolahan forensik digital dan keamanan informasi tersendiri yang berfokus pada penggunaan aplikasi tertentu dalam kegiatan pengolahan. Memasukkan *environment* pengolahan forensik digital dan keamanan informasi dapat mempengaruhi aplikasi yang dapat disarankan. Hal ini dapat menjadi sasaran penelitian lebih lanjut.

DAFTAR PUSTAKA

Alenezi, Ahmed, et al. "The Impact of Cloud Forensic Readiness on Security." *International Conference on Cloud Computing and Services Science*. Vol. 2. Scitepress, 2017.

Arrifin, A. et al. "Forensic Readiness: A Case Study on Digital CCTV Systems Antiforensics." *Elsevier : Computer and Security* (2017)

Antonis M., et al. "Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives." *IEEE*. 2013.

Antonis M., et al. "Digital Forensic Readiness: Are We There Yet." *Journal of International Commercial Law and Ttechnology*. Vol.9, No.3 , 2013.

Carrier, Brian, and Eugene H. Spafford. "Getting Physical with The Digital Investigation Process." *International Journal of digital evidence* 2.2 (2003): 1-20.

Daqiqil, Ibnu . "Framework CodeIgniter: Sebuah Panduan dan Best Practice, Pekanbaru." http://www.koder.web.id/Framework-codeignitersebuah-panduan-dan-best-practice, 2011 (diakses 30 April 2012)

Elyas, Mohamed, et al. "Digital Forensic Readiness: Expert Perspectives on A Theoretical Framework." *Elsevier : Computer and Security* (2015):70-89.

Endicott-Popovsky, Barbara, Deborah A. Frincke, and Carol A. Taylor. "A Theoretical Framework for Organizational Network Forensic Readiness." *JCP* 2.3 (2007): 1-11.

EZurich. The Liabilities of Technology Companies for Data Breaches. *JIR Article.* 2010.

Grobler, Cornelia P., and C. P. Louwrens. "Digital Forensic Readiness As A Component of Information Security Best Practice." *IFIP International Information Security Conference*. Springer, Boston, MA, 2007.

Jeroen de Wit. "Continuous Forensic Readiness." *University of twente thesis*. 2013

John Clement. "Worldwide Digital Population :Global Digital Population as of April 2020." https://www.statista.com/statistics/617136/digital-population-worldwide/, (diakses 11 Mei 2020)

K.Reddy and H.S Venter. "The Architecture of A Digital Forensic Readiness Management System." *Elsevier : Computer and Security* (2013):73-89.

Park, Sungmi, et al. "A Comparative Study on Data Protection Legislations and Government Standards to Implement Digital Forensic Readiness As Mandatory Requirement." *Fifth Annual DFRWS Europe* (2018): 93-100.

Rowlingson, Robert. "A Ten Step Process for Forensic Readiness." *International Journal of Digital Evidence* 2.3 (2004): 1-28.

Tan, John. "Forensic Readiness." *Cambridge, MA:@ Stake* (2001): 1-23.

Trenwith, Philip M., and Hein S. Venter. "Digital Forensic Readiness in The Cloud." *Information Security for South Africa*. *IEEE.* 2013.

Vidal, Chaz, et al. Cloud Security and Forensic Readiness: The Current State of an IaaS Provider. *Elsevier : Computer and Security* (2015)

Yasinsac, Alec, and Yanet Manzano. "Policies to Enhance Computer and Network Forensics." *Proceedings of the 2001 IEEE workshop on information assurance and security*. 2001.