Penerapan *Integrated Digital Forensic Investigation Framework v2* (IDFIF) pada Proses Investigasi *Smartphone*

Ruuhwan[#1], Imam Riadi[*2], Yudi Prayudi[#3]

[#]*Magster Teknik Informatika, Universitas Islam Indonesia*
Jl. Kaliurang KM 14,5 Yogyakarta 55584

[1]ruuhwan@yahoo.com

[3]prayudi@uii.ac.id

[*]*Teknologi Industri, Universitas Ahmad Dahlan*
Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164

[2]imam.riadi@is.uad.ac.id

***Abstrak*—Perkembangan teknologi yang semakin pesat, dapat menimbulkan permasalahan bagi pengguna teknologi itu sendiri, semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. *Smartphone* merupakan salah satu bentuk teknologi yang digunakan untuk melakukan penipuan melalui fasilitas *Short Message Service* (SMS). Pada saat *smartphone* yang digunakan untuk melakukan kejahatan maka *smartphone* tersebut dapat disita oleh aparat penegak hukum sebagai salah satu barang bukti. Cara pembuktian untuk mendapatkan bukti yang *valid* adalah dengan melakukan investigasi menggunakan pendekatan penanganan bukti digital yang dikenal dengan istilah *Framework. Integrated Digital Forensics Investigation Framework versi 2* (IDFIF v2) merupakan *framework* terbaru yang telah dikembangkan sehingga dapat digunakan untuk proses investigasi *smartphone*.**

***Kata kunci*— Barang Bukti, Framework, IDFIF v2, Smartphone**

I. PENDAHULUAN

Perkembangan teknologi yang semakin pesat, dapat menimbulkan permasalahan bagi pengguna teknologi itu sendiri, semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. Kejahatan juga menjadi sebagian dari hasil budaya itu sendiri, ini berarti bahwa semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya, hal tersebut dapat dilihat dari aplikasi yang ada pada *smartphone*[1].

Smartphone merupakan salah satu bentuk teknologi utama yang digunakan oleh orang untuk berkomunikasi dengan sesamanya dan tidak perlu menghabiskan waktu untuk bertemu secara fisik, salah satu teknologi komunikasi yang murah, mudah dan cepat yang digemari masyarakat sebagai layanan publik adalah *Short Message Service* (SMS).[1] Maraknya penipuan melalui SMS dapat menyebabkan terjadinya kejahatan berupa *spamming* SMS, dari berbagai laporan kejadian yang terjadi, baik yang diberitakan media maupun tidak, sudah banyak korban dari *spamming* SMS.

Pada saat *smartphone* yang digunakan seseorang sebagai alat untuk mengorganisasikan kejahatan maka *smartphone* tersebut dapat disita oleh aparat penegak hukum sebagai salah satu barang bukti. sehingga ketika ada barang bukti *smartphone* yang disita dari pelaku kejahatan, maka dapat diperiksa secara benar sesuai dengan prinsip-prinsip dasar *digital forensic*[2].

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[3]. Elemen yang paling penting dalam *digital forensic* adalah kredibilitas dari barang bukti digital tersebut[4]. Cara pembuktian untuk mendapatkan bukti yang *valid* adalah dengan melakukan investigasi menggunakan pendekatan prosedur pemeriksaan *digital forensic*[5]. Sejumlah tahapan pendekatan ini dalam penanganan bukti digital dikenal dengan istilah *Framework*[6].

Integrated Digital Forensics Investigation Framework versi 2 (IDFIF v2) merupakan *framework* terbaru yang telah dikembangkan sehingga diharapkan dapat menjadi standar metode penyelidikan oleh para penyidik karena IDFIF v2 ini memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital[7]. Namun IDFIF v2 ini belum pernah diterapkan pada proses investigasi *smarphone* sehingga IDFIF v2 ini menarik untuk diteliti lebih lanjut dalam proses investigasi *smartphone*.

II. KAJIAN PUSTAKA

A. Forensika Digital

Forensika digital merupakan ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisa terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan[8]. Ilmu forensika digital memiliki 4 prinsip dasar[9], yaitu:

- Sebuah lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang akan dibawa ke pengadilan.

- 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.
- 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.
- Setiap orang yang terlibat dalam proses investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan analisa untuk memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

B. Investigasi Forensika

Cabang ilmu forensika yang ada saat ini begitu luas sesuai perkembangan bidang ilmu pengetahuan. Ilmu forensika saat ini merupakan bidang yang sedang berkembang terutama terkait dengan teknologi informasi. Forensika itu sendiri adalah suatu proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum. Bidang forensika tersebut juga berkembang terhadap komputer. Forensika komputer adalah suatu proses mengidentifikasi, memelihara, menganalisis, dan menggunakan bukti digital menurut hukum yang berlaku. Ruang lingkup dari komputer forensik merupakan aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan, penyaringan dan dokumentasi bukti komputer dalam kejahatan komputer. Dari prosesproses tersebut dapat dilakukan analisis dan penyelidikan untuk menentukan potensi bukti-bukti yang legal[2].

Data-data yang dapat dipakai dan diambil dari sumber daya komputer diantaranya terdapat pada sistem komputer, jaringan komputer, jalur komunikasi, media penyimpanan, aplikasi komputer dan lain-lain. Data tersebut dapat diolah sesuai dengan prosedur yang berlaku sehingga dapat dijadikan sebagai bukti yang legal dan sah[2].

C. Barang Bukti

Barang bukti merupakan bagian yang sangat penting dalam sebuah kasus kejahatan. Dari barang bukti ini tim investigasi dan analis forensik dapat mengungkap kasus dengan kronologis yang lengkap[2]. Adapun barang bukti diklasifikasikan menjadi 2 bagian, yaitu:

1). Barang Bukti Elektronik

Merupakan barang bukti yang bersifat fisik dan dapat dikenali secara visual sehingga tim investigasi dan tim analisis dapat memahami dan mengenali masing barang bukti tersebut. Jenis barang bukti tersebut antara lain:

- Komputer, Laptop
- *Smartphone*
- *Flashdisk*
- *Harddisk*
- *Router*, *Switch*
- Kamera, dan lain-lain

2). Barang Bukti Digital

Barang bukti digital merupakan barang bukti yang di ekstrak ataupun direcovery dari barang bukti elektronik. Jenis barang bukti ini yang harus dicari oleh analis forensik yang kemudian akan diteliti keterkaitan barang bukti tersebut dengan kasus kejahatan. Contoh-contoh barang bukti digital antara lain :

- *Logical file*
- *Deleted file*
- *Lost file*
- *File slack*
- *Log file*
- *Encrypted file*
- *Steganography file*
- *Office file*
- *Audio file, video file, image file*
- *Email*
- *User ID dan password*
- *Short Message Service*(SMS)
- *Multimedia Message Service* (MMS)
- *Call logs*

D. Smartphone

Smartphone adalah telepon *internet-enabled* yang biasanya menyediakan fungsi *Personal Digital Assistant* (PDA) seperti fungsi kalender, buku agenda, buku alamat, kalkulator dan catatan[1]. *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 halnya dengan sistem operasi pada komputer *desktop*[10].

E. Perbedaan Computer Forensic Dan Smartphone Forensic

Saat ini perangkat *smartphone* memiliki fungsi yang sama dengan computer namun ada beberapa perbedaan dalam proses penanganan *digital forensic* diantara perangkat komputer dan *smartphone*[10]. Perbedaan tersebut dapat dilihat pada TABEL I.

TABEL I
PERBEDAAN COMPUTER FORENSIC DAN SMARPHONE FORENSIC

Aspect	***Computer Forensic***	***Smartphone Forensics***
Konektivitas	Terbatas	Tidak terbatas
Sumber bukti	- *Hard disk* - 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*

F. Potensi Bukti Digital Pada Smartphone

Informasi-informasi yang tersimpan pada *smartphone* tersebut berada pada beberapa media penyimpanan yang berbeda[2]. Adapun jenis media penyimpanan tersebut adalah:

1). SIM*(Subscriber Identity Module) Card*

Memiliki fungsi hanya untuk menyimpan data-data tertentu yang sifatnya terbatas yaitu sebagai berikut:

- *Phonebook*: Merupakan *contact* yang berisi nomor telepon yang berasosiasikan dengan nama tertentu yang dibuat oleh pemilik *smartphone* secara manual. Pada *smartphone, phonebook* tidak hanya menyimpan nama dan nomor saja namun juga dapat menyimpan beberapa informasi lainnya seperti alamat rumah, alamat perusahaan dan alamat *e-mail*.
- *Call log*: Berisi catatan panggilan yang pernah terjadi seperti panggilan masuk, panggilan keluar dan panggilan tak terjawab termasuk waktu dan durasi percakapan.
- *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.
- *Integrated Circuit Card Identifier* (ICCID): merupakan angka unik yang merupakan identitas dari *provider* untuk setiap SIM *card* guna keperluan yang bersifat administratif.
- *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 di dalam jaringannya.

2). Electronically Erasable And Programable Read-Only Memory (EEPROM)

Merupakan tempat penyimpanan data-data *default* (yang berasal dari pabrikan) seperti:

- System operasi dan aplikasi-aplikasi *default*.
- *International Mobile Equipment Identity*(IMEI): merupakan identitas (ID) yang unik bagi masing-masing *smartphone/smartphone* GSM yang terorganisasi secara internasional.
- *Electronic Serial number* (ESN): merupakan identitas *smartphone/smartphone* yang berbasis jaringan *Code Division Multiple Access* (CDMA).

3). Random Acces Memory (RAM)

Berfungsi untuk menyimpan data yang bersifat temporer yang berasal dari berbagai aplikasi. Data-data yang tersimpan bersifat *volatile*, yaitu hanya ada selama *smartphone/smartphone* tersebut hidup (*on*) dan akan hilang ketika *smartphone/smartphone* itu dimatikan (*off*).

4). Flash Read-Only Memory (ROM)

Sama dengan EEPROM sering kali dikenal dan disebut sebagai memori internal *smartphone/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.

5). 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.

6). Network Data

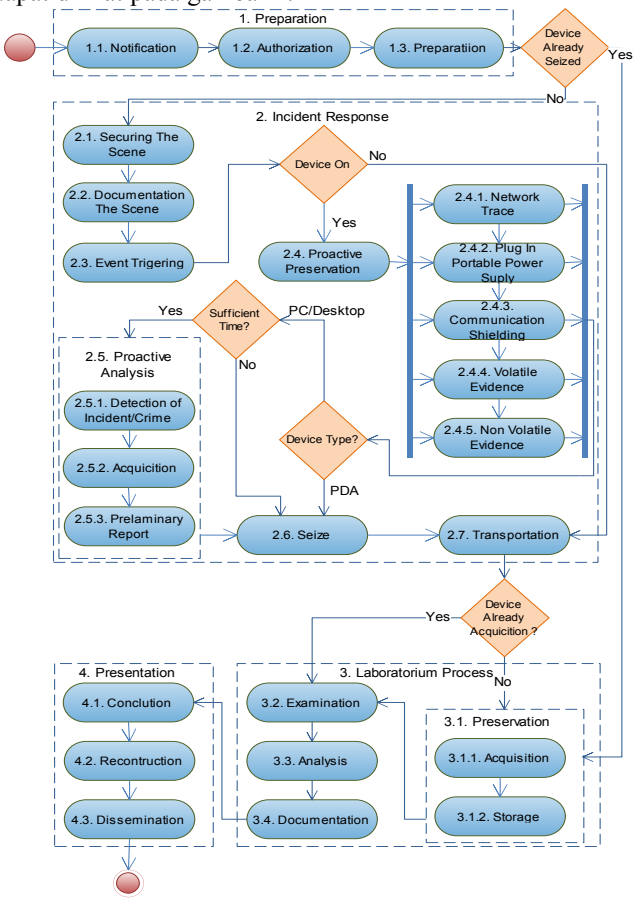
Merupakan penyimpanan data-data yang tersimpan di jaringan *provider/*penyedia layanan. Adapun cakupan *network data* tersebut adalah:

- *Call Data Record*: 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 *analys* dan *investigator* datang ke *provider* untuk meminta CDR dari nomor *subscriber* tertentu semakin baik.
- *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 *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.

- *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.
- *Cloud Storage*: merupakan media penyimpanan data yang dapat diakses dimana saja dan kapan saja melalui perantara jaringan yang terintegrasi dan tersinkronisasi melalui internet.

G. Integrated Digital Forensic Investigation Framework v2

Integrated Digital Forensics Investigation Framework versi 2 (IDFIF v2) merupakan *framework* terbaru yang telah dikembangkan sehingga diharapkan dapat menjadi standar metode penyelidikan para penyidik karena IDFIF v2 ini memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital[7]. Adapun tahapan-tahapan pada IDFIF v2 ini dapat dilihat pada gambar 1.



Gambar 1. Model IDFIF v2

1). Preparation

Merupakan persiapan yang harus dilakukan untuk melakukan proses investigasi dalam penanganan barang bukti digital dimulai dari olah tempat kejadian perkara hingga pembuatan laporan akhir.

- *Notification*: Pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum.
- *Authorization*: Tahapan untuk mendapatkan hak akses terhadap barang bukti dan status hukum proses penyelidikan.
- *Preparation*: Persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan.

2). Inciden Response

Merupakan kegiatan yang dilakukan di tempat kejadian perkara dengan tujuan untuk mengamankan barang bukti digital yang ada sehingga tidak terkontaminasi oleh hal-hal lain.

- *Securing The Scene*: Melakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.
- *Documentation The Scene*: Tujuan pokok dari tahapan ini adalah mengolah tempat kejadian perkara, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil gambar setiap detail TKP.
- *Event Trigering*: Melakukan analisa awal terhadap sebuah proses kejadian yang terjadi.
- *Proactive Preservation*: Memiliki 5 sub tahapan yaitu *network trace* melakukan pencarian jejak melalui jaringan yang digunakan oleh barang bukti digital. *Plug in portable power supply* merupakan proses pengamanan barang bukti digital dengan kondisi "*on*" sehingga daya yang terdapat pada barang bukti digital tersebut dapat terjaga selama diperjalanan hingga ke laboratorium forensik. *Communication shielding* merupakan tahapan penonaktifan komunikasi data pada barang bukti digital sehingga dapat mencegah perubahan data dari luar. *Volatile* dan *Non-Volatile evidence* merupakan proses pengamanan barang bukti digital. Di akhir tahap *proactive Preservation* terdapat *decision process*. Tahapan ini memang tidak disebut secara langsung menjadi tahapan, namun *output* dari *decision* ini juga penting untuk keberlangsungan proses penyelidikan. *Dari* tahapan ini diputuskan barang bukti digital tersebut harus langsung disita dan dilakukan pemeriksaan lebih lanjut di laboratorium forensik atau dilakukan pemeriksaan di tempat untuk mendapatkan laporan awal kejadian.
- *Proactive Analysis*: tahapan *live analysis* terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian. *Detection of Incident / Crime,* di tahap ini adalah tahap untuk memastikan bahwa telah terjadi pelanggaran hukum. *Acquicition* merupakan proses akuisisi data terhadap barang temuan sehingga meringankan beban kerja *digital forensic analys* di laboratorium. *Preliminary Report,* merupakan pembuatan laporan awal atas kegiatan penyelidikan proaktif yang telah dilakukan.

- *Seize*: Melakukan proses penyitaan terhadap barang bukti digital yang telah ditemukan untuk dianalisa lebih lanjut.
- *Transportation*: Merupakan proses pemindahan barang bukti digital dari tempat kejadian perkara menuju laboratorium digital foresik.

3). Laboratorium Process

Setelah penangan barang bukti digital di tempat kejadian pekara, maka pada tahapan ini adalah melakukan proses analisa data terhadap barang bukti yang telah didapatkan sebelumnya sehingga dapat ditemukan jenis kejahatan yang telah terjadi.

- *Preservation*: Menjaga integritas temuan dengan menggunakan *chain of custody* dan fungsi *hashing*.
- *Examinitation*: Pengolahan barang bukti untuk menemukan keterkaitanya dengan kejadian.
- *Analysis*: Merupakan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada.
- *Documentation*: melakukan dokumentasi terhadap seluruh kegiatan yang telah dilakukan dari awal proses penyelidikan hingga akhir proses analisa di laboratorium forensik.

4). Presentation

Merupakan tahapan akhir dalam proses investigasi digital. Pada tahap ini merupakan proses pembuatan laporan terkait hasil analisa yang dilakukan pada tahap sebelumnya dan memastikan bahwa setiap proses yang dilakukan tersebut telah sesuai dengan aturan hukum yang berlaku.

- *Conclution*: Menyimpulkan hasil dari investigasi yang telah dilakukan.
- *Recontruction*: Proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.
- *Dissemination*: Pencatatan proses penyelidikan dan catatan tersebut dapat disebarluaskan pada penyelidik lain yang melakukan penyedikan pada kasus serupa.

III. METODOLOGI PENELITIAN

Secara ringkas metode dan tahapan penelitian yang dilakukan dapat digambarkan seperti pada gambar 2:

Gambar 2. Metodologi Penelitian

Research problem merupakan langkah awal yang dilakukan untuk memperoleh dan menentukan topik penelitian yang akan diteliti lebih lanjut. Pada tahapan ini dimulai dengan melihat berbagai fenomena, kejadian dan informasi yang didapatkan dengan berbagai cara. *Literature review* diharapkan mampu 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 bagi setiap peneliti sehingga penelitian yang dilakukan dapat dijadikan acuan kembali dikemudian hari. *Case Study* merupakan proses penerapan IDFIF v2 terhadap proses investigasi *smartphone*. Conclution merupakan kesimpulan dari seluruh tahapan yang telah dilakukan dalam proses penelitian ini.

IV. SKENARIO KASUS

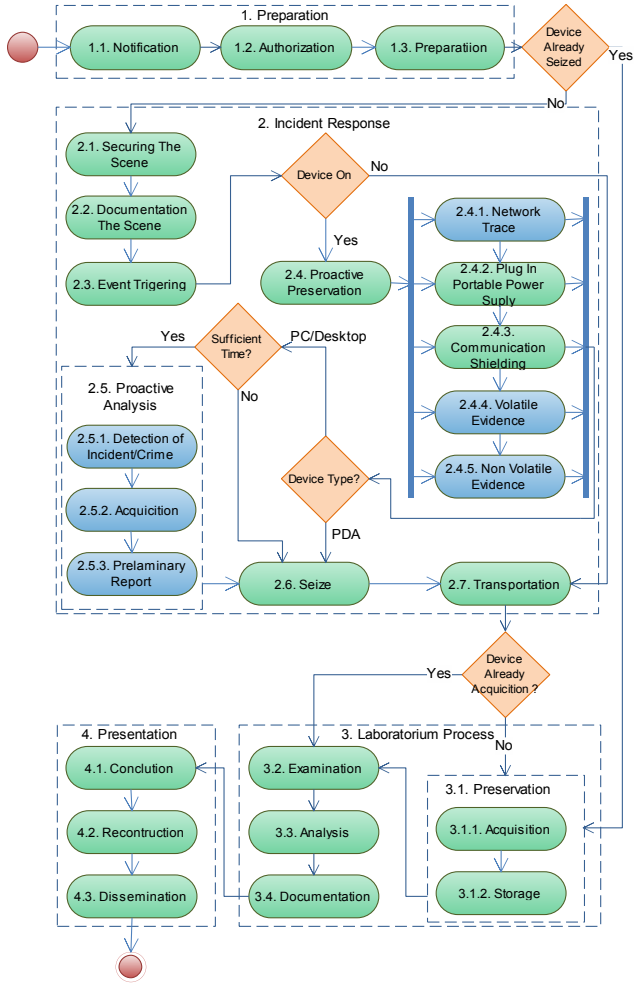
Skenario kasus dan simulasi di dalam penelitian ini disesuaikan dengan kasus penipuan melalui pesan singkat(SMS) yang mengadopsi dari kasus yang telah terjadi beberapa waktu yang lalu. Kasus tersebut adalah penipuan undian berhadiah. Perangkat *mobile* yang digunakan untuk mengirimkan SMS ke korban adalah Lenovo S860. Pelaku mengirimkan SMS ke korban dengan isi pesan bahwasanya 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. Setelah korban menghubungi pelaku, 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. Namun, setelah melakukan pengiriman sejumlah uang ke rekening yang telah di tentukan pelaku, korban merasa tertipu terhadap SMS yang diterimanya sehingga korban melaporkan kejadian ini kepada pihak yang berwajib.

V. HASIL DAN PEMBAHASAN

Dalam menangani kasus penipuan ini, investigator menerapkan model IDFIF v2 untuk menyelesaikan kasus ini. Secara umum, tahapan proses investigasi terhadap barang bukti digital baik itu komputer ataupun *smartphone* memiliki 4 (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*). Tahapan yang digunakan dalam investigasi *smartphone* ini dapat dilihat pada gambar 3.

Pre-process merupakan tahapan awal dalam proses investigasi barang bukti digital terutama pada investigasi *smartphone*. Pada tahap ini dilakukan berbagai persiapan dalam proses investigasi baik peralatan dan juga dokumen-dokumen yang diperlukan. Tahapan ini dibagi menjadi 3 sub tahapan yaitu:

- *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 di sini dapat menentukan langkah berikutnya dalam penyelidikan.



Gambar 3. Tahapan IDFIF v2 yang digunakan dalam investigasi *smartphone*

- *Authorization*: Penegak hukum melaksanakan kerjasama dan mengurus proses perizinan kepada operator seluler untuk mendapatkan hak akses dalam proses pelacakan terhadap pelaku penipuan. Setelah mendapatkan nomor *smartphone* dan nomor ICCID pelaku penipuan, investigator melakukan pelacakan untuk mendapatkan lokasi keberadaan pelaku penipuan tersebut.
- *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 III
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 analisa terhadap *smartphone* yang ditemukan di TKP.
Perangkat Komputer	Digunakan untuk melakukan proses pemindahan data digital dari *smartphone* ke media penyimpanan untuk dilakukan proses analisa

Proactive Process merupakan tahapan awal yang dilakukan dalam proses investigasi. 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. Adapun sub tahapannya adalah sebagai berikut:

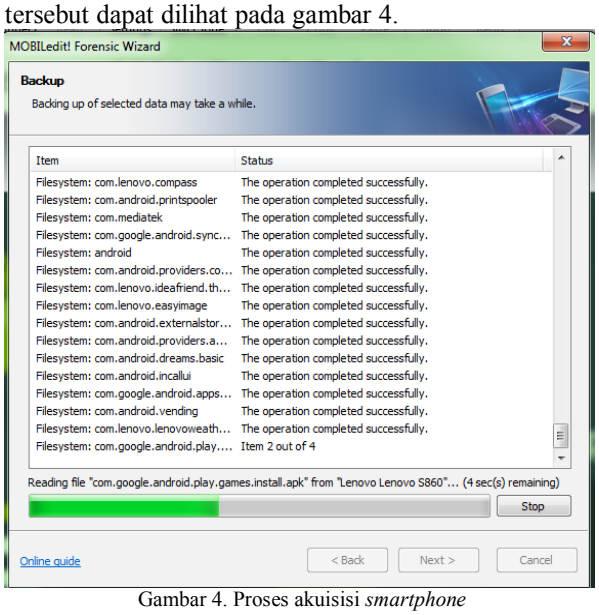
- *Securing The Scene*: Investigator melakukan suatu proses untuk menjaga agar TKP berada dalam keadaan sebagaimana pada saat dilihat dan diketemukan petugas yang melakukan tindakan pertama di TKP sehingga barang bukti yang diperlukan tidak hilang, rusak, tidak ada penambahan atau pengurangan dan tidak berbeda letaknya yang berakibat menyulitkan atau mengaburkan pengolahan TKP dan pemeriksaan secara teknis ilmiah.
- *Documentation The Scene*: Investigator melakukan dokumentasi TKP dengan cara memotret keadaan TKP dan semua barang bukti 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 di mana 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.
- *Event Trigering*: Setelah investigator mengamankan TKP, investigator melakukan proses analisa awal

terhadap suatu kejadian yang telah terjadi di tempat kejadian perkara serta melakukan pencarian pemicu kejadian di TKP sehingga investigator dapat menyimpulkan sementara jenis kejahatan yang telah dilakukan untuk proses analisa lebih lanjut di laboratorium *digital forensic*. Adapun barang bukti digital yang ditemukan adalah satu unit *smartphone* Lenovo S860 yang digunakan pelaku untuk melakukan aksi penipuannya

- *Proactive Preservation*: Investigator melakukan proses pengamanan barang bukti *smartphone* yang telah ditemukan di tempat kejadian perkara sehingga integritas data yang berada pada barang bukti *smartphone* tetap terjaga hingga proses analisa di laboratorium *digital forensic*.
- *Plug in portable power supply*: Investigator melakukan pengamanan barang bukti digital dalam hal ini *smarphone* dengan cara melakukan proses *charging* terhadap barang bukti *smartphone* menggunakan *portable power supply* karena kondisi daya baterai pada *smartpone* yang di temukan tidak selalu dalam keadaan penuh sehingga diperlukan proses *charging* menggunakan *portable power supply* untuk menjaga kondisi *smartphone* tersebut dalam kondisi "*on*" hingga ke laboratorium *digital forensic*. Ketika kondisi *smartphone* dalam kondisi terisolasi, kerja *smartphone* tersebut akan menjadi lebih berat dan akan menggunakan sumberdaya baterai yang maksimal untuk mencari jaringan komunikasi sehingga sumberdaya baterai akan cepat habis.
- *Communication shielding*: Investigator melakukan pengamanan barang bukti *smartphone* dengan cara melakukan isolasi terhadap komunikasi data menggunakan *faraday bag* sehingga tidak akan terjadi pertukaran data ataupun proses pengendalian jarak jauh melalui jaringan yang tersedia.
- *Seize*: Investigator melakukan proses penyitaan terhadap *smartphone* yang ditemukan di TKP
- *Transportation*: Investigator 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.

Reactive Process merupakan tahapan inti dari proses investigasi *smartphone*. Pada tahapan ini, *smartphone* yang telah didapatkan pada proses sebelumnya dilakukan analisa untuk mendapatkan bukti-bukti yang terkait dengan kejahatan yang terjadi. Tahapan ini dibagi menjadi beberapa tahapan yaitu:

- *Preservation*: Investigator melakukan proses pengamanan barang bukti *smartphone*. Kondisi *smartphone* ketika dalam proses akuisisi harus dalam keadaan terputus dari komunikasi data yang ada.
- Acquicition: Investigator melakukan pengambilan bukti digital dari perangkat *smarphone* yang ditemukan di TKP. Adapun proses aquisisi terhadap *smartphone* tersebut dapat dilihat pada gambar 4.



Gambar 4. Proses akuisisi *smartphone*

Hasil akuisisi smartphone terlihat secara detail informasi yang terdapat pada *smartphone* yaitu jenis *platform*, IMEI, *merk* dan model *smartphone*, data *phonebook*, data *panggilan*, data pesan, data aplikasi dan data *simcard*. Adapun tampilan awal ketika proses akuisisi selesai dapat dilihat pada gambar 5.

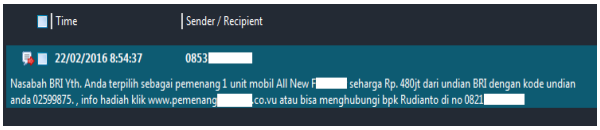
Gambar 5. tampilan awal hasil akuisisi *smartphone*

Proses akuisisi data pada *smartphone* ini menggunakan tool *mobiledit 7.5,* waktu yang diperlukan dalam proses akuisisi data pada *smartphone* ini tidak kurang dari 3 jam. Setelah proses akuisisi selesai, tahapan selanjutnya dalam *preservation* adalah *storage*.

- *Storage*: Investigator melakukan proses penyimpanan barang bukti *smartphone* ke tempat yang telah ditentukan. Bentuk dan isi bukti digital harus disimpan dalam tempat yang steril. Untuk benar-benar memastikan tidak ada perubahan-perubahan, hal ini sangat perlu diperhatikan karena sedikit perubahan saja dalam bukti digital, akan merubah juga hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak

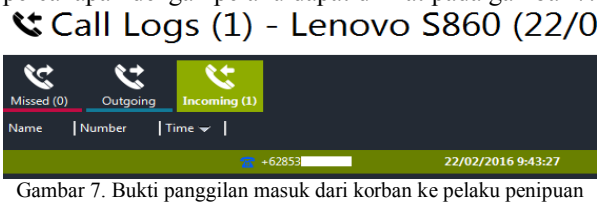
teliti akan sangat mudah sekali rusak, hilang, berubah, atau mengalami kecelakaan.

- *Examinitation*: Investigator 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 analis forensik, seperti penyidik atau pemeriksa forensik.
- *Analysis*: Setelah melakukan proses pemeriksaan terhadap *smartphone* tersebut, investigator melakukan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada baik antara pelaku dengan *smartphone* yang di dapat, *smartphone* yang didapat dengan korban dan pelaku dengan korban. 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 di penyimpanan internal *smartphone*. Pelaku memberitahukan ke calon korban bahwa telah memenangkan hadiah satu unit mobil. Adapun pesan yang dikirimkan pelaku dapat dilihat pada gambar 6.
-



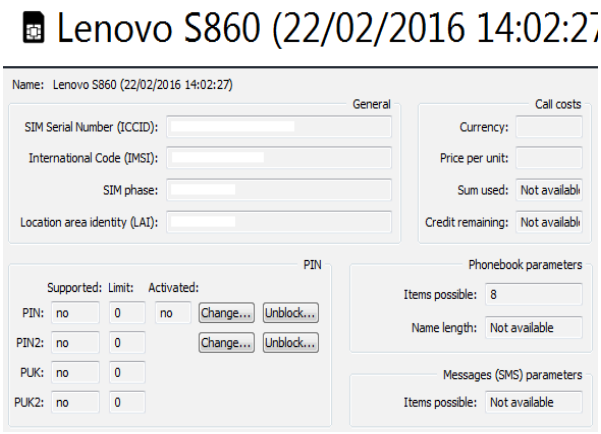
Gambar 6. Bukti SMS pelaku terhadap korban penipuan

Selanjutnya, karena korban merasa gembira atas hadiah yang didapatkan, maka korban menghubungi nomor yang telah ditentukan pelaku untuk melakukan konfirmasi. Adapun bukti korban telah melakukan percakapan dengan pelaku dapat dilihat pada gambar 7.



Gambar 7. Bukti panggilan masuk dari korban ke pelaku penipuan

Selanjutnya selain catatan panggilan keluar dan panggilan masuk serta SMS keluar dan SMS masuk, hal yang diketahui adalah informasi yang terdapat pada simcard yaitu ICCID(Integrated Circuit Card Identifier) dan IMSI(*International Mobile Subscriber Identity*). Kedua ID yang berupa kombinasi karakter dan angka tersebut ditanam kedalam *simcard* dan akan digunakan untuk autentifikasi jika pelanggan ingin menggunakan layanan komunikasi seluler. ICCID merupakan ICCID merupakan nomor registrasi manufaktur dari *simcard* yang terdiri dari 19 digit nomor dan dicetak di belakang *simcard*. IMSI sama seperti ICCID, IMSI melekat pada *simcard*. Namun, untuk alasan keamanan, IMSI tidak bisa dilihat dari perspektif pengguna. IMSI merupakan 15 digit nomer identifikasi pelanggan yang berlaku unik secara global. Tiga digit pertama merupakan kode negara (MCC**:** *Mobile Country Code*)**,** diikuti dengan 2 atau 3 digit kode operator (MNC: *Mobile Network Code*). Informasi yang terdapat pada simcard dapat dilihat pada gambar 8.



Gambar 8. Informasi ICCID dan IMSI

- *Documentation*: Setelah melakukan proses analisa terhadap *smartphone* yang telah ditemukan, tahapan selanjutnya adalah merangkai temuan pada tahap *analysis* untuk disampaikan pada pihak yang memiliki otoritas. Temuan disajikan dalam bentuk yang mudah di pahami dan di dukung dengan barang bukti yang cukup dan dapat diterima.

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 di tempat yang aman dan melakukan *review* pada investigasi yang telah dilaksanakan sebagai perbaikan pada penyelidikan berikutnya.

- *Conclusion*: Bukti dan informasi yang ditemukan oleh investigator sudah cukup untuk tim investigasi untuk menuntut tersangka SMS penipuan undian berhadiah dan dapat memasukkan pelaku ke dalam tahanan.
- *Recontruction*: Selanjutnya investigator harus melakukan rekontruksi ulang berdasarkan hasil temuan dari analisa yang telah dilakukan sehingga proses kegiatan pelaku dapat diketahui lebih jelas dalam melakukan proses penipuan undian berhadiah.
- *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*.

VI. KESIMPULAN

Berdasarkan hasil penerapan IDFIF v2 yang terlah dilakukan pada proses investigasi *smartphone*, maka IDFIF v2 ini diharapkan dapat menjadi standar dalam proses investigasi barang bukti digital di Indonesia sehingga nantinya tidak akan ada perbedaan hasil investigasi dalam proses penanganan barang bukti yang telah didapatkan karena *framework* tersebut memiliki fleksibilitas dalam menangani barang bukti digital yang ditemukan TKP.

REFERENSI

[1] 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

[2] Al-Azhar, M. N. (2012). Digital Forensic Panduan Praktis Investigasi Komputer. Jakarta: Penerbit Salemba Infotek.

[3] 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

[4] 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

[5] 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

[6] 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.

[7] Ruuhwan. (2016). Evaluasi Tahapan *Integrated Digital Forensics Investigation Framework* (IDFIF) untuk Investigasi *Smartphone* Menggunakan *Soft System Methodology*. Universitas Islam Indonesia

[8] 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.

[9] 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

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