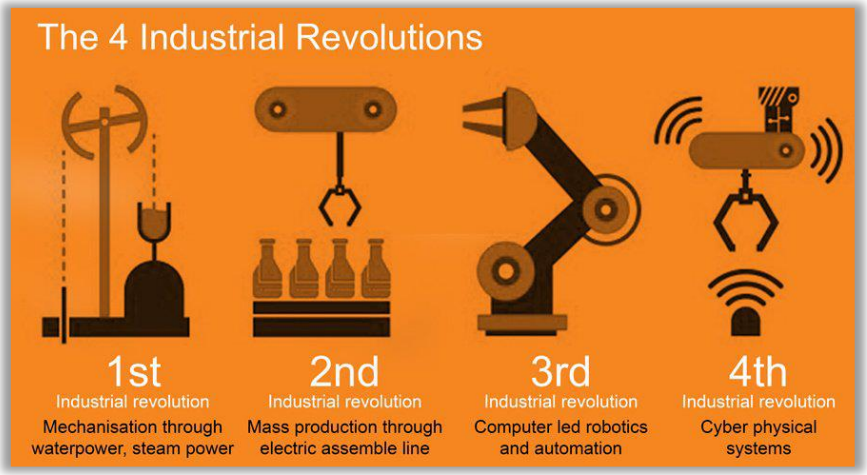
BAB 1
Pendahuluan

1.1 Latar Belakang Masalah

Adanya dorongan pemerintah untuk melaksanakan standar industri 4.0 yang mencakup penggunaan perangkat Internet Of Think (IoT) sebagai salahsatunya, hal tersebut secara tidak sadar sudah menjadi bagian dari kehidupan kita sehari-hari, adanya Peraturan Baru, meningkatnya Serangan Dunia Maya maupun meningkatnya Ketergantungan Aset Digital IT (Rahardjo, 2019) telah menyebabkan Peran adanya Forensik Digital pada Sebuah Organisasi agar lebih diperhitungkan. Oleh karena itu, Sebuah Organisasi harus siap secara Forensik Digital untuk memaksimalkan potensi mereka dalam merespon peristiwa Cyber Crime dan dapat dengan tepat menunjukkan identifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital serta bagaimana faktor-faktor ini bekerja bersama untuk mencapai kesiapan Forensik Digital dalam suatu organisasi.

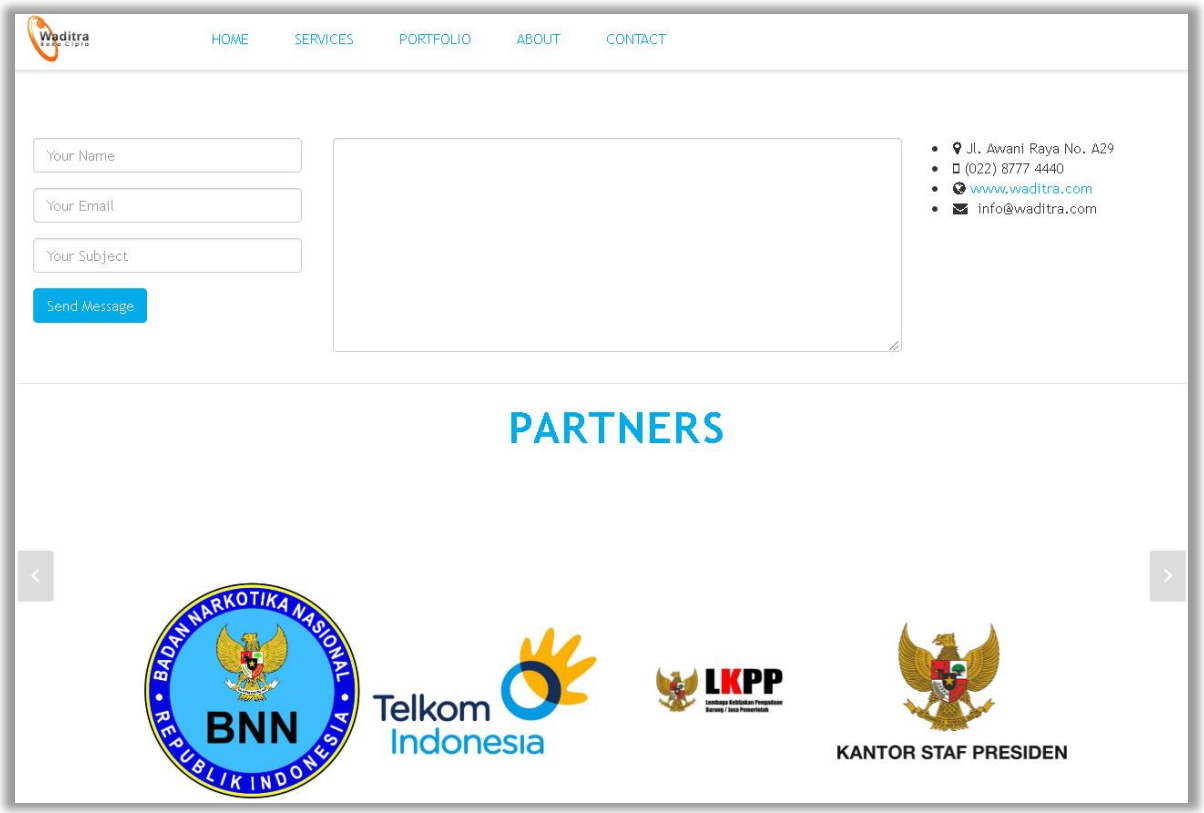


Gambar 1.1 Ilustrasi Perkembangan Industri

Meskipun Digital Forensik telah berkembang saat ini dalam menyelesaikan kasus-kasus Cyber Crime seperti carding, hacking, cracking, defacing, phising, spamming serta kejahatan lainnya yang berbasis digital, tetapi masih memerlukan adanya suatu standar yang sistemik untuk menentukan seberapa siapkah suatu organisasi dalam melakukan Forensik Digital.

Namun, untuk penelitian mengenai kesiapan forensik digital sebuah organisasi masih minim. Untuk itu perlu dilakukannya suatu penelitian supaya bisa mengidentifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital yang nantinya bisa diukur dan setelah dihitung akan mengahasilkan sebuah nilai yang disebut *Digital Forensic Readiness Index*(DiFRI).

PT Waditra Reka Cipta Bandung adalah Salahsatu Konsultan IT yang berkedudukan di Kabupaten Bandung Barat yang menyediakan layanan solusi IT (mengkhususkan pada pengembangan perangkat lunak beserta implementasi dan Tata Kelola sistem informasi/ teknologi informasi) bagi beragam kebutuhan pelanggan di berbagai industri dan jasa. Perusahaan ini mempunyai komitmen untuk menjadi mitra terpercaya bagi pelanggan dan membantu mereka dalam upaya mencapai target bisnisnya melalui penyediaan solusi IT. Serta mempunyai tujuan untuk memberikan kualitas layanan yang tinggi pada setiap proyek pekerjaan yang ditangani.

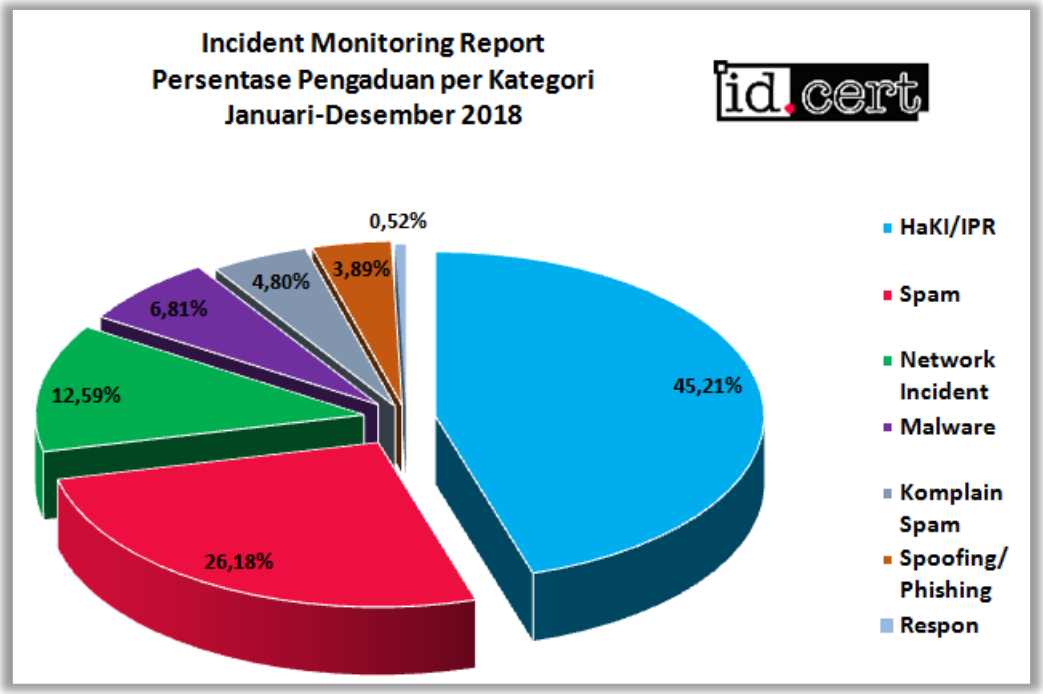


Gambar 1.2 Website PT Waditra Reka Cipta bandung

Berdasarkan hasil dari statistik terkait *handling incident* diketahui bahwa layanan TI merupakan salah satu sasaran yang diincar untuk dijadikan obyek serangan siber (ID-CERT,

2018). Dengan adanya kebijakan DFR, PT WRC Bandung dapat mengefisiensikan proses penanganan apabila terjadi insiden terhadap layanan TI. Namun, sampai sekarang belum terdapat kebijakan terkait dengan DFR di lingkungan perusahaan.

Berdasarkan hal tersebut, pada penelitian ini akan dilakukan perancangan kebijakan DFR khusus untuk layanan TI di PT WRC bandung. Hal ini dikarenakan, saat sebuah insiden tidak tertangani dengan baik, maka akan memengaruhi dan menghambat proses bisnis dari masing-masing unit kerja yang menggunakan serta menyediakan layanan TI di PT WRC Bandung ini. Selain itu kebijakan ini dapat dijadikan sebagai bentuk prosedural apabila terjadi *cyber crime* di Perusahaan.



Gambar 1.3 Incident Monitoring ID-CERT Tahun 2018

Perancangan kebijakan DFR pada PT WRC Bandung ini menggunakan pengembangan dari model DiFRI (Digital Forensic Readiness Index) yang dikemukakan oleh (Widodo, 2016)

1.2 Rumusan Masalah

Berdasar latar belakang dapat ditarik suatu rumusan masalah pada penelitian ini yakni "Bagaimana menerapkan kebijakan *Digital Forensic Readiness* (DFR) untuk layanan TI pada PT Waditra Reka Cipta Bandung?".

1.3 Tujuan Penelitian

Berdasarkan rumusan yang dibuat maka dapat diambil suatu tujuan terhadap penelitian ini yakni memberikan pemahaman, menambah pengetahuan dan dapat di adaptasi dalam melaksanakan perancangan kebijakan pada suatu organisasi.

1.4 Batasan Masalah

Berdasarkan rumusan yang dibuat maka dibuat Batasan permsalahan agar penelitian lebih fokus dan tepat sasaran, Batasan tersebut antara lain :

1. Penelitian dilakukan pada salah satu Perusahaan Penyedia Jasa TI yakni PT Waditra Reka Cipta Bandung
2. Penelitian berfokus pada seberapa siapkah perusahaan dalam menghadapi masalah yang berkaitan dengan *Digital Forensik.*

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari dibuatnya penelitian ini adalah memberikan suatu rancangan kebijakan Digital Forensic Readiness (DFR) untuk mengoptimalisasikan serta tanggap insiden TI pada PT Waditra Reka Cipta Bandung

1.6 Review Penelitian

Perkembangan Teknologi informasi dan Komunikasi semakin berkembang sehingga dapat menyebabkan peningkatan tindak kejahatan dalam dunia maya atau sering disebut “cyber crime”. Maka dibutuhkan suatu kesiapan dari sebuah organisasi dalam menghadapi hal tersebut. Kesiapan itu sendiri dapat disebut dengan istilah *Readiness* yang berdasarkan pada proses bisnis serta fungsi dari teknologi tersebut. Dalam penelitian ini topik pembahasannya mengenai *Digital Forensic Readiness* pada suatu organisasi.

Kemudian dari berbagai studi dan telaah terkait *Digital Forensic Readiness,* ditemukan beberapa penelitian dan jurnal terkait serta membahas tentang *Digital Forensic Readiness,* diantaranya sebagai berikut :

A. Penelitian dilakukan oleh (Mohamed, B., Atif, & Andrew, 2014) yang membagi kesiapan forensic menjadi dua bagian fokus utama yakni Kesiapan Infrastruktur dan Kesiapan Operasional. Kesiapakan infrastruktur berfokus pada menjamin ketersediaan data pada suatu organisasi disajikan dengan tepat, sedangkan pada

kesiapan operasional berfokus pada penyediaan peralatan serta pelatihan individu yang akan terlibat pada digital forensic itu sendiri.

B. Penelitian dilakukan oleh (Elyas, Ahmad, Maynard, & Lonie, 2015) beberapa ahli merumuskan model atau *framework* logis dari *Digital Forensic Readiness* yang dapat digunakan secara umum. Dalam model atau *framework* logis yang disusun ini terdapat beberapa faktor atau aspek yang saling mempengaruhi dan berhubungan, antara lain *forensic readiness capability* yang berhubungan dengan *forensic radiness objective*. Dalam *forensic readiness capability* terdapat 2 faktor yang mempengaruhi, yaitu *Organizatinal Factors* dan *Forensic Strategy*. Sementara dalam *forensic readiness objectives* ada 4 faktor yang mempengaruhi, yaitu *regulatory compliance, legal evidence management, forensic respone, business objectives*.

C. Penelitian dilakukan oleh (Robert Rownlingston, 2004) memaparkan dalam penelitiannya bahwa ada sepuluh tahapan dalam proses *Digital Forensic Readiness,* mulai dari skenario bisnis yang memerlukan bukti digital, identifikasi bukti-bukti digital, hingga tindakan-tindakan legal di dalam menangani insiden yang terjadi.

D. Penelitian dilakukan oleh (Grobler & Louwrens, 2007) memaparkan dalam penelitiannya tentang *Digital Forensic Readiness* sebagai sebuah komponen dalam keamanan sistem informasi. Pada penelitian ini dibahas berbagai isu keamanan dari sistem informasi dan *Digital Forensic Readiness*, belum adanya keseimbangan antara keamanan sistem dan *Digital Forensic Readiness*, serta tujuan dari *Digital Forensic Readiness* sebagai bentuk keamanan sistem informasi.

E. Penelitian dilakukan oleh (Barske, Stander, & Jordaan, 2010) memaparkan dalam penelitiannya tentang *framework* atau model *Digital Forensic Readiness* untuk Usaha Kecil dan Menengah (UKM) di Afrika Selatan. Pada penelitian ini mereka membuat model *Digital Forensic Readiness* dan faktor-faktor yang harus diperhitungkan, mulai dari strategi, kebijakan dan prosedur, teknologi yang digunakan, *digital forensic respone*, hingga pada pengawasan. Model yang dibuat oleh Barske, Stander dan Jordaan ini masih memiliki kekurangan, yaitu tidak adanya metode perhitungan dari kompone-komponen penyusun model *Digital Forensic Readiness,* sehingga masih sulit diaplikasikan.

F. Penelitian dilakukan oleh (Mouhtaropoulos, Li, & Grobler, 2014) memaparkan pada

penelitian ini seharusnya sebelum insiden atau tindak kejahatan terjadi mayoritas institusi / organisasi sudah menyiapkan cara mengatasi masalah yang akan ditimbulkan dari tindakan tersebut. Maka dibutuhkan *Digital Forensic Readiness* untuk menjadi penghubung antara kelangsungan usaha/bisnis dengan investigasi forensik yang berjalan baik. *Digital Forensic Readiness* dijelaskan sebagai rencana pra-insiden yang berhubungan dengan identifikasi bukti digital, pelestarian, penyimpanan, analisis dan penggunaan serta meminimalkan biaya penyilidikan forensik. Dengan kata lain *Digital Forensic Readiness* ini bertujuan untuk mengelola bukti digital, membantu proses penyelidikan forensik agar tepat waktu dan menghemat biaya penyelidikan.

G. Penelitian dilakukan oleh (Widodo, 2016) memaparkan dalam penelitiannya tentang Model *Digital Forensic Readiness Index* (DiFRI) untuk mengukur tingkat kesiapan Institusi dalam menanggulangi aktivitas *Cyber Crime*. Pada penelitian ini dijelaskan komponen-komponen yang membentuk *Digital Forensic Readiness Index* (DiFRI), seperti komponen strategi, kebijakan dan prosedur, teknologi dan keamanan, *digital forensic respone*, kontrol, *legality*. Komponen-komponen tersebut juga dilengkapi dengan indikator-indikator yang nantinya berguna untuk menghitung kesiapan dari institusi-institusi tersebut.
H. Jurnal Penelitian (Sachowski & Sachowski, 2019). Dijelaskan mengenai pentingnya kesiapan suatu organisasi dalam Forensik Digital, terutama saat pengumpulan dan penanganan barang bukti digital untuk dikelola oleh auditor suatu organisasi sebelum disajikan ke ranah hukum.
I. Penelitian dilakukan oleh (Reddy & Venter, 2008) mengusulkan serangkaian kebijakan untuk meningkatkan potensi forensik suatu organisasi dalam membantu menerapkan kemampuan kesiapan forensic untuk suatu insiden informasi, Secara khusus, kerangka kerja memberikan panduan untuk menentukan kebijakan tingkat tinggi, proses bisnis dan fungsi organisasi, dan untuk menentukan prosedur forensik tingkat perangkat, standar dan proses yang diperlukan untuk menangani insiden privasi informasi.
J. Penelitian dilakukan oleh (Moussa, Ithnin, & Miaikil, 2014) menyarankan kesiapan forensic bagi para penyedia layanan cloud (internet) agar dapat bertanggungjawab dalam mengumpulkan bukti digital ketika terjadinya insiden. Karena kurangnya

respon insiden secara efisien dan konsumen tidak mempunyai pilihan lain, selain menerima bukti digital dari penyedia.

K. Penelitian dilakukan oleh (Kazadi & Jazri, 2015) membahas tentang bagaimana pentingnya seorang administrator system pada suatu organisasi dalam mengamankan dan melindungi system informasi. Selain pada system juga bertanggungjawab dalam penyiapan alat keamanan untuk mengamankan system computer serta menyiapkan bukti digital bila diperlukan.

Rangkuman terhadap penelitian-penelitian yang telah dilakukan sebelumnya, dapat dilihat pada tabel perbandingan penelitian-penelitian yang disebutkan sebelumnya dan dapat dilihat pada tabel 1.1 seperti tabel di bawah ini.

Tabel 1.1 Perbandingan Penelitian Terdahulu

No	**Penulis Paper**	**Komponen yang diteliti**	**Persamaan atau perbedaan penelitian**
1	(Mohamed et al., 2014)	Kesiapan Infrastruktur dan Kesiapan Operasional	beberapa komponen yang diteliti yakni kesiapan infrastruktur organisasi serta operasional organisasi
2	(Elyas, *et al.*, 2015)	Terdapat 7 komponen, yaitu *Strategy, Policy & Procedure, Technology, Security, Digital Forensic Response, Control, Legality.*	Terdapat komponen-komponen yang diteliti dalam penelitian ini
3	(Robert Rownlingston, 2004)	Terdapat 3 komponen, yaitu *Policy&Procedure, Security, Legality.*	Memiliki komponen yang diteliti yakni *policy,procedure,security dan legality*
4	(Grobler & Louwrens, 2007)	Terdapat 1 komponen, yaitu *Security*.	Salah satu aspek yang diteliti dalam penelitian ini

5	(Barske, Stander, et al., 2010)	Terdapat 5 komponen, yaitu *Strategy, Policy & Procedure, Technology, Digital Forensic Response, Control.*	Beberapa komponen yang diteliti seperti *strategy,policy,procedure,digital forensic respone*
6	(Mouhtaropoulos et al., 2014)	Terdapat 6 komponen, yaitu *Technology, Security, Digital Forensic Response, Control, Cost, Legality.*	Ada beberapa komponen yang di uji kecuali "cost"
7	(Widodo, 2016)	Terdapat 6 komponen, yaitu *Strategy, Policy & Procedure, Technology & Security, Digital Forensic Response, Control, Legality.*	dikembangkan dari 6 komponen menjadi 5 komponen dalam menilai forensic readiness suatu organisasi/perusahaan.
8	(Sachowski & Sachowski, 2019).	Pengumpulan dan penanganan barang bukti digital oleh auditor organisasi	Merupakan aspek yang akan diteliti
9	(Reddy & Venter, 2008)	Serangkaian kebijakan dalam penerapan *forensic readiness* di organisasi	Merupakan aspek yang akan diteliti
10	(Moussa, et al., 2014)	kesiapan forensic bagi para penyedia layanan jasa	Memiliki kesamaan dengan tempat studi kasus yang diteliti
11	(Kazadi & Jazri, 2015)	Pentingnya administrator system pada suatu organisasi dalam *forensic readiness*	Sebagai bahan penelitian ditempat studi kasus
12	Usulan Penelitian	Membangun sebuah kerangka kerja DFR dari hasil penghitungan *Digital Forensic Readiness Index* (DiFRI) terhadap suatu perusahaan, agar lebih tanggap insiden *Digital Forensik*	

1.7 Metodologi Penelitian

Metode dalam penelitian ini menggunakan beberapa tahapan metodologi penelitian yang dapat dilihat pada Gambar 1.4.

Gambar 1.4 Bagan Proses Metodologi Penelitian

1.8 Sistematika Penulisan

Adapun sistematika penulisan yang dimaksud adalah sebagai berikut :

BAB 1 PENDAHULUAN

Pada bagian ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, *review* penelitian, metodologi penelitian dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bagian ini berisi tentang teori-teori yang terkait dengan kebijakan keamanan, *digital forensic*, *digital forensic readiness*, tahapan *digital forensic readiness* dan DiFRI.

BAB 3 METODOLOGI PENELITIAN

Pada bagian ini berisi tentang langkah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB 4 HASIL DAN PEMBAHASAN

Pada ini berisi tentang pembuatan model *Digital Forensic Readiness* berdasarkan

penelitian-penelitian yang telah ada, serta hasil uji coba dan evaluasi dari model yang telah dibangun tersebut.

BAB 5 KESIMPULAN DAN SARAN

Pada bagian ini berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan serta saran dan rekomendasi untuk penelitian selanjutnya.