

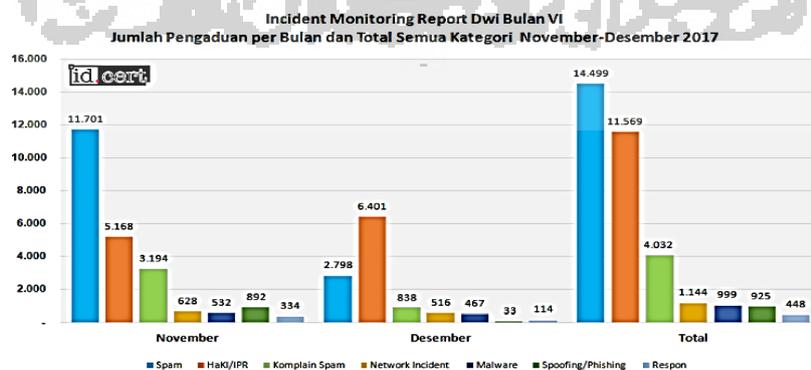
# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

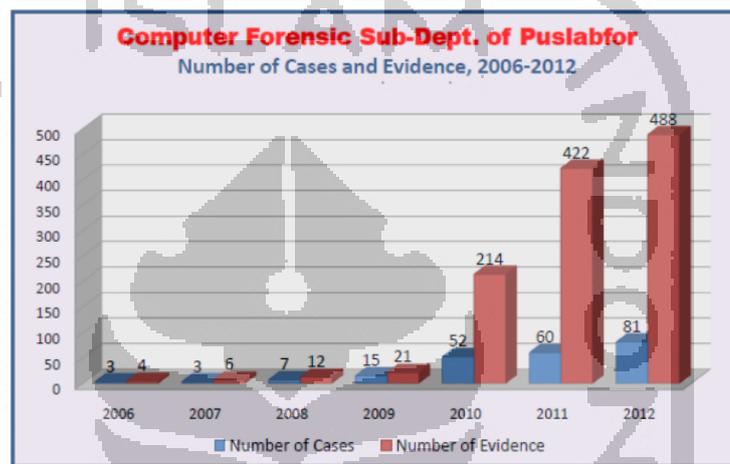
Dewasa ini, perkembangan tindak kejahatan meningkat tajam, cara dan modus operandi pun juga semakin bervariasi, menyesuaikan pola kebiasaan masyarakat dan perkembangan teknologi. Kejahatan tidak lagi berupa kejahatan konvensional seperti pencurian barang, perampokan atau penipuan. Kejahatan saat ini semakin canggih karena melibatkan teknologi informasi maupun peralatan elektronik. Diperkirakan 556 juta orang setiap tahun menjadi korban kejahatan internet, selain itu kerugian diperkirakan mencapai 28 miliar dollar diakibatkan oleh malware, virus, spam, hacking dan penipuan/pencurian (Infosecurity, 2017). Dari sumber yang sama juga disebutkan bahwa motif kejahatan dunia maya yang dilakukan adalah 40% kejahatan dunia maya murni, 50% kejahatan dunia maya untuk tujuan tertentu seperti politik (ujaran kebencian), 3% perang cyber dan 7% mata-mata data informasi.

Berdasarkan penelitian dari ID-CERT (Indonesia Computer Emergency Response Team) yang menjadi laporan Dwi Bulan VI Tahun 2017, diperoleh data dari empat puluh satu (41) responden yang terdiri dari Kominfo, ID-CERT, PANDI, APJII, Detik.net, Zone-h, Anti Fraud Command Center (AFCC), dan Kaspersky, 3 (tiga) operator telekomunikasi, 7 (tujuh) NAP, 22 (dua puluh dua) Penyedia Jasa Internet(PJI/ISP), dan KEMDIKBUD. Hasil penelitian tersebut dapat dilihat pada Gambar 1.



Gambar 2. Jumlah Pengaduan Dwi Bulan VI Tahun 2017

Dari berbagai pemaparan diatas, terlihat bahwa tindak kejahatan internet selalu meningkat. Sayangnya tingkat kejahatan tersebut tidak diimbangi dengan jumlah barang bukti yang tersedia. Muhammad Nuh Al Azhar, ketua Digital Forensic Analyst Team (DFAT) Laboratorium Forensik POLRI menyampaikan dari tahun ke tahun, barang bukti digital masih sangat minim, tidak sebanding dengan tindak kejahatan internet. Hal ini dapat terlihat pada Gambar 2.



**Gambar 3. Jumlah Cybercrime dan Jumlah Barang Bukti Digital (Hadfex 2013)**

Dari gambar 2 terlihat kenaikan barang bukti digital secara signifikan. Meskipun demikian jumlah kasus yang ditangani kepolisian masih sangat jauh dari jumlah kasus yang terjadi. Minimnya laporan tindak kejahatan internet dan barang bukti digital, mengindikasikan kurangnya pemahaman masyarakat akan Cybercrime dan barang bukti digital. Selain itu, minimnya barang bukti digital tersebut juga mengindikasikan kurangnya kesiapan dari berbagai lembaga dalam hal ini instansi pemerintahan dalam mengantisipasi dan mendokumentasikan setiap kejadian maupun kejahatan internet. Kesiapan institusi dalam hal digital forensic tersebut seringkali dikenal dengan istilah digital forensic readiness (Tan, 2001).

Pada era modern dan berjalannya penegakan hukum seperti sekarang, sudah saatnya instansi pemerintahan tidak hanya bersikap pasif, tetapi juga aktif untuk menindak dan melaporkan pelaku kejahatan di lingkungan pemerintahan. Tindakan aktif ini berupa perhatian akan pentingnya barang bukti digital, sehingga sebisa mungkin setiap aktivitas dunia maya dan transaksi elektronik

terdokumentasikan dan tercatat dengan baik. Dengan adanya digital *forensic readiness*, suatu instansi pemerintahan akan lebih siap ketika tertimpa insiden, proses investigasi akan lebih cepat, diterima oleh hokum dan adanya barang bukti yang cukup untuk menjerat pelaku kejahatan ke pengadilan.

Penelitian terkait digital *forensic readiness* sudah dilakukan antara lain oleh (Mouhtaropoulos et al. 2014),(Elyas et al. 2015), (Widodo 2016), (Karie & Karume 2018) dan (Sunardi et al. 2019) tetapi berdasarkan telaah, belum ada penelitian yang membahas tentang penyusunan indicator, implementasi digital *forensic readiness* atau cara menghitung digital *forensic readiness* indeks di lingkungan instansi pemerintahan, sehingga penelitian ini sangat penting dan bermanfaat sekali bagi instansi pemerintahan, khususnya wilayah Kabupaten Banyumas.

## **1.2. Rumusan Masalah**

Dari latar belakang dan permasalahan di atas, dapat dirumuskan berbagai permasalahan yang akan diteliti, antara lain:

1. Apakah konsep DiFRI yg diterapkan masih relevan?
2. Bagaimana konsep DiFRI yg lebih relavan diterapkan?
3. Bagaimana Kesiapan instansi pemerintahan Kabupaten Banyumas dalam menghadapi aktifitas *cybercrime*
4. Bagaimana meningkatkan aspek keamanan computer dan Sistem Informasi serta jumlah dan ketersediaan barang bukti

## **1.3. Batasan Masalah**

Dari rumusan masalah tersebut, dibuat batasan-batasan masalah yang akan diteliti, agar penelitian lebih fokus dan tepat sasaran, batasan-batasan masalah tersebut adalah :

1. Konsep DiFRI yang diterapkan berdasarkan penelitian terdahulu
2. Metode penghitungan DiFRI menggunakan Statistik
3. Metode penghitungan DiFRI diterapkan di instansi pemerintahan Kabupaten Banyumas.

#### **1.4. Tujuan Penelitian**

Penelitian ini bertujuan antara lain :

1. Membandingkan antar instansi Pemerintah agar dapat menyiapkan diri, menangkal, menghadapi serta menindak lanjuti aktifitas *Cybercrime*.
2. Dapat meningkatkan aspek keamanan computer dan Sistem Informasi serta jumlah dan ketersediaan barang bukti.
3. Dapat mencegah dan lebih siap dalam menghadapi aktifitas *Cybercrime*.

#### **1.5. Manfaat Penelitian**

Penelitian ini diharapkan dapat memberi kontribusi dalam kehidupan manusia dan dapat diterapkan dalam dunia nyata. Adapun manfaat penelitian ini antara lain

##### **1. Bagi Instansi Pemerintahan**

Dengan adanya penelitian ini, diharapkan instansi pemerintahan wilayah Kabupaten Banyumas dapat mengetahui dan lebih memperhatikan kesiapan institusi dalam digital *forensic readiness*, sehingga dapat menghadapi *Cybercrime*.

##### **2. Bagi peneliti**

Dengan penelitian ini, diketahui berbagai konsep tentang digital forensik, digital *forensic readiness*, indikator masing-masing konsep serta cara mengetahui tingkat digital *forensic readiness* dalam indeks.

##### **3. Bagi penegak hukum**

Penegak hukum diharapkan lebih intensif mensosialisasikan berbagai kasus dan penanggulangan *Cybercrime*. Bagaimana aturan, regulasi dan tindakan hukum terkait *Cybercrime*.

##### **4. Bagi masyarakat luas**

Dengan adanya penelitian ini diharapkan masyarakat luas lebih berhati-hati dalam menggunakan perangkat teknologi informasi dan komunikasi agar tidak menjadi korban *Cybercrime*. Selain itu diharapkan masyarakat luas juga mengetahui berbagai hal tentang *Cybercrime*, hal-hal yang termasuk *Cybercrime* dan hukuman-hukuman bagi pelaku *Cybercrime*, agar masyarakat tidak melakukan *Cybercrime*.

## 1.6. Review Penelitian

*Readiness* berarti kesiapan, banyak sekali bentuk kesiapan yang harus disiapkan maupun diketahui Instansi Pemerintahan, sesuai dengan proses bisnis dan fungsi teknologi informasi dan komunikasi. Adakalanya *information readiness*, adakalanya *network readiness*, *e-learning readiness*, *digitalforensic readiness*, *cloud readiness* dan sebagainya.

Dari beberapa telaah terkait *digital forensic readiness*, ditemukan beberapa kemampuan organisasi untuk memaksimalkan penggunaan bukti digital dan mengantisipasi litigasi. Ketidacukupan penelitian teknis dan peraturan perundang-undangan dan kebutuhan yang terus meningkat mekanisme pengawetan bukti telah membawa kebutuhan akan kesiapan forensik dan pembuatan kebijakan di masa depan, untuk mengungkap kesenjangan yang perlu dijumpai. (Mouhtaropoulos et al. 2014)

, memvalidasi dan memperbaiki kerangka kesiapan forensik digital melalui serangkaian kelompok fokus ahli. Menggambar pada pertimbangan para ahli dikelompok fokus, kami membahas masalah kritis yang dihadapi praktisi dalam mencapai digital kesiapan forensik. (Elyas et al. 2015)

membahas tentang penyusunan indikator, implementasi *digital forensic readiness* atau cara menghitung *digital forensic readiness* indeks untuk mencegah & menindak lanjuti kejahatan dunia maya, sehingga penelitian ini sangat penting dan bermanfaat sekali untuk diterapkan dan dianalisa bagi instansi Pemerintah. (Widodo 2016)

konsentrasi: langkah-langkah proaktif berbeda yang dapat dianut oleh organisasi sebagai cara untuk meningkatkan kemampuan untuk menanggapi insiden keamanan dan menciptakan lingkungan siap-forensik digital. (Karie & Karume 2018)

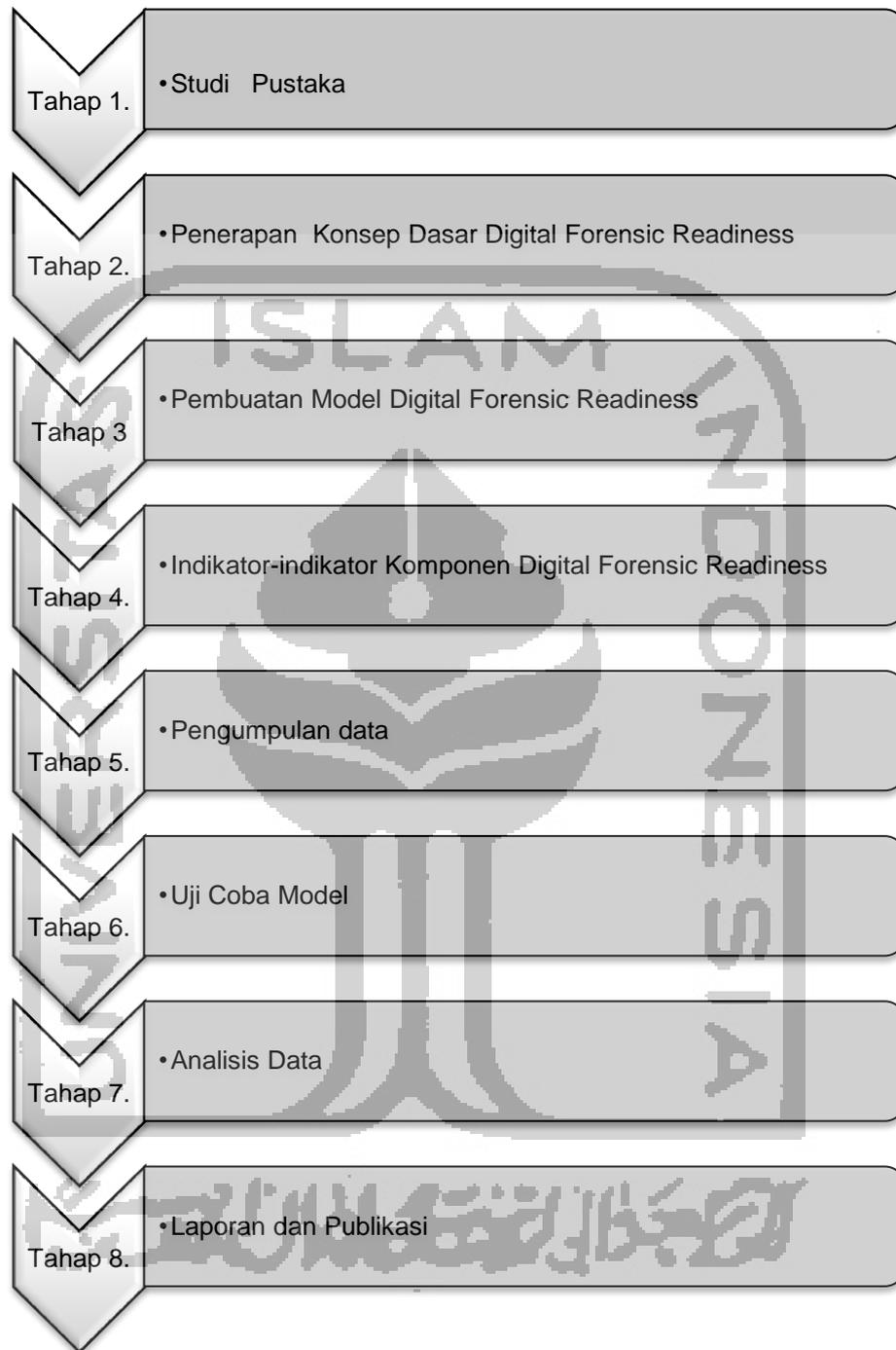
menyelidiki bukti digital pada *file log* aplikasi web kemas yang dijalankan pada sistem *cluster* yang dibangun oleh Docker Swarm. Investigasi ini dilakukan dengan menggunakan kerangka kerja Grr Rapid Response (GRR) (Sunardi et al. 2019).

Pada penelitian yang dilakukan oleh Widodo juga melakukan penelitian terkait digital *forensic readiness* dimana menggabungkan atau mengkolaborasikan dari beberapa penelitian sebelumnya. Penelitian tersebut memiliki model DiFRI mulai dari strategi, kebijakan dan prosedur, teknologi&sekuriti, digital forensik respons, kontrol, dan *legality* yang memiliki masing-masing indikator (Widodo, 2016). Dari penelitian tersebut masih cukup kurang untuk diterapkan di instansi pemerintahan khususnya Kabupaten Banyumas. Hal ini dikarenakan kebijakan, teknologi dan digital forensik respons sudah tidak sesuai dengan perkembangan teknologi saat ini.

Pada penelitian ini akan dilakukan penyempurnaan dan kompilasi berbagai model indikator yang telah dikembangkan sebelumnya, kemudian disempurnakan agar dapat diterapkan di instansi pemerintahan khususnya Kabupaten Banyumas dan sesuai dengan perkembangan infrastruktur teknologi sekarang ini.

### **1.7. Metodologi Penelitian**

Untuk menjaga agar penelitian fokus dan sistematis, maka dibuatlah langkah-langkah penelitian seperti pada Gambar 3 berikut :



Gambar 4. Langkah-langkah Penelitian

## **1. Studi Pustaka**

Diadakan studi dan pelacakan secara teoritis terhadap berbagai pembahasan mengenai digital *forensic readiness* pada penelitian-penelitian maupun karya ilmiah terdahulu, agar tidak terjadi perulangan pembahasan yang menjadikan penelitian tidak efektif dan kurang bernilai.

## **2. Konsep Dasar Digital *Forensic readiness***

Selanjutnya dari berbagai penelitian yang telah ada dirumuskan aspek-aspek utama pada digital *forensic readiness*, faktor-faktor dan komponen utamaapa saja, agar diperoleh pemahaman yang komprehensif mengenai konsep digital *forensic readiness*.

## **3. Model DiFRI**

Setelah dilakukan analisa mendalam, kemudian dilakukan perhitungan DiFRI untuk menilai instansi pemerintahan. Pada penelitian ini, peneliti akan menghitung model digital *forensic readiness* yang telah dikembangkan sebelumnya, yaitu dengan merumuskan komponen utama dan indikator-indikator berdasarkan penelitian-penelitian yang sudah ada. Agar didapat model digital *forensic readiness* yang dapat memberikan gambaran detail status instansi pemerintahan terkait digital *forensic readiness*

## **4. Indikator-indikator Komponen DiFRI**

Dari model tersebut, selanjutnya dibuat indikator-indikator untuk masing-masing komponen penyusun model digital *forensic readiness*. Indikator tersebut diperoleh dari telaah penelitian terdahulu dan kajian pustaka.

## **5. Perumusan Metode Penghitungan**

Dari indikator-indikator yang telah ditentukan, dibuatlah metode penghitungan skor atau indeks dari masing-masing komponen digital *forensic readiness* tersebut, maupun DiFRI secara keseluruhan.

## **6. Uji Coba Model**

Selanjutnya model DiFRI yang telah dirancang tersebut diuji coba pada instansi untuk diketahui bagaimana hasil maupun gambaran digital *forensic readiness* dari suatu instansi.

## **7. Analisis Data**

Data hasil uji coba model DiFRI tersebut kemudian dianalisis dan diolah sehingga menghasilkan nilai berupa indeks yang menggambarkan tingkat digital *forensic readiness* instansi.

## **8. Laporan**

Semua kegiatan penelitian yang dilakukan akan dibuat laporan dan dokumentasi, sebagai karya ilmiah sekaligus sebagai bahan acuan dan referensi penelitian berikutnya.

### **1.8. Sistematika Penulisan**

Untuk memudahkan penelitian, baik proses penelitian maupun pembuatan laporan penelitian. Dibuatlah sistematika dan runtutan proses penelitian sebagai berikut:

#### **BAB I PENDAHULUAN.**

Bab ini berisi Latar Belakang Penelitian, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Review Penelitian, Metodologi Penelitian, dan Sistematika Penulisan.

#### **BAB II TINJAUAN PUSTAKA.**

Pada bab ini, akan dibahas tentang landasan-landasan teori terkait dengan digital *forensic*, digital *forensic readiness*, tahapan-tahapan digital *forensic readiness*.

#### **BAB III METODOLOGI PENELITIAN.**

Pada bab ini, dibahas tentang detail Metodologi Penelitian. Dari langkah-langkah penelitian, mulai dari studi pustaka, konsep dasar digital *forensic readiness*, Model digital *forensic readiness*, indikator-indikator masing-masing komponen digital *forensic readiness*, Metode pengumpulan data, metode penghitungan data, dan skala DiFRI.

#### **BAB IV HASIL DAN PEMBAHASAN**

Bab ini, berisi pembahasan meliputi Model DiFRI, penerapan DiFRI, validitas dan reliabilitas indikator, hasil penerapan dan analisa-analisa data maupun hasil penelitian.

## **BAB V KESIMPULAN DAN SARAN.**

Pada Kesimpulan dan Saran ini disampaikan kesimpulan dari hasil penelitian, baik terkait model maupun penerapan model. Selain itu, juga berisi saran maupun masukan untuk kemajuan penelitian selanjutnya.

