BAB I
PENDAHULUAN

1.1. Latar Belakang

Upaya untuk melakukan pengungkapan kasus-kasus *cybercrime* dilakukan melalui sebuah proses yang dikenal dengan *digital forensics*. Dalam hal ini *digital forensics* adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekontruksi kejadian serta keabsahan proses peradilan.

Hal yang penting yang harus diperhatikan oleh setiap *digital investigator* dalam menjalankan aktivitas *digital forensics* adalah diikutinya setiap tahapan dan prosedur dalam *digital forensics*. Tahapan tersebut dikenal dengan *terminology frameworks*. Dalam hal ini menurut Pollitt (1995) tahapan dalam proses *digital forensics* harus sesuai dengan aturan hukum dan juga mekanisme yang tepat. Pollitt (1995) sendiri memperkenalkan empat langkah yang berbeda dalam menjalankan aktivitas investigasi digital, yaitu : *acquisition, identifications, evaluation* dan *admission.*

Terdapat beberapa penelitian lainnya yang juga melakukan kajian tentang metodologi atau *frameworks* untuk *digital forensics*. Selamat, dkk. (2011) melakukan penelitian di bidang metodologi forensika digital dengan cara menyederhanakan 15 langkah *Digital Forensics Investigation Framework* (DFIF) yang menjadi objek penelitiannya hingga didapat 5 tahapan umum DFIF pada semua kasus insiden tanpa merusak bukti dan melindungi *chain of custody*. Rahayu (2014) dalam penelitian tesisnya telah menghasilkan metodologi berdasarkan konsep *Integrated Digital Forensics Investigation Framework* (IDFIF). IDFIF ini diharapkan dapat menjadi standar metode penyelidikan para penyidik. IDFIF telah memperhitungkan DFIF sebelumnya sehingga DFIF yang telah ada sebelumnya dapat diakomodir oleh IDFIF.

Suharno (2014) melakukan penerapan IDFIF terhadap jajaran penegak hukum di Indonesia (POLRI, KPK dan BNN) dalam proses investigasi terhadap

barang bukti digital berupa *hardisk* dan *flashdisk*. *Framework* standar IDFIF dapat mengakomodir *cybercrime* di lapangan baik kasus besar ataupun kasus kecil, tingkat efisiensi, efektifitas dan reliabilitasnya lebih baik. Namun, IDFIF ini perlu dievaluasi pada tahap 2 *proactive* untuk langkah 2.6 *securing the scene* disarankan ditempatkan pada posisi 2.1 pada *proactive collection* karena untuk melakukan investigasi di TKP harus diadakan *securing the scene* terlebih dahulu.

IDFIF merupakan metode terbaru yang dikembangkan oleh Rahayu(Tesis dan *paper*, 2014) namun belum pernah diterapkan pada proses *investigasi smartphone* sehingga IDFIF ini menarik untuk diteliti lebih lanjut dalam proses investigasi *smartphone*. Gary, dkk. (2007) menyatakan bahwa *smartphone* adalah telepon *Internet-enabled* yang biasanya menyediakan fungsi *Personal Digital Assistant* (PDA) seperti fungsi kalender, buku agenda, buku alamat, kalkulator, dan catatan. *Smartphone* mempunyai fungsi yang menyerupai komputer, sehingga kedepannya teknologi *smartphone* akan menyingkirkan teknologi komputer desktop terutama dalam hal pengaksesan data dari Internet. Setiap *smartphone* memiliki sistem operasi yang berbeda-beda, sama hal nya dengan sistem operasi pada komputer *desktop*.

Penerapan IDFIF terhadap proses investigasi *smartphone* perlu dilakukan evaluasi terlebih dahulu terhadap tahapan IDFIF tersebut karena *smartphone* memiliki karakteristik yang unik sehingga tidak bisa disamakan dengan penanganan komputer biasa. Widoyoko (2012), evaluasi merupakan proses yang sistematis dan berkelanjutan untuk mengumpulkan, mendeskripsikan, menginterpretasikan, dan menyajikan informasi tentang suatu program untuk dapat digunakan sebagai dasar membuat keputusan, menyusun kebijakan maupun menyusun program selanjutnya.

Proses evaluasi terhadap model IDFIF memerlukan suatu model pendekatan yang tidak hanya memberikan rekomendasi perbaikan terhadap model IDFIF tersebut namun juga dapat menerapkan hasil rekomendasi perbaikan tersebut sehingga menghasilkan IDFIF v2 yang memiliki kemampuan untuk investigasi secara dinamis khususnya terhadap proses penanganan investigasi *smartphone*, Adapun tahapan IDFIF yang dievaluasi hanya dilakukan pada tahapan *proactive*

process dan *reactive process* sehingga model IDFIF tersebut dapat lebih *fleksible* dan dapat diterapkan untuk proses investigasi *smartphone*.

Model pendekatan yang dipilih untuk melakukan evaluasi terhadap tahapan IDFIF adalah *soft system methodology*(SSM). SSM merupakan suatu metode evaluasi yang tidak hanya membandingkan suatu model dengan model model lainnya melainkan membandingkan model konseptual dengan suatu proses di dunia nyata sehingga dapat diketahui kekurangan dari model konseptual tersebut dan langsung melakukan tindakan perbaikan terhadap model konseptual itu sehingga tidak ada perbedaan antara model konseptual dan aktivitas riil. Prinsip pada SSM adalah memandang permasalahan secara utuh, bukan memecah menjadi bagian-bagiannya sebab pemecahan masalah seringkali menghilangkan kondisi yang sebenarnya dihadapi sehingga dapat menciptakan system aktivitas dan hubungan manusia dalam sebuah organisasi atau grup dalam rangka mencapai tujuan bersama, maka SSM dapat diterapkan sebagai solusi terhadap evaluasi tahapan IDFIF untuk proses investigasi *smartphone*.

1.2. Rumusan Masalah

Dari latar belakang diatas dapat ditarik permasalahan untuk dijadikan perumusan masalah antara lain :

1. Bagaimanakah konsep dari *soft system methodology* yang bisa diterapkan untuk melakukan evaluasi IDFIF?
2. Bagaimanakah perbaikan dan pengembangan IDFIF berdasarkan *soft system methodology*?
3. Bagaimanakah pengujian dan kinerja IDFIF v2 pada lingkungan *smartphone investigation*?

1.3. Batasan Masalah

Batasan-batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Penelitian dilakukan untuk melakukan evaluasi terhadap IDFIF pada tahap *Proactive* dan *Reactive.*
2. Fokus penelitian ini hanya dilakukan pada penanganan *Smartphone Android v4.2.2. Jelly Bean.*

1.4. Tujuan Penelitian

Berdasarkan rumusan yang dibuat maka dapat diambil tujuan dari penelitian ini. Tujuan dari dibuatnya penelitian ini antara lain:

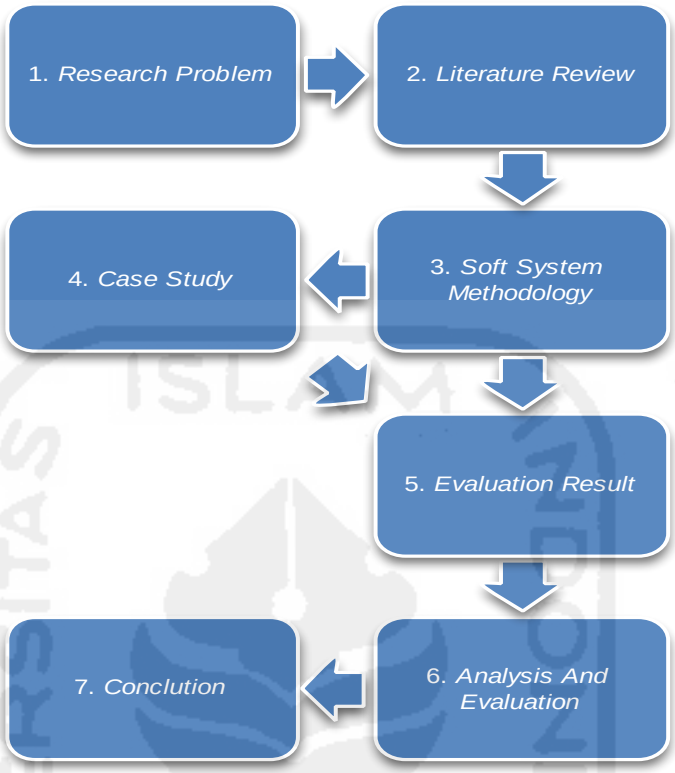
1. Mengetahui konsep *soft system methodology* untuk perbandingan model.
2. Mengetahui hasil perbaikan dan pengembangan IDFIF berdasarkan *soft system methodology*.
3. Melakukan uji coba kinerja IDFIF v2 dalam sebuah simulasi pada *smartphone investigation.*

1.5. Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

1. Memberi kontribusi pada area penelitian pada *Digital Forensics*, melalui *review* beberapa penelitian terkini kemudian dilanjutkan dengan melakukan evaluasi terhadap *Integrated Digital Forensics Investigation Framework* khususnya dalam *smartphone investigation*.
2. Penelitian ini diharapkan mampu memudahkan pengguna dalam hal ini penyidik untuk melakukan proses forensik yang terjadi dalam *Digital Forensics Investigation* khususnya pada *smartphone*, dimana informasi tersebut dapat segera diketahui untuk ditindaklanjuti sebagai bahan untuk membantu mengungkap kejahatan yang terjadi.

1.6. Metodologi Penelitian



Gambar 1.1. Metodologi Penelitian

Gambar 1.1 menunjukkan penelitian ini menggunakan 7 tahapan metodologi penelitian yakni (1) *Research Problem* (2) *Literature Review* (3) *Soft System Methodology for IDFIF* (4) *Case Study* (5) *Evaluation Result* (6) *Analysis and Evaluation* (7) *Conclution*.

1.7. Review Penelitian

Soft system methodology telah banyak diterapkan di dunia teknologi informasi dan hasil rekomendasinya telah banyak membantu organisasi/perusahaan memperbaiki sistem menjadi lebih baik. Penelitian dalam institusi pendidikan di afrika yang dilakukan oleh Maduhu, dkk. (2015) menjelaskan bahwa ada 64 situs pendidikan tinggi rentan terkena serangan computer. Salah satu serangan yang telah teridentifkasi dalam aplikasi web tersebut adalah *bug heartbleed* yang merupakan kelemahan yang ditemukan dalam *OpenSSL*, *open source software* kriptografi. Untuk melakukan evaluasi

tersebut, maka pendekatan yang dipilih adalah *Soft System Methodology* karena, dengan metode tersebut dapat diketahui kebutuhan untuk mengambil langkah-langkah keamanan yang sesuai pada masing-masing komponen *website* tersebut.

Penerapan *soft system methodology* juga dilakukan oleh Rachman (2014) pada institusi kesehatan yang membahas tentang evaluasi alur sistem informasi kesehatan beserta perbaikannya yang kemudian di aplikasikan pada sebuah organisasi, yaitu puskesmas Cipedes untuk melihat kinerja alur sistem informasi yang ada.

Parra, dkk. (2013) melakukan penelitian di bidang *enterprise computer security* pada perusahaan di Mexiko dengan menggunakan pendekatan *soft system methodology* yang kemudian membahas tentang bagaimana cara melakukan evaluasi perencanaan penanganan keamanan computer sehingga menghasilkan tahapan-tahapan penanganan computer yang lebih baik dari yang telah ada sebelumnya.

Sabbagh & Kowalski (2013) melakukan evaluasi terhadap keamanan computer pada suatu organisasi dengan menerapkan *soft system methodology*. SSM ini dipilih karena memungkinkan analis keamanan computer untuk menganalisa kasus-kasus nyata sehingga dapat diketahui berbagai kemungkinan tersiko yang akan terjadi terhadap keamanan computer dalam suatu organisasi dan kemudian melakukan perbaikan mekanisme yang sedang digunakan untuk diterapkan pada organisasi tersebut. Gutmann (2013) juga melakukan penelitian terhadap keamanan computer dan menemukan beberapa kelemahan atau celah yang menyebabkan kebocoran informas. Untuk mengatasi masalah terebut, maka dipilihlah pendekatas SSM dengan tujuan dapat memberikan solusi terhadap pengguna akhir dalam menangani masalah keamanan komputer.

Lusa (2010) menerapkan *soft system methodology* di institusi pendidikan untuk melakukan evaluasi sistem informasi akademik pada universitas XYZ. Dalam penelitian ini juga melakukan identifikasi tantangan dan permasalahan yang kongkret terjadi sebagai pembelajaran yang memberikan gambaran pengembangan dan penerapan sistem informasi akademik tersebut sehingga menjadi lebih baik dari sebelumnya. Cox (2010) melakukan evaluasi di beberapa

perguruan tinggi dengan menggunakan *soft system methodology*. Dari hasil penelitian tersebut tidak banyak system *e-learning* yang digunakan dalam proses pembelajaran dikarenakan kurang inovasi sehingga ada beberapa proses bisnis yang perlu diubah dan kemudian menerapkan system e-learning yang telah dievaluasi.

Andini (2009) melakukan analisa dan evaluasi terhadap pembangunan system pendukung keputusan dalam perencanaan transportasi untuk penanganan kemacetan di kota XYZ. Pendekatan yang dipilih adalah menggunakan *soft system methodology* dan *conceptagon analytical tools*. SSM merupakan bentuk sederhana pendekatan system yang memandang problem secara utuh tanpa menghilangkan kondisi yang sebenarnya dihadapi. SSM ini digunakan untuk menangani kompleksitas dalam pembuatan sistem pendukung keputusan dalam perencanaan transportasi untuk penanganan kemacetan.

Ramabhadran (2007) menyebutkan banyak model forensik digital yang diusulkan di berbagai belahan dunia. Namun tidak ada kerangka yang tepat karena setiap kerangka hanya dapat bekerja dengan baik dengan jenis investigasi tertentu. *Windows Mobile Forensics Process Model* (WMFPM) dikembangkan untuk membantu praktisi forensik dan aparat penegak hukum dalam penyelidikan kejahatan yang melibatkan perangkat *windows mobile*. Yu, dkk. (2009) juga mengembangkan *Symbian Smartphones Forensic Process Model* (SSFPM) yang dikhususkan untuk perangkat *symbian smartphone* sehingga dapat membantu praktisi forensik dan aparat penegak hukum dalam penyelidikan kejahatan. ACPO (2011) dan NIST (2014) menyatakan bahwa dalam proses investigasi terhadap barang bukti digital tidak akan selalu sama, karena setiap barang bukti digital yang ditemukan akan selalu berbeda. Sehingga, untuk mengatasi hal tersebut haruslah dibuat model *digital forensics investigation* yang lebih dinamis.

Goel, dkk. (2012) smartphone memiliki fungsi sama dengan komputer, namun ada beberapa perbedaan dalam proses penanganan *digital forensics* diantara perangkat komputer dan *smartphone* sehingga diperlukan *Smartphone Forensics Investigation Process Model* (SFIPM) untuk proses investigasi terhadap segala jenis perangkat *smartphone* untuk membantu aparat penegak hukum dalam

proses penyelidikan. ISO (2014) membuat suatu model yang dapat diterapkan pada proses *smartphone investigation*. Adapun model yang dapat digunakan untuk proses *smartphone investigation* ISO/ IEC 27041

Raymond & Venter (2014) melakukan evaluasi dan pengujian terhadap *Harmonised Digital Forensic Investigation Process* (HDFIP) untuk proses penanganan *smartphone*. Hasil dari pengujian tersebut, model HDFI tidak hanya diterapkan pada penanganan komputer forensik, tetapi dapat diterapkan juga pada proses penanganan *smartphone*. Rahayu (2014) menyatakan tidak ada *framework* standar dalam proses *digital investigation* sehingga diperlukan suatu framework yang yang dapat mengakomodir seluruh tahapan dalam proses investigasi barang bukti digital. Dalam penelitian tesisnya telah menghasilkan metodologi berdasarkan konsep *Integrated Digital Forensics Investigation Framework* (IDFIF) yang diharapkan dapat menjadi standar metode penyelidikan para penyidik.

Merujuk pada penelitian terdahulu, maka tabel perbandingan penelitian seperti yang tertera pada tabel 1.1.

Tabel 1.1. Perbandingan Penelitian Terdahulu

No	Isu	Peneliti	Hasil	Ket.
1	Evaluasi *framework* penanganan keamanan *website* perguruan tinggi menggunakan SSM	Maduhu, dkk. (2015)	*Framework* yang lebih baik dalam penanganan masalah keamanan *website* perguruan tinggi di Afrika	
2	Evaluasi alur sistem informasi puskesmas menggunakan SSM	Rachman (2014)	Penerapan hasil perbaikan aplikasi sistem informasi yang dapat membantu berjalannya pelayanan puskesmas secara terkomputerisasi pada transaksi pasein	
3	Evaluasi *framework* untuk menangani masalah keamanan komputer menggunakan SSM	Parra, dkk. (2013)	*Framework* penanganan masalah keamanan komputer pada perusahaan - perusahaan besar di Meksiko	

Lanjutan Tabel 1.1. Perbandingan Penelitian Terdahulu

No	Isu	Peneliti	Hasil	Ket.
4	Evaluasi *framework* untuk menangani masalah keamanan komputer menggunakan SSM	Sabbagh & Kowalski (2013)	*Framework* baru tentang penanganan masalah keamanan komputer dalam suatu organisasi.	
5	Evaluasi *framework* untuk menangani masalah keamanan komputer menggunakan SSM	Gutmann (2013)	*Framework* baru dalam penanganan keamanan komputer yang lebih *fleksible* untuk pengguna akhir komputer	
6	Evaluasi *Action plan* untuk perubahan sisfokampus menggunakan SSM	Lusa & Iskandar (2012)	*Action plan* untuk perubahan sisfokampus sehingga menjadi lebih baik dari segi kelayakan dan aspek organisi secara menyeluruh di perguruan tinggi X	
7	Evaluasi sistem *e-learning* menggunakan SSM	Cox (2010)	Perbaikan sistem *e-learning* di perguruan tinggi Afrika Selatan	
8	Analisis dan evaluasi penanganan kemacetan lalu lintas menggunakan SSM	Andini (2009)	*Framework* perancangan Sistem Pendukung Keputusan yang lebih baik dalam menangani kemacetan lalu lintas serta menerapkan aplikasi pendukung keputusan tersebut	
9	DFIF hanya dapat bekerja dengan baik pada jenis investigasi tertentu.	Ramabhadran (2007)	*Windows Mobile Forensics Process Model* (WMFPM)	
10	Tidak ada *framework* khusus untuk *symbian smartphone investigation*	Yu, dkk. (2009)	*Symbian Smartphones Forensic Process Model* (SSFPM)	
11	Barang bukti yang ditemukan di TKP tidak selalu sama	ACPO (2011)	ACPO Guidelines Computer Evidence	
12	Tidak ada *framework* standar dalam proses *smartphone investigation*	Goel, dkk. (2012)	*Smartphone Forensics Investigation Process Model* (SFIPM)	
13	Proses *smartphone investigation* harus menggunakan *framework* khusus	ISO (2014)	ISO/IEC 27041	

Lanjutan Tabel 1.1. Perbandingan Penelitian Terdahulu

No	Isu	Peneliti	Hasil	Ket.
14	Barang bukti yang ditemukan di TKP tidak selalu sama	NIST (2014)	Guidelines on Mobile Device Forensics	
15	Pengujian *Harmonised Digital Forensic Investigation Process* (HDFIP) pada penanganan *smartphone forensics*	Raymond & Venter (2014)	Penerapan *Harmonised Digital Forensic Investigation Process* (HDFIP) pada penanganan *smartphone forensics*	
16	Tidak ada *framework* standar dalam proses digital investigation	Rahayu (2014)	*Integrated Digital Forensics Investigation Framework* (IDFIF)	

Melihat pada tabel 1.1. sangat jelas bahwa evaluasi yang menggunakan *soft system methodology* di bidang *digital forensics* belum pernah dilakukan sehingga perlu dilakukan uji coba terhadap evaluasi tahapan IDFIF karena pada penelitian sebelumnya belum dilakukan evaluasi dalam penanganan *smartphone.*

1.8. Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian yang dibuat , maka dibuat sistematika penulisan pada penelitian ini :

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta sistematika penulisan.

BAB II KAJIAN TEORI

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan *smartphone,* DFIF untuk *smartphone investigation,* IDFIF dan *Soft System Methodology.*

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langlah-langkah penelitian dan gambaran umum langkah penyelesaian. Berisi tentang arsitektur, model simulasi, skenario evaluasi.

BAB IV PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat, evaluasi dan penentuan hasil analisis.

BAB V KESIMPULAN DAN SARAN

Simpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.