Analisis Kelayakan *Integrated Digital Forensics Investigation Framework* Untuk Investigasi *Smartphone*

Ruuhwan[1], Imam Riadi[2], Yudi Prayudi[3]
[1]Teknik Informatika, Universitas Perjuangan, Jl. Pembela Tanah Air 177, Tasikmalaya
[1,3]Magister Teknik Informatika, Universitas Islam Indonesia, Jl. Kaliurang KM 14,5 Yogyakarta
[2]Teknologi Industri, Universitas Ahmad Dahlan, Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta
E-mail: [1]ruuhwan@yahoo.com, [2]imam.riadi@is.uad.ac.id, [3]prayudi@uii.ac.id

Masuk: 24 Februari 2016; Direvisi: 29 Maret 2016; Diterima: 3 April 2016

Abstract. *The handling of digital evidence each and every digital data that can proof a determination that a crime has been committed; it may also give the links between a crime and its victims or crime and the culprit. How to verify a valid evidence is to investigate using the approach known as the Digital Forensic Examination Procedures. Integrated Digital Forensic Investigation Framework (IDFIF) is the latest developed method, so that it is interesting to further scrutinize IDFIF, particularly in the process of investigation of a smartphone. The current smartphone devices have similar functions with computers. Although its functions are almost the same as the computer, but there are some differences in the process of digital forensics handling between computer devices and smartphones. The digital evidence handling process stages need to overcome the circumstances that may be encountered by an investigator involving digital evidence particularly on electronic media and smartphone devices in the field. IDFIF needs to develop in such a way so it has the flexibility in handling different types of digital evidence.*
Keywords*: digital evidence, IDFIF, investigation, smartphone*

Abstraks. *Penanganan bukti digital mencakup setiap dan semua data digital yang dapat menjadi bukti penetapan bahwa kejahatan telah dilakukan atau dapat memberikan link antara kejahatan dan korbannya atau kejahatan dan pelakunya. Cara pembuktian untuk mendapatkan bukti valid adalah dengan melakukan investigasi dengan pendekatan Prosedur Pemeriksaan Digital Forensic. Integrated Digital Forensics Investigation Framework (IDFIF) merupakan metode terbaru sehingga IDFIF ini menarik untuk diteliti lebih lanjut terutama dalam proses investigasi smartphone. Saat ini perangkat smartphone memiliki fungsi yang sama dengan komputer. Meskipun demikian, ada beberapa perbedaan dalam proses penanganan digital forensics diantara perangkat komputer dan smartphone. Tahapan proses penanganan barang bukti digital seharusnya dibuat untuk mengatasi keadaan umum yang mungkin dihadapi oleh investigator yang melibatkan barang bukti digital terutama pada perangkat smartphone dan media elektronik terkait di lapangan. IDFIF perlu dikembangkan sehingga memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital.*
Kata Kunci*: bukti digital, IDFIF, investigasi, smartphone*

1. Pendahuluan

Penanganan bukti digital mencakup setiap dan semua data digital yang dapat menjadi bukti penetapan bahwa kejahatan telah dilakukan atau dapat memberikan *link* antara kejahatan dan korbannya atau kejahatan dan pelakunya (Ademu, dkk., 2011). Elemen yang paling penting dalam *digital forensic* adalah kredibilitas dari barang bukti digital tersebut (Agrawal, dkk. 2011). Cara pembuktian untuk mendapatkan bukti *valid* adalah dengan melakukan investigasi dengan pendekatan Prosedur Pemeriksaan *Digital Forensic* (Alharbi, dkk., 2011). Sejumlah tahapan pendekatan ini dalam penanganan bukti digital dikenal dengan istilah *Framework*. Tahapan penyelidikan harus sesuai dengan hukum dan ilmu pengetahuan yang ada dengan

menggunakan lima langkah yang berbeda dalam investigasi barang bukti untuk dipresentasikan di pengadilan yang terdiri dari *pre-process, acquisition & preservation, analysis, presentation* dan *post-process* (Yusoff, dkk., 2011).

Penyederhanaan tahapan *Digital Forensic Investigation Framework* (DFIF) yang terlalu banyak perlu dilakukan sehingga dari 15 langkah yang ada dapat disederhanakan menjadi lima tahapan umum DFIF pada semua kasus insiden tanpa merusak bukti dan melindungi *chain of custody* (Selamat, dkk., 2008). *Integrated Digital Forensics Investigation Framework* (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 (Rahayu & Prayudi, 2014).

IDFIF merupakan metode terbaru sehingga IDFIF ini menarik untuk diteliti lebih lanjut terutama dalam proses investigasi *smartphone*. *Smartphone* adalah telepon *Internet-enabled* yang biasanya menyediakan fungsi *Personal Digital Assistant* (PDA) seperti fungsi kalender, buku agenda, buku alamat, kalkulator, dan catatan (Farjamfar, dkk., 2014). *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* (Ayers, dkk., 2014).

Saat ini, di Indonesia ada empat jenis sistem operasi *smartphone* yaitu Android OS, Windows Phones OS, RIM OS dan iOS. Setiap sistem operasi pada *smartphone* terus mengalami perkembangan sehingga memiliki beberapa versi salah satunya adalah Android OS. Android OS memiliki beberapa versi berdasarkan perkembangannya sejak dirilis pertama kali hingga sekarang yaitu Android CupCake(1.5), Android Donut(1.6), Android Eclair(2.0-2.1), Android Froyo(2.2), Android GinggerBread(2.3-2.3.7), Android Honeycomb(3.1-3.2), Android Ice Cream Sandwich(4.0.3-4.0.4), Android Jelly Bean(4.1-4.3), Android KitKat(4.4) dan Android Lollipop (5.0).

Saat ini perangkat *smartphone* memiliki fungsi yang sama dengan komputer. Meskipun fungsinya sama dengan komputer, namun ada beberapa perbedaan dalam proses penanganan *digital forensics* diantara perangkat komputer dan *smartphone* karena *smartphone* memiliki karakteristik yang unik sehingga tidak bisa disamakan dengan penanganan komputer biasa (Ademu, dkk., 2011). Sehubungan dengan alasan tersebut, diperlukan adanya analisis kelayakan IDFIF terhadap investigasi *smartphone* untuk mengetahui kelebihan dan kekurangan dari model IDFIF tersebut. Tujuan dari penelitian ini adalah melakukan penerapan model IDFIF dalam proses investigasi *smartphone*. Analisis ini juga menghasilkan rekomendasi perbaikan yang harus dilakukan sehingga model IDFIF tersebut dapat digunakan dalam proses investigasi terhadap setiap jenis barang bukti digital yang ditemukan.

2. Kajian Pustaka

2.1. Forensika Digital

Forensika digital merupakan ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisis terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan (Kalbande & Jain, 2013). Ilmu forensika digital memiliki empat prinsip dasar (Goel, dkk., 2012), yaitu: (1) Sebuah lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang akan dibawa ke pengadilan. (2) Seseorang yang mengakses data digital yang tersimpan dalam media penyimpanan barang bukti haruslah memiliki kompetensi, relevansi dan implikasi dari tindakan yang dilakukan terhadap barang bukti. (3) Harus ada catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan sehingga ketika ada pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama. (4) Setiap orang yang terlibat dalam proses investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan analisis untuk memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

2.2. Perbedaan *Computer Forensics* Dan *Smartpone Forensics*

Saat ini perangkat *smartphone* memiliki fungsi yang sama dengan komputer namun ada beberapa perbedaan dalam proses penanganan *digital forensics* diantara perangkat komputer dan *smartphone* (Ayers, dkk., 2014). Perbedaan tersebut dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan *Computer & Smartphone Forensics*

Aspect	*Computer Forensics*	*Smartphone Forensics*
Konektivitas	Terbatas	Tidak Terbatas
Sumber Bukti	*Hard disc.*, RAM, *External storage*	SIM *card*, RAM, ROM, *External Memory, Network Data*
Melepas *Internal Storage*	Ya	Tidak
Melewati Sandi	Ya	Tidak Bisa Melewati Sandi Saat Melakukan *Logical Acquisition*
Daya Dan Kabel Data	Standar	Berbagai Kabel Daya Dan Data
File System	Sistem *File* Standar	Berbagai Sistem *File*

2.3. Potensi Bukti Digital Pada *Smartphone*

Informasi-informasi yang tersimpan pada *smartphone* tersebut berada pada beberapa media penyimpanan yang berbeda (Ayers, dkk., 2014). Adapun jenis media penyimpanan tersebut adalah (1) SIM *(Subscriber Identity Module) Card*, (2) *Electronically Erasable And Programable Read-Only Memory* (EEPROM), (3) *Random Acces Memory* (RAM), (4) *Flash Read-Only Memory* (ROM), (5) Memori Eksternal (*External Memory*), dan (6) *Network Data*.

SIM *Card* memiliki fungsi hanya untuk menyimpan data-data tertentu yang sifatnya terbatas yaitu sebagai berikut: (a) *Phonebook*: merupakan *contact-contact* yang berisi nomor telepon yang berasosiasikan dengan nama tertentu yang dibuat oleh pemilik *smartphone* secara manual. *Phonebook* pada *smartphone* tidak hanya menyimpan nama dan nomor saja namun juga dapat menyimpan beberapa informasi lainnya seperti alamat rumah, alamat perusahaan dan alamat *e-mail*. (b) *Call log*: berisi catatan panggilan yang pernah terjadi seperti panggilan masuk, panggilan keluar dan panggilan tak terjawab termasuk waktu dan durasi percakapan. (c) *Short Message Service*: pesan (teks) singkat baik pesan masuk, pesan keluar dan pesan tersimpan. Penyimpanan SMS di SIM *card* bersifat terbatas dan hanya dapat menyimpan 40 SMS. (d) *Integrated Circuit Card Identifier* (ICCID): merupakan angka unik yang merupakan identitas dari *provider* untuk setiap SIM *card* guna keperluan yang bersifat administratif. (e) *International Mobile Subscriber Identity* (IMSI): merupakan identitas yang unik untuk setiap *subscriber* yang diberikan oleh *provider* ketika *subscriber* menggunakan jaringannya setelah melalui proses otentifikasi sebelumnya. *Provider* menggunakan nomor IMSI untuk mengizinkan SIM *card* yang satu berkomunikasi dengan SIM *card* yang lain didalam jaringannya.

EEPROM merupakan tempat penyimpanan data-data *default* (yang berasal dari pabrikan) seperti: (a) system operasi dan aplikasi-aplikasi *default*. (b) *International Mobile Equipment Identity* (IMEI): merupakan identitas (ID) yang unik bagi masing-masing *handphone/smartphone* GSM yang terorganisasi secara internasional. (c) *Electronic Serial number* (ESN): merupakan identitas *handphone/smartphone* yang berbasis jaringan *Code Division Multiple Access* (CDMA).

RAM berfungsi untuk menyimpan data yang bersifat temporer yang berasal dari berbagai aplikasi. Data-data yang tersimpan bersifat *volatile*, yaitu hanya ada selama *handphone/smartphone* tersebut hidup (*on*) dan akan hilang ketika *handphone/smartphone* itu dimatikan (*off*). *Flash Read-Only Memory* (ROM) sama dengan EEPROM sering kali dikenal dan disebut sebagai memori internal *handphone/smartphone. Flash* ROM ini memiliki ukuran yang cukup besar untuk *smartphone* sehingga *flash* ROM dapat menyimpan data-data berupa *phonebook*, call log, SMS/MMS, *file-file* audio, *file-file* video, *file-file* gambar, calendar, data-data penggunaan internet dan aplikasi tambahan. Memori Eksternal (*External Memory*) merupakan media penyimpanan data yang bersifat eksternal dengan menggunakan *memory card*. Memori eksternal juga menyimpan banyak data seperti *file-file* audio, *file-file* video, *file-file* gambar, *file-file office* dan aplikasi tambahan.

Network Data merupakan penyimpanan data-data yang tersimpan di jaringan *provider/*penyedia layanan. Adapun cakupan *network data* tersebut adalah: (a) *Call Data Record* (CDR): berisi catatan panggilan (*call logs*) dan pesan SMS yang dibuat oleh masing-masing *subscriber*. Penyimpanan CDR di jaringan *provider* ini dibatasi oleh rentan waktu. Untuk itu, semakin cepat *forensic analysis* dan *investigator* datang ke *provider* untuk meminta CDR dari nomor *subscriber* tertentu semakin baik. (b) *Voice Mails*: dikenal juga sebagai kotak suara yang merupakan pesan dari *caller* (pemanggil) yang tidak terjawab oleh *recipient* (yang dipanggil/penerima panggilan) kemudian tersambung dengan *recorder* (alat rekam suara) dari *provider* untuk merekam pesan dari *caller* dan *provider* akan memberikan pemberitahuan akan adanya *voice mail* ke *recipient*. Selanjutnya ketika *recipient* memegang dan mengakses *handphone/smartphone*, maka *recipient* akan mengetahui bahwa ada *voice mails* dan selanjutnya *recipient* akan mengakses nomor tertentu yang telah disediakan oleh *provider* untuk mendapatkan/mengetahui *voice mails* tersebut. (c) *Mobile Subscriber Integrated Service Digital Network* (MSISDN): merupakan nomor panggilan yang unik untuk setiap *subscriber*. MSISDN ini tidak tersimpan di SIM *card*. Di Indonesia, MSISDN ini diawali dengan digit +62xx dimana xx merupakan digit unik yang diberikan oleh otorisasi telekomunikasi untuk masing-masing *provider* setiap produknya. (d) *Cloud Storage*: merupakan media penyimpanan data yang dapat diakses dimana saja dan kapan saja melalui perantara jaringan yang terintegrasi dan tersinkronisasi melalui internet.

2.4. Penanganan *Smartphone*

Smarphone memiliki fasilitas koneksi jaringan yang selalu terhubung dengan lalulintas data atau internet setiap saat sehingga proses investigasi *smarphone* akan lebih sulit daripada proses investigasi komputer (Pilli, dkk., 2010). Beberapa prosedur yang harus dilaksanakan dalam penanganan barang bukti *smartphone* (Goel, dkk., 2012) yaitu: (1) Apabila *smartphone* dalam keadaan nyala (*ON*) maka yang harus dilakukan adalah: (a) Biarkan *smartphone* tersebut dalam keadaan menyala. (b) Pastikan arah komunikasi perangkat elektronik temuan dan mekanisme yang diperlukan untuk barang bukti tersebut seperti (penelusuran, pemutusan, pemblokiran dll). (c) *Recovery* sistem dan mengumpulkan bukti temuan pelacakan jaringan. (d) Temukan kegiatan mencurigakan yang dihasilkan dari kegiatan pengumpulan barang bukti. (e) Dokumentasi TKP seperti pengisian chain custody dan memotret detail TKP. (f) Simpan data/kegiatan yang mencurigakan melalui metode *hashing*. (g) *Live analysis* terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian. (h) Buat laporan awal atas kegiatan penyelidikan proaktif yang telah dilakukan. (i) Lakukan analisis terhadap *smartphone*. (2) Apabila *smartphone* dalam keadaan mati (*OFF*) maka yang harus dilakukan adalah: (a) Biarkan *smartphone* tersebut dalam keadaan mati dan jangan menghidupkan kembali *smartphone*. (b) *Documenting the Scene*, ditahap ini dilakukan dokumentasi TKP seperti pengisian *chain custody* dan memotret detail TKP. (c) Lakukan analisis terhadap *smartphone*.

2.5. *Smartphone Forensics Investigation Framework*

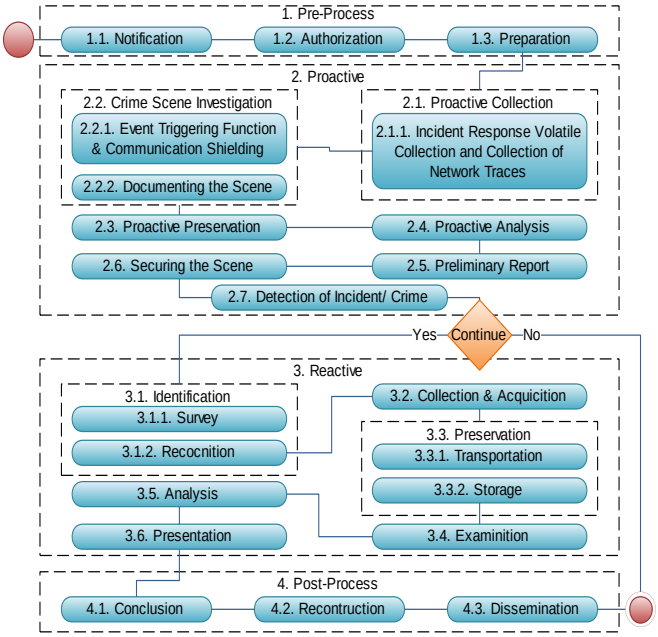
Smartphone forensics investigation framework adalah pola kerja dalam menangani *smartphone forensic*. Setiap *framework* memiliki pola kerja serta kelebihan dan kekurangan yang berbeda-beda namun memiliki tujuan akhir yang sama. Metodologi forensika digital memiliki lima tahapan umum yang terdiri dari (1) *Pre-process.* (2) *Acquicition & preservation.* (3) *Analisys.* (4) *Presentation.* dan (5) *Post-process* (Yusoff, dkk., 2011).

Smartphone forensic investigation process model (SFIPM) dirancang khusus untuk penanganan *smartphone forensics* terdiri dari beberapa tahapan, yaitu (1) *Preparation & securing the scene.* (2) *Documentation.* (3) *PDA mode.* (4) *Communication shielding.* (5) *Evidence collection.* (6) *Preservation.* (7) *Examination.* (8) *Analysis.* (9) *Presentation.* dan (10) *review* (Goel, dkk., 2012). Selain itu juga, *Smartphone forensics process model* (SFPM) yang khusus digunakan untuk perangkat *symbian smartphone* memiliki lima tahapan, yaitu (1) *Preparation and identification.* (2) *Remote evidence acquisition.* (3) *Internal evidence acquisition.* (4) *Analysis.* dan (5) *Presentation and review* (Mohtasebi & Dehghantanha, 2013).

NIST membuat panduan penanganan *smartphone* yang dimaksudkan untuk mengatasi keadaan umum yang mungkin dihadapi oleh staf keamanan yang melibatkan barang bukti digital yang terdapat pada perangkat *smartphone* dan media elektronik terkait. Proses penanganan *smartphone forensic investigation* itu terdiri dari empat tahap yaitu: (1) *preservation (securing and evaluating the scene, documenting the scene, isolation, packaging/seize, transporting, storing evidence, triage processing, decision making),* (2) *acquicition,* (3) *examination & analysis* dan (4) *reporting* (Ayers, dkk., 2014).

2.6. *Integrated Digital Forensics Investigation Framework* (IDFIF)

IDFIF *(Integrated Digital Forensic Investigation Framework)* merupakan *framework* yang dibangun dengan melakukan analisis dan evaluasi terhadap *framework-framework forensics* yang sudah ada sebelumnya. *Framework* dievaluasi untuk menghasilkan sebuah *framework* baru yang lebih ringkas dan detail (Rahayu & Prayudi, 2014) seperti pada Gambar 1.



Gambar 1. Model *IDFIF*

Gambar 1 merupakan hasil penelitian yang memiliki beberapa tahapan dalam penanganan barang bukti digital, yaitu: (1) *Pre-Process* merupakan tahapan permulaan yang terdiri dari: (a) *Notification.* Pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum. (b) *Authorization.* Tahapan untuk mendapatkan hak akses terhadap barang bukti dan status hukum proses penyelidikan. (c) *Preparation.* Persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan. (2) Dalam tahapan *Proactive* terdapat tujuh tahapan pendukung yakni: (a) *Proactive Collection* merupakan tindakan cepat mengumpulkan barang bukti ditempat kejadian perkara(TKP). Tahapan ini termasuk *Incident response volatile collection and Collection of Network Traces. Incident response volatile collection* sendiri merupakan mekanisme penyelamatan dan pengumpulan barang bukti, terutama yang bersifat *volatile. Collection of Network Traces* adalah mekanisme pengumpulan barang bukti dan melacak rute sampai ke sumber barang bukti yang berada dalam jaringan. Tahapan ini juga memperhitungkan keberlangsungan sistem dalam pelaksanaan pengumpulan barang buktinya. (b) *Crime Scene Investigation* sendiri terdiri dari tiga tahapan pokok yakni *Event triggering function & Communicating Shielding* dan *Documenting the Scene.* Tujuan pokok dari tahapan ini adalah mengolah TKP, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil gambar setiap detail TKP. (c) *Proactive preservation* ini adalah tahapan untuk

menyimpan data/kegiatan yang mencurigakan melalui metode *hashing*. (d) *Proactive Analysis* adalah tahapan *live analysis* terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian. (e) *Preliminary Report*, merupakan pembuatan laporan awal atas kegiatan penyelidikan proaktif yang telah dilakukan. (f) *Securing the Scene* ditahap ini dilakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti. (g) *Detection of Incident / Crime,* ditahap ini adalah tahap untuk memastikan bahwa telah terjadi pelanggaran hukum berdasarkan *premilinary report* yang telah dibuat. Akhir dari tahap *proactive* terdapat *decision process*. Tahapan ini memang tidak disebut secara langsung menjadi tahapan, namun *output* dari *decision* ini juga penting untuk keberlangsungan proses penyelidikan. Tahapan ini diputuskan penyelidikan cukup kuat untuk dilanjutkan atau tidak. (3) Tahapan *Reactive* merupakan tahapan penyelidikan secara tradisional meliputi enam tahapan yaitu: (a) *Identification.* Melakukan identifikasi TKP yang mencakup memotret, sketsa, pemetaan TKP, pengolahan *chain custody* sampai mencatat siapa saja yang terlibat dalam TKP. (b) *Collection & Acquisition.* Proses pengumpulan barang bukti fisik ataupun digital baik *volatile* maupun *non-volatile*. (c) *Preservation.* Menjaga integritas temuan dengan menggunakan *chain custody* dan fungsi *hashing.* (d) *Examination.* Pengolahan barang bukti untuk menemukan keterkaitanya dengan kejadian (e) *Analysis.* Merupakan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada. (f) *Presentation*. Seluruh temuan dan keterkaitannya disusun dalam bentuk yang mudah dipahami. (4) Tahapan *Post-Process* merupakan tahap penutup investigasi yang terdiri dari: (a) *Conclusion*. Menyimpulkan hasil dari investigasi yang telah dilakukan. (b) *Recontruction*. Proses analisis dan evaluasi keseluruhan terhadap hasil investigasi. (c) *Dissemination*. Pencatatan proses penyelidikan dan catatan tersebut dapat disebarluaskan pada penyelidik lain yang melakukan penyedikan pada kasus serupa.

3. Metodologi Penelitian

Secara ringkas metode dan tahapan penelitian yang dilakukan dapat digambarkan seperti pada Gambar 2. *Research problem* merupakan langkah awal yang dilakukan untuk memperoleh dan menentukan topik penelitian yang akan diteliti. *Literature review* menggali seluruh informasi yang terkait dengan permasalahan yang akan diteliti dan obyek yang menjadi tujuan penelitian serta memberikan dasar bagi arah penelitian yang akan dilakukan serta menjadi awal pemikiran sehingga penelitian yang dilakukan dapat dijadikan acuan kembali dikemudian hari. *Analysis* merupakan proses penerapan IDFIF terhadap proses investigasi *smartphone*. *Conclusion* merupakan kesimpulan dari seluruh tahapan yang telah dilakukan dalam proses penelitian ini.

Gambar 2. Metodologi

4. Analisis

4.1. Skenario Kasus

Skenario kasus dan simulasi didalam penelitian ini disesuaikan dengan kasus penipuan melalui pesan singkat (SMS) yang mengadopsi dari kasus yang telah terjadi beberapa waktu yang lalu. Kasus tersebut adalah penipuan undian berhadiah. Perangkat *mobile* yang digunakan untuk mengirimkan SMS ke korban adalah Lenovo S860. Pelaku mengirimkan SMS ke korban dengan isi pesan bahwa korban telah memenangkan undian berhadiah dari PT. X berupa satu unit mobil Y senilai 400 juta rupiah dan korban diperintahkan untuk mengubungi nomor yang telah ditentukan oleh pelaku. Korban melakukan apa yang diperintahkan oleh pelaku tanpa memperhatikan nomor pengirim SMS. Korban diperintahkan untuk mengirimkan uang ke rekening pelaku sebesar 10% dari nilai hadiah tersebut untuk biaya administrasi dan biaya pengiriman hadiah tersebut. Tanpa berpikir panjang, akhirnya korban melakukan transfer uang sebesar 10% dari nilai hadiah yang akan diterima. Korban merasa tertipu terhadap SMS yang diterimanya setelah melakukan pengiriman sejumlah uang ke rekening yang telah ditentukan

pelaku sehingga korban melaporkan kejadian ini kepada pihak yang berwajib. Adapun *smartphone* pelaku yang ditemukan di TKP berada dalam kondisi menyala.

4.2. Hasil dan Pembahasan

Model IDFIF ini memiliki tahapan yang sangat lengkap dibandingkan model-model DFIF sebelumnya karena model IDFIF ini mengakomodir setiap tahapan dari model-model DFIF yang ada sehingga dalam menangani kasus penipuan ini, investigator menerapkan model IDFIF untuk menyelesaikan kasus ini. Secara umum, tahapan proses investigasi terhadap barang bukti digital baik itu komputer ataupun *smartphone* memiliki empat tahapan utama, yaitu persiapan (*pre-process*), olah TKP (*proactive process*), pemeriksaan barang bukti di laboratorium *digital forensics* (*reactive process*) dan laporan hasil pemeriksaan barang bukti digital (*post-pocess*).

4.2.1. *Pre-Process*

Pre-process merupakan tahapan awal dalam proses investigasi barang bukti digital terutama pada investigasi *smartphone*. Tahapan ini dilakukan untuk melakukan berbagai persiapan dalam proses investigasi baik peralatan dan juga dokumen-dokumen yang diperlukan. Tahapan ini dibagi menjadi tiga sub tahapan yaitu: (1) *Notification*: Korban melaporkan kasus penipuan yang dialaminya kepada pihak penegak hukum untuk dilakukan proses penyelidikan. Lembaga penegak hukum yang bertanggung jawab dapat ditentukan oleh kriteria geografis (lokasi TKP) atau sifat insiden kejahatan. Pemberitahuan ini sangat penting, karena informasi yang dikumpulkan disini dapat menentukan langkah berikutnya dalam penyelidikan. (2) *Authorization*: Penegak hukum melaksanakan kerjasama dan mengurus proses perizinan kepada operator seluler untuk mendapatkan hak akses dalam proses pelacakan terhadap pelaku penipuan. (3) *Preparation*: Penegak hukum harus mempersiapkan segala kebutuhan dalam proses investigasi mulai dari personil, peralatan penyelidikan, perangkat keras hingga perangkat lunak. Peralatan yang digunakan dalam proses investigasi *smartphone* dapat dilihat pada Tabel 2.

Tabel 2. Peralatan yang diperlukan untuk proses investigasi *smartphone*

Peralatan	Kegunaan
Media Penyimpanan	Digunakan untuk menyimpan salinan bukti digital yang telah diperoleh selama penyelidikan.
Kamera Digital	Digunakan untuk mengambil gambar di TKP sebagai bukti bahwa telah terjadi suatu kejahatan
Faraday Bag	Sebuah tas yang digunakan untuk mengamankan *smartphone* dari komunikasi data.
Portable Power Supply	Merupakan sebuah alat penambah daya baterai *smartphone* dan digunakan untuk menjaga kondisi *smartphone* dalam kondisi "*on*"
USB Dongle	Digunakan untuk menghubungkan *smartphone* ke komputer untuk mendapatkan akses penuh terhadap *smartphone* tersebut
Mobile Edit 7.5	Merupakan aplikasi yang digunakan untuk melakukan proses analisis terhadap *smartphone* yang ditemukan di TKP.
Perangkat Komputer	Digunakan untuk melakukan proses pemindahan data digital dari *smartphone* ke media penyimpanan untuk dilakukan proses analisis

4.2.2. *Proactive Process*

Proactive Process merupakan tahapan awal yang dilakukan dalam proses investigasi. Adapun sub tahapannya adalah sebagai berikut: (1) *Proactive Collection*: Investigator mengumpulkan bukti dari korban berupa nomor *handphone* pelaku dan nomor ICCID dari operator seluler terkait untuk melakukan proses proses pelacakan terhadap pelaku penipuan tersebut. (a) *Incident Response Volatile Collection and Collection of Network Trace*: Investigator melakukan pelacakan untuk mendapatkan lokasi keberadaan pelaku penipuan tersebut. (2) *Crime Scene Investigation*: Ketika keberadaan pelaku penipuan telah diketahui, investigator bergegas menuju tempat persembunyiannya untuk melakukan proses penangkapan terhadap pelaku penipuan tersebut. Tempat yang digunakan pelaku penipuan untuk melakukan aksi penipuannya itu disebut dengan TKP. Di TKP investigator juga menemukan satu buah *smartphone* Lenovo S860 yang digunakan pelaku untuk melakukan aksi penipuannya. (a) *Event Triggering Function and Communication Shielding*: Investigator melakukan proses pencarian

pemicu kejadian di TKP sehingga investigator dapat menyimpulkan sementara jenis kejahatan yang telah dilakukan untuk proses analisis lebih lanjut di laboratorium *digital forensic*. Selanjutnya, setelah menemukan pemicu kejadian kejahatan tersebut. Investigator harus melakukan pemutusan komunikasi data pada *smartphone* untuk menghindari terkontaminasinya data yang ada dalam *smartphone* tersebut dengan cara memasukan perangkat tersebut kedalam *faraday bag*. Keadaan *smartphone* pada saat disimpan dalam *faraday bag* dalam kondisi menyala, akan menghabiskan banyak daya baterai karena ketika koneksi data terputus, kerja *smartphone* dalam mencari jaringan seluler akan semakin keras sehingga diperlukan *portable power supply* untuk menjaga kondisi *smartphone* dalam keadaan menyala. (b) *Documenting the Scene*: Investigator harus mendokumentasikan TKP dengan cara memotret keadaan TKP dan semua barang bukti yang yang telah ditemukan di TKP termasuk perangkat *smartphone* ataupun barang bukti yang dapat menyimpan data bersama dengan semua *peripheral* kabel, konektor daya, *removable* media dan konektifitas tanpa menyentuh perangkat tersebut saat memotret pada lingkungan dimana perangkat itu ditemukan. Jika layar perangkat dalam keadaan dapat dilihat, isi layar harus difoto dan jika perlu direkam secara manual untuk mendapatkan informasi waktu, status layanan, kondisi baterai, dan ikon yang ditampilkan. (3) *Proactive Preservationi*: Investigator tidak dapat melaksanakan sub proses ini pada proses investigasi *smartphone* karena seluruh dokumentasi kegiatan yang dilakukan tidak dilaksanakan di TKP. (4) *Proactive Analysis*: adalah tahapan *live analysis* terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian di TKP. Proses penanganan *smartphone* tidak bisa dilaksanakan di TKP karena dalam melakukan analisis *smartphone* harus dilakukan di tempat yang kedap frekuensi. (5) *Preliminary Report*: Merupakan pembuatan laporan awal atas kegiatan *proactive analysis* yang telah dilakukan. Proses ini tidak dapat dilakukan dalam penanganan *smartphone* karena analisis terhadap *smartphone* tidak dilakukan secara *live analysis* di TKP sehingga untuk laporan kegiatan dilakukan setelah pemeriksaan *smartphone* di laborotorium. (6) *Securing the Scene*: Investigator harus melaksanakan suatu proses untuk menjaga agar TKP berada dalam keadaan sebagaimana pada saat dilihat dan ditemukan petugas yang melakukan tindakan pertama di TKP sehingga barang bukti yang diperlukan tidak hilang, rusak, tidak ada penambahan atau pengurangan dan tidak berbeda letaknya yang berakibat menyulitkan atau mengaburkan pengolahan TKP dan pemeriksaan secara teknis ilmiah. (7) *Detection of Incident/Crime*: Investigator harus memastikan bahwa kegiatan yang dilakukan oleh pelaku tersebut adalah suatu kegiatan yang telah melanggar hukum.

4.2.3. *Reactive Process*

Reactive Process merupakan tahapan inti dari proses investigasi *smartphone*. Barang bukti yang telah didapatkan pada proses sebelumnya dilakukan analisis untuk mendapatkan bukti-bukti yang terkait dengan kejahatan yang terjadi. Tahapan ini dibagi menjadi beberapa tahapan yaitu: (1) *Identifications*: Investigator melakukan identifikasi terhadap barang bukti *smartphone* yang telah ditemukan di TKP dengan mencatat kode IMEI, merk *smartphone*, model *smartphone* dan nomor telepon yang terdapat pada smartphone tersebut. *Smartphone* tersebut kemudian difoto dan didokumentasikan berdasarkan *chain of custody*. (a) *Survey*: Tahap ini merupakan proses penggalian informasi awal di TKP, namun pada proses investigasi *smartphone* tahapan ini tidak digunakan. (b) *Recognition*: investigator harus melakukan proses sinkronisasi perangkat *smartphone* terhadap perangkat komputer untuk mendapatkan hak akses terhadap perangkat *smartphone* tersebut sehingga tahapan *Collection and Acquicition* dapat dilakukan. (2) *Collection and Acquicition*: Dalam beberapa kasus, terkadang memerlukan pengumpulan bukti fisik dan logis berupa ekstaksi data, namun dalam kasus ini, bukti-bukti yang diperlukan hanyalah catatan panggilan keluar dan panggilan masuk serta SMS keluar dan SMS masuk yang terletak dipenyimpanan internal *smartphone*. Bukti digital dikumpulkan mengunakan *mobile edit v 7.5*. (3) *Preservation*: Investigator harus melakukan pengamanan terhadap *smartphone* yang telah ditemukan di TKP yang selanjutnya harus dipindahkan ke laboratorium untuk proses analisis. (a) *Transportation*: Investigator harus melakukan proses pemindahan barang bukti digital dalam hal ini perangkat *smartphone* dari TKP menjuju ke

laboratorium untuk proses pemeriksaan lebih lanjut. Dalam proses tersebut, *smartphone* harus disimpan dalam keadaan yang sangat aman sehingga ketika sampai di laboratorium, *smartphone* tersebut tetap dalam kondisi yang baik. (b) *Storage*: Merupakan proses penyimpanan atau penggandaan hasil akuisisi dari perangkat *smartphone*. Proses ini sangat diperlukan untuk menjaga keamanan data yang telah didapat dengan cara melakukan proses pemeriksaan terhadap hasil duplikasi data yang telah diakuisisi dan menyimpan data yang aslinya. (4) *Examinition:* Investigator harus melakukan proses pemeriksaan untuk mengungkapkan bukti digital termasuk yang mungkin tersembunyi atau dihilangkan dalam perangkat *smartphone*. Hasilnya diperoleh melalui penerapan metode ilmiah dan harus menjelaskan isi dan keadaan data sepenuhnya. Proses pemeriksaan barang bukti digital harus dilakukan oleh seorang ahli forensik sedangkan untuk proses analisis dapat dilakukan dengan peran selain analisis forensik, seperti penyidik atau pemeriksa forensik. (5) *Analysis*: Tahapan selanjutnya dalam melakukan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada baik antara pelaku dengan *smartphone* yang didapat, *smartphone* yang didapat dengan korban dan pelaku dengan korban. (6) *Presentation:* Investigator merangkai temuan pada tahap *analysis* untuk disampaikan pada pihak yang memiliki otoritas. Temuan disajikan dalam bentuk yang mudah dipahami dan didukung dengan barang bukti yang cukup dan dapat diterima.

4.2.4. *Post-Process*

Post-Process merupakan tahap penutup investigasi. Tahapan ini mengolah barang bukti yang telah digunakan sebelumnya. Tahapan ini meliputi mengembalikan barang bukti pada pemiliknya, menyimpan barang bukti ditempat yang aman dan melakukan *review* pada investigasi yang telah dilaksanakan sebagai perbaikan pada penyelidikan berikutnya. (1) *Conclusion*: Bukti dan informasi yang ditemukan oleh investugator sudah cukup untuk tim investigasi untuk menuntut tersangka sms penipuan undian berhadiah dan dapat memasukkan pelaku ke dalam tahanan. (2) *Recontruction*: Selanjutnya investigator harus melakukan rekontruksi ulang berdasarkan hasil temuan dari analisis yang telah dilakukan sehingga proses kegiatan pelaku dapat diketahui lebih jelas dalam melakukan proses penipuan undian berhadiah. (3) *Dissemination*: Selanjutnya, tahapan terakhir adalah melakukan pencatatan terhadap proses investigasi sehingga apabila investigator lain mendapatkan kasus serupa, proses ini dapat dijadikan sebagai rujukan dalam proses investigasi *smartphone*.

4.3. Temuan dan Rekomendasi Perbaikan Model IDFIF

Berdasarkan hasil analisis yang telah dilakukan pada model IDFIF terhadap proses investigasi *smartphone*, maka ditemukan beberapa kekurangan sebagai berikut: (1) Tahapan *securing the scene* dilakuakan pada akhir proses olah TKP sehingga keadaan TKP selama proses investigasi tidak terjamin keamanannya. (2) Tahapan *documenting the scene* dilakukan pada pertengahan proses olah TKP sehingga ketika ada perubahan TKP tidak dapat diketahui. (3) Tahapan *Proactive Preservation, Proactive Analysis* dan *Preliminary Report* tidak dapat dilakukan pada proses investigasi *smartphone* karena pemeriksaan pada *smartphone* seluruhnya dilakukan di laboratorium. (4) Tidak ada tahapan penyitaan (*seize*) barang bukti digital yang telah ditemukan di TKP sehingga proses pemeriksaan barang bukti digital hanya dilakukan di TKP. (5) Tahapan pemindahan (*transportation*) barang bukti digital dilakukan setelah proses *collecting & acquicition*.

Berdasarkan temuan yang didapatkan dari hasil analisis model IDFIF terhadap proses investigasi *smartphone* maka disusun rekomendasi untuk perbaikan model tersebut. Beberapa rekomendasi tersebut adalah: (1) Tahapan *securing the scene* seharusnya diletakan pada awal proses olah TKP sehingga keadaan TKP selama proses investigasi dapat terjamin keamanannya. (2) Tahapan *documenting the scene* seharusnya diletakkan setelah tahapan *securing the scene* dilakukan sehingga keadaan awal TKP sebelum proses investigasi dapat terdokumentasikan. (3) Setelah tahapan *documenting the scene* seharusnya ada tahapan untuk pemilihan proses investigasi yang akan dilakukan selanjutnya sehingga apabila barang bukti digital yang telah ditemukan di TKP tidak bisa diperiksa ditempat, maka tahapan *Proactive Preservation*,

Proactive Analysis dan *Preliminary Report* bias dilewati. (4) Harus ditambahkan tahapan penyitaan (*seize*) barang bukti digital yang telah ditemukan di TKP karena seluruh barang bukti digital yang ditemukan di TKP harus disita untuk proses pemeriksaan lebih lanjut di laboratorium *digital forensic*. (5) Tahapan pemindahan (*transportation*) barang bukti digital terutama *smartphone* seharusnya dilakukan setelah tahapan penyitaan (*seize*).

5. Kesimpulan

IDFIF merupakan suatu model untuk proses investigasi barang bukti digital dan diklaim memiliki tahapan yang lengkap serta dapat mengakomodir seluruh tahapan pada proses investigasi *cybercrime*. Setelah dilakukan analisis terhadap proses investigasi *smartphone*, IDFIF memliki beberapa tahapan yang tidak sesuai dengan prosedur investigasi *smartphone* serta tidak adanya proses penyitaan barang bukti yang telah ditemukan di TKP. Dengan demikian, saat ini model IDFIF belum bias dijadikan sebagai standar untuk proses investigasi *smartphone*.

6. Saran

Model IDFIF ini perlu dikembangkan lagi sehingga memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital terutama untuk proses investigasi *smartphone*.

Referensi

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensics Model for Digital Forensic Investigation. *International Journal of Advance Computer Science and Applications(IJACSA)*, Vol. 2 No. 12, 175-178.

Agrawal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security(IJCSS)*, Vol. 5 No. 1, 118-131.

Alharbi, S., Jahnke, J. W., & Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. *International Journal of Security and Its Applications(IJCSIA)*, Vol. 5 No. 4, 59-72.

Ayers, R., Brother, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics*. Wasington D. C.: National Institute of Standards and Technology(NIST).

Farjamfar, A., Abdullah, M. T., Mahmod, R., & Udzir, N. I. (2014). A Review on Mobile Device's Digital Forensic Process Models. *Research Journal of Applied Sciences, Engineering and Technology*, Vol. 8 No. 3, 358-366

Goel, A., Tyagi, A., & Agrawal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security(IJCSS)*, Vol. 6 No. 5, 322-341.

Kalbande, D. & Jain, N. (2013). Comparative Digital Forensic Model. *International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET)*, Vol. 2 No. 8, 3414-3419.

Mohtasebi, S. H., & Dehghantanha, A. (2013). Towards a Unified Forensic Investigation Framework of Smartphone. *International Journal of Computer Theory and Engineering(IJCTE)*, Vol 5. No. 2, 351-355.

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). A Generic Framework for Network Forensics. *International Journal of Computer Applications(IJCA)*, Vol. 1 No. 11, 1-6.

Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation Framework(IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional Teknologi Informasi dan Komunikasi(Sentika)*.

Selamat, S. R., Yusof, R., Sahib, S., & . (2008). Mapping Process of Digital Forensics Investigation Framework. *International Journal of Computer Science and Network Security(IJCSNS)*, Vol. 8 No. 10, 163-169.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics. *International Journal of Computer Science & Information Technology(IJCSIT)*, Vol. 3 No. 3, 17-31.