BAB IV
ANALISIS DAN PEMBAHASAN

Bab ini, akan membahas tentang hasil analisis yang dilakukan terhadap apa yang diperoleh, ditinjau secara kualitatif. Data yang didapat dari hasil studi pustaka diolah sesuai dengan standar penanganan bukti digital untuk *smartphone.* Berdasarkan hasil evaluasi tersebut maka akan dapat dilihat bagaimana *framework* penanganan *smartphone* berdasarkan IDFIF.

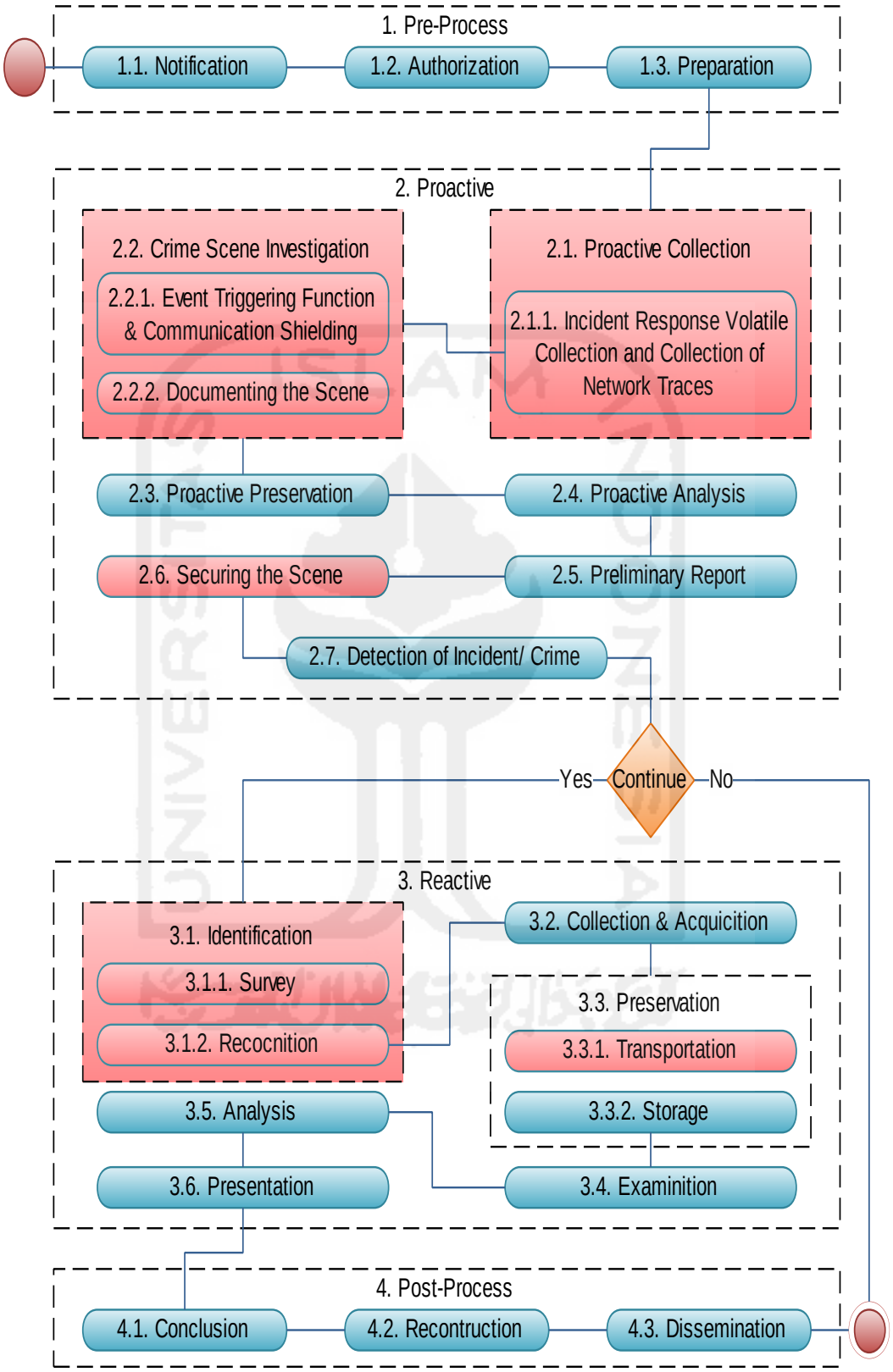
4.1. Tahap 1 SSM: *Situation Considered Problematic*

Secara umum situasional permasalahan berdasarkan hasil temuan dalam proses penerapan *Integrated Digital Forensics Investigation Framework* (IDFIF) antara lain:

1. Langkah 2.6 *securing the scene* seharusnya ditempatkan pada posisi 2.1 pada *proactive collection.*
2. Tidak ada pengkondisian apabila barang bukti yang ditemukan itu dalam mode "*on*" atau "*off*" terutama dalam penanganan *smartphone.*
3. Tidak ada penentuan penanganan barang bukti digital apakah proses penanganannya akan dilaksanakan di tempat atau di lab computer forensic.

4.2. Tahap 2 SSM: *Problem Situation Expressed*

Berdasarkan situasi masalah yang berhasil ditemukan pada model *Integrated Digital Forensics Investigation Framework* (IDFIF) dalam penanganan *smartphone* digambarkan pada gambar 4.1.



Gambar 4.1. *Rich Picture* Model IDFIF

Tahapan *Proactive process* dan *reactive process* model IDFIF pada gambar 4.1 memiliki tahapan yang tidak sesuai dengan kondisi di lapangan serta hanya menjelaskan tahapan untuk penanganan komputer. Evaluasi perbaikan terhadap model IDFIF tersebut sangat diperlukan sehingga model IDFIF itu dapat diterapkan secara global pada proses penanganan barang bukti digital.

4.3. Tahap 3 SSM: *Root Definition Of Relevant System*

Tahapan ini adalah tahapan yang digunakan untuk mendefinisikan setiap tahapan dari IDFIF berdasarkan *root definition* yang nantinya akan disesuaikan dengan DFIF untuk *smartphone investigation* dan *real word*.

1.3.1. Identifikasi Tahapan IDFIF

IDFIF memiliki 4 tahapan utama dan setiap tahapan memiliki sub tahapan. Adapun definisi setiap tahapan dari IDFIF adalah sebagai berikut:

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. *Proactive Proceses* terdapat tujuh tahapan pendukung yakni :
   a. *Proactive Collection* merupakan tindakan cepat mengumpulkan barang bukti di tempat kejadian perkara. Tahapan ini termasuk *Incident response volatile collection and Collection of Network Traces. Incident response volatile collection* sendiri merupakan mekanisme penyelmatan dan pengumpulan barang bukti, terutama yang bersifat *volatile.* Sedangkan *Collection of Network Traces* adalah mekanisme pengumpulan barang bukti dan melacak rute sampai ke sumber barang bukti yang berada dalam jaringan. Tahapan ini juga memperhitungan

keberlangsungan system dalam pelakasanaan 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 tempat kejadian perkara, 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 meyimpan 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* di tahap ini dilakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.

g. *Detection of Incident / Crime*, di tahap ini adalah tahap untuk memastikan bahwa telah terjadi pelanggaran hukum berdasarkan *premilinary report* yang telah dibuat. Di akhir 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. *Dari* tahapan ini diputuskan penyelidikan cukup kuat untuk dilanjutkan atau tidak.

3. *Reactive Process* merupakan tahapan penyelidikan secara tradisional meliputi 6 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*. Di tahap ini seluruh temuan dan keterkaitanya disusun dalam bentuk yang mudah di pahami.

4. *Post-Process* merupakan tahap penutup investigasi yang terdiri dari:

a. *Conclusion*. Menyimpulkan hasil dari investigasi yagng telah dilakukan.

b. *Recontruction*. Proses analisa 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.

1.3.2. Identifikasi DFIF Untuk *Smartphone Investigation*

Proses ini digunakan untuk mengidentifikasi tahapan-tahapan dalam DFIF untuk *smartphone investigation* yang telah dikembangkan sebelumnya. Penelitian ini menggunakan model IDFIF tahun 2014 dan model DFIF untuk *smartphone investigation* dari tahun 2007-2014 dan. Berdasarkan hasil dari proses *review*, DFIF yang digunakan untuk *smartphone investigation* terdiri dari 7 *framework*. DFIF yang digunakan sebagai bahan kajian dalam penelitian ini dapat dilihat pada tabel 4.1.

Tabel 4.1. IDFIF dan DFIF untuk *smartphone investigation*

No	Nama *Framework*	Peneliti/ Rujukan	∑ Tahapan
1	*Windows Mobile Device Forensic Model* (WMDFM)	Ramabhadran, A. (2007). Forensics Investigation Process Model for Windows Mobile Devices. 1-16	12
2	*Symbian Smartphones Forensic Process Model* (SSFPM)	Mohtasebi, S. H., & Dehghantanha, A. (2013). Towards a Unified Forensic Investigation Framework of Smartphone. *International Journal of Computer Theory and Engineering*, 351-355	6
3	ACPO *Smartphone Forensic Investigation*	ACPO. (2011). *The ACPO Good Practice Guide for Computer-Based Electronic Evidence.*	10
4	*Smartphone Forensic Investigation Process Model* (SFIPM)	Goel, A., Tyagi, A., & Agrawal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security(IJCSS)*, 322-341	13
5	ISO/IEC 27041 *Smartphone Forensic Investigation*	ISO/IEC 27041. Assurance for digital evidence investigation methods	12
6	NIST *Smartphone Forensic Investigation*	Ayers, R., Brothers , S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics.* Wasington D. C.: National Institute of Standards and Technology(NIST)	9
7	*Harmonised Digital Forensic Investigation Process* (HDFIP)	Mumba, E. R., & Venter, H. S. (2014). Mobile Forensics Using the Harmonised Digital Forensic Investigation Process. *IEEE*	18
8	*Integrated Digital Forensics Investigation Framework (IDFIF)*	Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation Framework(IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional Teknologi Informasi dan Komunikasi(Sentika)*	30

Seluruh tahapan yang terdapat pada IDFIF dan DFIF untuk *smartphone investigation* sebanyak 110 tahapan dan dapat dilihat pada lampiran 1. Selanjutnya adalah pemberian *ID* pada setiap tahapan IDFIF dan DFIF untuk *smartphone investigation* berdasarkan urutan tertinggi dari tahapan tersebut. Namun, dari

seluruh tahapan tersebut terdapat beberapa tahapan yang sama sehingga untuk tahapan yang sama akan diberi *ID* yang sama untuk memudahkan proses evaluasi terhada IDFIF. Adapun tahapan tersebut dapat dilihat pada lampiran 2.

1.3.3. *Terminology Process* DFIF Untuk *Smartphone Investigation*

Proses identifikasi DFIF yang telah ada sebelumnya menghasilkan 8 DFIF. DFIF yang digunakan adalah DFIF pada Tabel 4.1. DFIF tersebut memiliki jumlah tahapan yang berbeda-beda dengan penggunaan istilah tahapan yang berbeda pula. Tiap tahapan DFIF di terminologikan istilah dan pengertiannya sesuai tujuan DFIF dan dapat dilihat pada lampiran 3.

1.3.4. Tahapan *Smartphone Investigation* Di Dunia Nyata

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. Adapun kemungkinan keadaan *smartphone* saat ditemukan di TKP dapat dilihat pada tabel 4.2.

Tabel 4.2. Kondisi *smartphone* saat ditemukan di TKP

No	Kondisi *Smartphone* di TKP	Solusi
1	Dalam keadaan *"off"*	Lakukan proses penyitaan
2	Dalam keadaan *"on"*	Lakukan proses pengamanan sumber daya baterai pada *smartphone* dan pemutusan komunikasi data
3	Dalam keadaan "normal"	Lakukan proses *aquicision* di ruangan yang kedap frekuensi(laboratorium)
4	Dalam keadaan "rusak/tidak bisa di *acquicition*"	Lakukan proses *documentation* terkait seluruh hasil temuan yang telah dilakukan berdasarkan hasil temuan investigasi

ACPO (2007) dan NIST (2014) telah memperhitungkan segala kemungkinan-kemungkinan yang terjadi dilapangan dalam penanganan barang bukti digital terutama pada penanganan perangkat *smartphone*. Adapun tahapan-tahapan yang harus dilakukan dalam proses *smartphone innvestigation* berdasarkan kemungkinan keadaan *smartphone* saat ditemukan di TKP adalah sebagai berikut:

1. *Incident Response*

Incident Response merupakan proses penanganan barang bukti digital di tempat kejadian perkara(TKP) terutama dalam penanganan perangkat *smartphone*. *Incident response* setidaknya memiliki 7 proses seperti pada gambar 4.2.

Gambar 4.2. *Incident response process*

a. *Securing The Scene*

Secara umum dapat dikatakan bahwa setiap tempat dimana diduga telah terjadi pidana harus dianggap sebagai tempat kejadian perkara (TKP), karena ditempat ini merupakan sumber keterangan yang penting dan bukti-bukti yang dapat menunjukkan atau membuktikan adanya hubungan antara korban, pelaku, barang bukti serta TKP. *Securing the scene* merupakan 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.

Prosedur yang salah atau penanganan yang tidak tepat dari perangkat *smartphone* dapat menyebabkan hilangnya bukti digital. Kewaspadaan untuk karakteristik perangkat *smarphone* dan perangkat tambahan (seperti adapter, media, kabel, dan listrik) harus diperlukan. Banyak perangkat *smartphone* memiliki kode *master reset* yang dapat menghapus isi dari perangkat ke kondisi asli pabrik. *Master reset* juga dapat dilakukan dari jarak jauh sehingga memerlukan tindakan pencegahan yang tepat seperti isolasi jaringan untuk memastikan bahwa bukti tidak diubah atau dihancurkan.

Perangkat *smartphone* dan media terkait juga dapat ditemukan dalam keadaan rusak yang disebabkan oleh tindakan disengaja atau disengaja. Peralatan yang rusak harus dibawa ke laboratorium untuk pemeriksaan lebih

dekat. Perbaikan komponen yang rusak pada perangkat *smartphone* harus dilakukan sehingga dapat memulihkan perangkat tersebut untuk pemeriksaan dan analisis yang dimungkinkan.

b. *Documenting The Scene*

Bukti yang ada harus diidentifikasi secara akurat sehingga dapat dipertanggungjawabkan di depan hakim. Bukti non-elektronik seperti faktur, manual, dan bahan kemasan dapat memberikan informasi yang berguna tentang kemampuan perangkat, jaringan yang digunakan, informasi rekening, dan membuka kode PIN tersebut. Memotret TKP bersama dengan mendokumentasikan laporan tentang keadaan masing-masing perangkat digital.

Semua perangkat digital, termasuk perangkat *smartphone*, yang dapat menyimpan data, harus difoto bersama dengan semua *peripheral* kabel, konektor daya, *removable* media, dan koneksi. Hindari menyentuh atau mencemari perangkat *smartphone* saat memotret dan lingkungan di mana ditemukan. Jika layar perangkat dalam keadaan dapat dilihat, isi layar harus difoto dan jika perlu, direkam secara manual, menangkap waktu, status layanan, tingkat baterai, dan ikon yang ditampilkan lainnya.

c. *Event Trigering*

Event Trigering merupakan proses pencarian pemicu kejadian di tempat kejadian perkara sehingga penyidik di lapangan bias menyimpulkan sementara jenis kejahatan yang telah dilakukan untuk dilakukannyn proses analisa lebih lanjut di laboratorium *digital forensic*.

d. *Plug In Portable Power Suply*

Perangkat *smartphone* yang ditemukan di TKP tidak selalu dalam daya baterai yang penuh terkadang juga ditemukan dalam keadaan daya baterai yang sangat minim sehingga diperlukan proses *charging* menggunakan *portable power supply.* Proses tersebut perlu dilakukan untuk menjaga kondisi perangkat *smartphone* dalam keadaan *on* hingga sampai ke laboratorium untuk proses pemeriksaan lebih lanjut. Perangkat *smartphone* dengan keadaan terisolasi akan memperpendek masa pakai baterai karena

peningkatan konsumsi daya ketika berusaha untuk menghubungkan ke jaringan sehingga meningkatkan kekuatan sinyal yang maksimal.

e. *Communication Shielding*

Banyak *smartphone* menawarkan pengguna dengan kemampuan untuk melakukan penguncian jarak jauh atau *remote wipe* hanya dengan mengirimkan perintah (seperti pesan teks) ke perangkat *smartphone*. Alasan tambahan untuk menonaktifkan konektivitas jaringan termasuk data yang masuk (seperti panggilan masuk dan keluar atau pesan teks) yang dapat mengubah keadaan saat ini data yang tersimpan pada perangkat *smartphone*.

Oleh karena itu, investigator perlu menyadari dan mengambil tindakan pencegahan ketika mengamankan perangkat *smartphone* untuk mengurangi kemungkinan modifikasi data. Mengisolasi perangkat *smartphone* dari perangkat lain yang dapat digunakan untuk sinkronisasi data ini penting untuk menjaga data baru mengkontaminasi data yang ada. Perangkat *smartphone* harus disita bersama dengan perangkat keras yang terkait. Juga, menyita komputer yang terhubung ke perangkat *smartphone* untuk memperoleh data yang disinkronkan dari *hard disk* yang mungkin tidak diperoleh dari perangkat.

Mengisolasi perangkat *smartphone* dari semua jaringan radio (seperti *WiFi*, *Bluetooth*, komunikasi data) sangat penting untuk menjaga lalu lintas data, seperti pesan SMS dan lain sebagainya. Metode dasar untuk mengisolasi perangkat *smartphone* dari radio komunikasi dan mencegah masalah ini adalah menempatkan perangkat dalam modus pesawat, matikan perangkat, atau yang terakhir menempatkan perangkat dalam *faraday bag*. Setiap metode memiliki kelemahan tertentu, yaitu:

1) Mengaktifkan "*Airplane Mode*" memerlukan interaksi dengan perangkat *smartphone* dengan menggunakan keypad, yang menimbulkan beberapa risiko.
2) Mematikan perangkat *smartphone* dapat mengaktifkan kode otentikasi (misalnya, PIN UICC dan / atau handset kode keamanan), yang kemudian diperlukan untuk mendapatkan akses ke perangkat

smartphone sehingga proses akuisisi menjadi rumit dan menunda pemeriksaan.

3) Menempatkan perangkat *smartphone* kedalam *faraday bag* merupakan metode terbaik dalam proses pengamanan perangkat *smartphone* dari semua jaringan radio karena tidak memerlukan interaksi atau mengaktifkan kode otentikasi perangkat *smartphone* tersebut.

f. *Seize*

Seize merupakan proses penyitaan terhadap barang bukti digital terutama pada perangkat *smartphone*. Setelah perangkat *smartphone* siap untuk disita, investigator harus menyimpan perangkat tersebut kedalam tempat yang sesuai serta diberi label. Perangkat *smartphone* memiliki sifat *volatile* sehingga proses pemeriksaannya harus dilakukan di laboratorium *forensic computer*. Tempat penyimpanan barang bukti digital pun harus di tempat yang sejuk, kering sesuai standar untuk penyimpanan barang elektronik.

g. *Transportation*

Transportation merupakan proses pemindahan barang bukti digital terutama pada perangkat *smartphone* dari TKP menjuju ke laboratorium untuk proses pemeriksaan lebih lanjut. Dalam proses tersebut, barang bukti digital harus disimpan dalam keadaan yang sangat aman sehingga ketika sampai di laboratorium, barang bukti digital tersebut tetap dalam kondisi yang baik.

2. *Laboratorium Process*

Labolatorium process merupakan proses pemeriksaan barang bukti digital terutama perangkat *smartphone* di labolatorium. *Laboraotium process* tersebut memiliki 5 tahapan seperti pada gambar 4.3.

Gambar 4.3. *Laboratorium Process*

a. *Acquicition*

Acquicition merupakan suatu proses untuk memperoleh data atau informasi dari perangankat *smartphone* atau media yang terkait (seperti *simcard* dan *memory card*). Melakukan proses *acquicition* di TKP dapat meminimalisir hilangnya informasi karena menipisnya daya baterai dan kerusakan perangkat *smartphone* pada proses *transportation* namun harus memiliki kontrol kerja dan keahlian yang sangat baik serta akan memiliki resiko perubahan data yang sangat tinggi. Oleh karena itu, proses *acquicition* terhadap perangkat *smartphone* harus dilakukan di laboratorium *digital forensics*.

Proses pemeriksaan dimulai dengan melakukan identifikasi terhadap perangkat *smartphone*, jenis *smartphone*, sistem operasi, dan karakteristik lain sehingga dapat menentukan langkah-langkah yang diambil dalam proses *acquicition* ini. Setelah proses akuisisi selesai, investigator harus mengkonfirmasi bahwa isi dari perangkat itu telah di ambil dengan benar. Namun, apabila perangkat *smartphone* yang ditemukan di TKP tidak dapat diakuisisi, maka hal yang harus dilakukan investigator adalah melakukan pembuatan laporan terkait hasil penyidikan yang telah dilakukan terkait temuan-temuan yang ada.

b. *Storage*

Storage merupakan proses penyimpanan atau penggandaan hasil akuisisi dari barang bukti digital. Proses ini sangat diperlukan untuk menjaga keamanan data yang telah di dapat dengan cara melakukan proses pemeriksaan terhadap hasil duplikasi data yang telah di akuisisi dan menyimpan data yang aslinya.

c. *Examination*

Proses pemeriksaan mengungkapkan bukti digital termasuk yang mungkin tersembunyi atau dihilangkan. Hasilnya diperoleh melalui penerapan metode ilmiah dan harus menjelaskan isi dan keadaan data sepenuhnya. Proses pemeriksaan barang bukti digital harus dilakukan oleh seorang ahli forensic sedangkan untuk proses analisis dapat dilakukan

dengan peran selain analis forensik, seperti penyidik atau pemeriksa forensik.

d. *Analisys*

Analisys merupakan proses kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada baik Antara pelaku dengan barang bukti yang di dapat, barang bukti yang didapat dengan korban dan pelaku dengan korban.

e. ***Documentation***

Pelaporan merupakan proses mempersiapkan ringkasan rinci dari semua langkah yang diambil dan kesimpulan yang dicapai dalam penyelidikan kasus. Pelaporan tergantung pada mempertahankan semua tindakan dan observasi, menjelaskan hasil tes dan ujian, dan menjelaskan kesimpulan yang ditarik dari bukti. Sebuah laporan yang baik bergantung pada dokumentasi yang baik, catatan, foto, dan konten yang dihasilkan.

Banyak alat forensik dengan fasilitas pelaporan *built-in* yang biasanya mengikuti *template* yang telah ditetapkan dan memungkinkan dapat diubah sesuai dengan kebutuhan. Perubahan yang disesuaikan dengan kebutuhan dapat dilakukan termasuk memungkinkan untuk merubah logo organisasi dan laporan header dan pilihan gaya dan struktur untuk memberikan tampilan yang lebih profesional disesuaikan dengan kebutuhan organisasi.

4.4. Tahap 4 SSM: *Conceptual Model Of System Described And Root Definition*

Carrier and Spafford (2003) menyatakan bahwa untuk menangani barang bukti digital diperlukan langkah yang memiliki fleksibilitas dalam menangani berbagai jenis barang bukti digital dikarenakan bahwa setiap adegan kejahatan itu selalu berbeda-beda dan menggunakan alat yang berbeda juga. Selanjutnya, menurut ACPO(2003) para investigator harus bekerja berdasarkan prinsip-prinsip penanganan yang ada. Berdasarkan *rich picture* pada gambar 4.1., bahwasanya model IDFIF yang telah diterapkan tersebut memiliki beberapa kekurangan diantaranya:

1. Model IDFIF mencoba untuk mengakomodir semua aspek kegiatan digital forensic dalam satu model namun menjadi terlalu berat dan rumit.
2. Model IDFIF tidak memberikan alternative penanganan barang bukti digital yang telah didapatkan.

Dari kekurangan diatas, maka model IDFIF ini akan evaluasi sehingga dapat mengakomodir seluruh penanganan barang bukti digital yang ada terutama pada penanganan *smartphone*. Prinsip-prinsip utama yang harus diikuti oleh praktisi forensik digital dalam penanganan barang bukti digital terutama *smarphone* adalah sebagai berikut:

1. Kegiatan praktisi forensik digital tidak harus mengubah data asli. Jika persyaratan pekerjaan berarti bahwa hal ini tidak mungkin maka efek dari tindakan praktisi pada data asli harus diidentifikasi secara jelas dan proses yang menyebabkan perubahan dibenarkan
2. Sebuah catatan lengkap dari semua kegiatan yang berhubungan dengan akuisisi dan penanganan data asli dan salinan dari data asli harus dijaga. Ini termasuk kepatuhan dengan aturan yang tepat dari bukti-bukti, seperti memelihara rantai rekor tahanan, dan proses verifikasi seperti hashing
3. Praktisi forensik digital tidak harus melakukan kegiatan yang berada di luar kemampuan atau pengetahuan mereka
4. Praktisi forensik digital harus mempertimbangkan semua aspek keselamatan pribadi dan peralatan sementara melakukan pekerjaan mereka
5. Setiap saat hak hukum orang dipengaruhi oleh tindakan Anda harus dipertimbangkan
6. Praktisi harus menyadari semua kebijakan dan prosedur organisasi yang berkaitan dengan kegiatan mereka
7. Komunikasi harus dijaga sesuai dengan klien, praktisi hukum, pengawas dan anggota tim lainnya.

1.4.1. IDFIF v2 *Contruction*

Berdasarkan pemberian *ID* pada setiap tahapan IDFIF dan DFIF untuk *smartphone investigation* maka dihasilkan 74 terminologi dan untuk memetakannya dirangkum dalam bentuk tabel seperti pada lampiran 4. Tahapan-tahapan tersebut diberi urutan tahapan dan yang tertinggi diawali dari 1 dan seterusnya, sedangkan sub bagian di beri urutan.urutan sub bagian contoh (1.1).

1.4.2. Normalisasi DFIF Untuk *Smarphone Investigation*

Hasil pembahasan dari 74 terminologi IDFIF dan DFIF untuk *smarphone investigation*, maka untuk keefektifan IDFIF v2 perlu dilakukan proses eliminasi terhadap tahapan-tahapan yang terdapat pada lampiran 4. Namun sebelum melakukan proses eliminasi yang pertama harus dilakukan adalah menghilangkan tahapan yang sesuai dengan tahapan *Pre-Process* (*Notification, Authorization, Preparation*) dan tahapan *Post-Proces* (*Conclution, Recontruction, Dissemination*) pada IDFIF karena tahapan yang akan dievaluasi hanyalah tahapan yang terdapat pada *Proactive Process* dan *Reactive Process* pada IDFIF sehingga menjadi lebih dinamis. Adapun proses eleminasi dan normalisasi terhadap IDFIF dan DFIF untuk *smarphone investigation* adalah sebagai berikut:

1. Proses eliminasi tahapan yang sesuai dengan tahapan *Pre-Process* dan *Post-Proces* pada IDFIF harus dilakukan sehingga tahapan yang tersisa dari 74 tahapan tersebut hanya yang sesuai dengan tahapan *Proactive* dan *Reactive Process*. Adapun tahapan-tahapan yang dieleminasi dapat dilihat pada lampiran 5. Kolom yang berwarna menunjukkan tahapan yang sesuai dengan tahapan *Pre-Process* (*Notification, Authorization, Preparation*) dan tahapan *Post-Proces* (*Conclution, Recontruction, Dissemination*) pada IDFIF yang harus dihilangkan sehingga setelah tahapan-tahapan yang ada sesuai dengan *Proactive dan Reactive Process.* Adapun tahapan-tahapan yang sesuai *Proactive dan Reactive Process* dapat dilihat pada lampiran 6.
2. Selanjutnya melakukan identifikasi terhadap seluruh baris yang memiliki tahapan yang sesuai dengan tahapan *Proactive Process* pada model IDFIF. Tahapan-tahapan yang sesuai dengan tahapan yang terdapat pada *Proactive Process* model IDFIF dapat dilihat pada lampiran 7. Kolom yang berwarna

menunjukkan tahapan yang teridentifikasi sebagai tahapan yang sesuai dengan tahapan *Proactive Process* pada model IDFIF.

3. Mulai dari baris pertama yang telah teridentifikasi, identifikasi juga dekripsi terminologinya, apabila terdapat baris lain yang memiliki deskripsi yang sama, hapus/gabung baris tersebut, sisipkan tahapan yang dihapus/digabung pada baris yang bertahan.
    a. Tahapan yang memiliki terminologi yang sama dengan *documenting the scene* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 8. *Documenting the scene* memiliki terminologi yang sama dengan *documentation, report writing, Incident scene documentation, evaluation the scene* dan *crime scene investigation*. *Documenting the scene* merupakan tahapan untuk melakukan dokumentasi terhadap tempat kejadian dengan mengambil gambar setiap detail TKP. Atas pertimbangan tersebut, maka istilah yang diambil adalah *documenting the scene.*
    b. Selanjutnya tahapan yang memiliki terminologi yang sama dengan *event trigerting* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 9. *Event trigerting* memiliki terminologi yang sama dengan *identification, potential digital evidence identification, triage processing, investigation processes, crime scene investigation* dan *event triggering function*. *Event trigerting* merupakan tahapan untuk mengolah tempat kejadian perkara serta mencari sumber pemicu kejadian di TKP. Atas pertimbangan tersebut, maka istilah yang diambil adalah *event trigerting.*
    c. Selanjutnya tahapan yang memiliki terminologi yang sama dengan *proactive preservation* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 10. *Proactive preservation* memiliki terminologi yang sama dengan *communication shielding, volatile evidence, non-volatile evidence, evidence collection, volatile memory, non-volatile memory, isolation, potential digital evidence collection,*

potential digital evidence preservation, proactive collection, incident response volatile collcetion dan *incident response collection network trace*. *Proactive Preservation* merupakan tahapan untuk mengumpulkan bukti secara *proactive* dengan tujuan bukti yang mudah hilang dapat diamankan dan jejak jaringan yang mudah hilang juga dapat direkam sebagai bukti kejahatan. Atas pertimbangan tersebut yang digabung hanya *network trace*, *communication shielding, volatile evidence* dan *non-volatile evidence*.

d. Selanjutnya tahapan yang memiliki terminologi yang sama dengan *proactive analysis* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 11. *Proactive analysis* memiliki terminologi yang sama dengan *acquicition, remote evidence acquicition, internal evidence acquicition, preminilary report* dan *detection of incident/crime*. *Proactive analysis* merupakan tahapan *live acquicition and analysis* terhadap barang temuan dan membangun hipotesa/laporan awal dari sebuah kejadian. Atas pertimbangan tersebut yang digabung hanya *detection of incident crime, acquicition* dan *preminary report*.

4. Identifikasi seluruh baris yang memiliki urutan tahapan yang sesuai dengan tahapan *Reactive Process* pada model IDFIF. Tahapan-tahapan yang sesuai dengan tahapan yang terdapat pada *Reactive Process* model IDFIF dapat dilihat pada lampiran 12. Kolom yang berwarna menunjukkan tahapan yang teridentifikasi sebagai tahapan yang sesuai dengan tahapan *Reactive Process* pada model IDFIF.
5. Mulai dari baris pertama yang telah teridentifikasi, identifikasi juga dekripsi terminologinya, apabila terdapat baris lain yang memiliki deskripsi yang sama, hapus/gabung baris tersebut, sisipkan tahapan yang dihapus/digabung pada baris yang bertahan.
   a. Tahapan yang memiliki terminologi yang sama dengan *identification* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 13. *Identification* memiliki terminologi yang sama dengan

survey dan *recognition*. *Identification* merupakan tahapan untuk melakukan identifikasi TKP yang mencakup memotret, sketsa, pemetaan TKP, pengolahan *chain custody* sampai mencatat siapa saja yang terlibat dalam TKP. Namun, tahapan ini memiliki terminologi yang sama dengan dengan tahapan *documenting the scene* dan *event trigering* pada tahapan *proactive process.* Atas pertimbangan tersebut, maka istilah *identification* tidak digunakan lagi pada tahapan *reactive process* untuk menghindari pengulangan tahapan tersebut.

b. Tahapan yang memiliki terminologi yang sama dengan *acquicition* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 14. *acquicition* memiliki terminologi yang sama dengan *digital evidence acquicition, acquicition processes* dan *potential digital evidence acquicition. Acquicition* merupakan proses pengumpulan barang bukti digital baik *volatile* maupun *non-volatile* dari barang bukti digital. Atas pertimbangan tersebut, maka istilah yang diambil adalah *acquicition.*

c. Tahapan yang memiliki terminologi yang sama dengan *Preservation* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 15. *Preservation* memiliki terminologi yang sama dengan *storage* yang merupakan tahapan untuk menjaga integritas temuan dengan menggunakan *chain custody* dan fungsi *hashing*. Namun, *transportation* adalah tahapan yang digunakan untuk melakukan pemindahan barang bukti dari TKP ke laboratorium. Adapun tahapan yang sama dengan proses *preservation* adalah acquicition. Atas pertimbangan tersebut maka tahapan yang digabung ke tahapan preservation hanya *acquicition* dan *storage* sedangkan untuk *transportation* disimpan di tahapan *proactive process.*

d. Tahapan yang memiliki terminologi yang sama dengan *examination* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 16. *Examination* memiliki terminologi yang sama dengan *digital eviden examination* dan *digital evidence interpretation.*

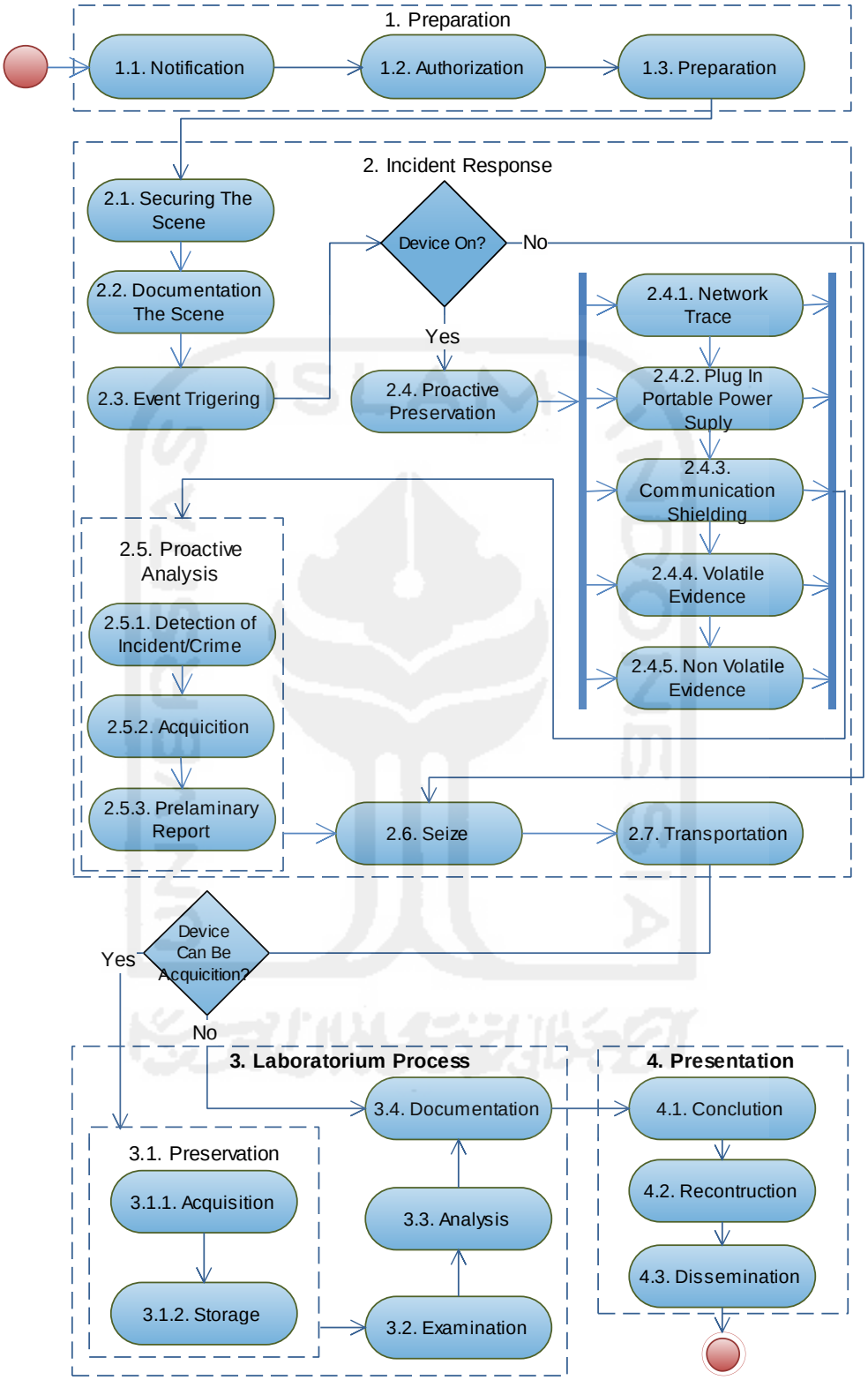
Examination merupakan proses pengolahan barang bukti untuk menemukan keterkaitanya dengan kejadian. Atas pertimbangan tersebut, maka istilah yang diambil adalah *examination.*

e. Tahapan yang memiliki terminologi yang sama dengan *analysis* pada model IDFIF ditandai dengan baris yang berwarna seperti pada lampiran 17. *Analysis* memiliki terminologi yang sama dengan *digital eviden analysis. Analysis* merupakan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada. Atas pertimbangan tersebut, maka istilah yang diambil adalah *analysis.*

6. Apabila semua baris yang teridentifikasi telah terevaluasi namun masih tersisa lebih dari satu baris maka kemudian berikan tahapan baru untuk deskripsi yang bertahan dengan memperhitungkan deskripsi terminologinya, adapun tahapan yang tidak teridentifikasi ditandai dengan baris yang berwarna seperti pada lampiran 18. *Package/packaging* dan *Seize* memiliki terminologi yang tidak dapat dipisahkan sama sekali karena *packaging* proses yang dilakukan secara bersamaan dengan *seize*. Atas pertimbangan tesebut yang digabung hanya menjadi *seize*. Sedangkan *off-set/cloud* memiliki fungsi yang sama dengan tahapan *volatile evidence*. Atas pertimbangan tesebut yang digabung hanya menjadi *volatile evidence*.
7. Berdasarkan pertimbangan antara model DFIF untuk *smartphone investigation* beserta deskripsi terminologinya dan disesuaikan dengan *smartphone investigation activity* di dunia nyata, maka menghasilkan pengurutan dan penyisipan tahapan yang baru seperti pada lampiran 19. Berdasarkan *smartphone investigation activity* di dunia nyata, maka tahapan *proactive process* pada IDFIF diubah namanya menjadi *incident response* sedangkan *reactive process* diubah namanya menjadi *labolatorium process*.

1.4.3. Tahapan IDFIF v2

Setelah mengalami proses eliminasi dan penetuan tahapan baru, tahapan tahapan tersebut di konstruksi kembali menjadi IDFIF v2. Tahapan IDFIF v2 dalam proses investigasi barang bukti digital terutama pada *smartphone* memiliki 4 tahapan utama dan setiap tahapan memilik sub-proses seperti pada gambar 4.2.



Gambar 4.4. Tahapan 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.

a. *Notification* : Pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hokum.
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. *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.

a. *Securing The Scene* : Melakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.
b. *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.
c. *Event Trigering* : Melakukan analisa awal terhadap sebuah proses kejadian yang terjadi. Setelah tahapan ini terdapat *decision process* untuk kondisi barang bukti yang telah ditemukan di TKP yang disebut dengan *Device Mode*. *Dari* tahapan ini diputuskan barang bukti digital tersebut harus langsung disita dan dilakukan pemeriksaan lebih lanjut di laboratorium forensic atau dilakukan pemeriksaan di tempat untuk mendapatkan laporan awal kejadian.
d. *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 lab forensic. *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.

e. *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

f. *Seize* : Memasukkan barang bukti digital yang telah ditemukan di TKP ke tempat yang telah diberi label dan kemudian melakukan proses penyitaan terhadap barang bukti digital tersebut untuk dianalisa lebih lanjut di laboratorium *digital forensics.*

g. *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.

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

4. *Presentation*

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

a. *Conclution* : Menyimpulkan hasil dari investigasi yagng telah dilakukan
b. *Recontruction* : Proses analisa 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

1.5. Tahap 5 SSM: *Comparison Of Model And Real World*

Selanjutnya pada tahapan ini proses membandingkan model konseptual agar sesuai dengan situasi permasalahan pada saat ini(*real world*). Perbandingan tersebut dapat dilihat pada tabel 4.3.

Tabel 4.3. Perbandingan model konseptual dan aktifitas nyata

Model IDFIF v2	Aktifitas Nyata	Rekomendasi
Notification	Ya	-
Authorization	Ya	-

Lanjutan Tabel 4.3. Perbandingan model konseptual dan aktifitas nyata

Model IDFIF v2	**Aktifitas Nyata**	**Rekomendasi**
Preparation	Ya	Setelah *preparation* itu harus ada *decision process* untuk menentukan proses penanganan investigasi yang akan dilakukan. Jika belum dilakukan proses investigasi, maka tim investigasi harus menuju lapangan untuk memeriksa seluruh kejadian namun apabila tim investigasi sebelumnya telah melakukan proses penyitaan terhadap barang bukti digital tersebut, maka proses selanjutnya adalah poses analisa yang dilakukan di laboratorium *forensic*.
Securing The Scene	Ya	-
Documentation The Scene	Ya	-
Event Trigering	Ya	-
Proactive Preservation	Ya	Setelah melakukan tahapan *proactive preservation*, harus ada *decision process* untuk menentukan jenis barang bukti dan proses analisa barang bukti yang telah ditemukan. Apabila memungkinkan untuk dilakukan analisa di tempat maka berlanjut ke proses *proactive analysis* namun apabila waktunya tidak memungkinkan, maka barang bukti tersebut harus langsung disita untuk di bawa ke laboratorium.
Proactive Analysis	Ya	-
Seize	Ya	-
Transportation	Ya	Setelah proses *transportation*, *decision process* selanjutnya adalah untuk menentukan proses penanganan barang bukti digital ke tahapan berikutnya. Jika barang bukti digital yang telah ditemukan tersebut telah dilakukan proses akuisisi di tempat, maka tahapan berikutnya adalah ke proses *examination*. Namun apabila belum dilakukan akuisisi, maka proses berikutnya adalah *preservation*.

Lanjutan Tabel 4.3. Perbandingan model konseptual dan aktifitas nyata

Model IDFIF v2	Aktifitas Nyata	Rekomendasi
Preservation	Ya	Setelah proses *acquicition* pada tahap *preservation* harus ada *decision process* untuk menentukan proses penyimpanan barang bukti ke *evidence room* dan penyimpanan bukti digital ke *evidence storage*.
Examinitation	Ya	-
Analysis	Ya	-
Documentation	Ya	-
Conclution	Ya	-
Recontruction	Ya	-
Dissemination	Ya	-

1.6. Tahap 6 SSM: *Changes Systematically Desirable And Culturally Feasiable*

Proses selanjutnya adalah menentukan hasil perbaikan berdasarkan rekomendasi yang telah ditentukan pada tahap sebelumnya. Adapun hasil dari rekomendasi perbaikan tersebut dapat dilihat pada tabel 4.4.

Tabel 4.4. Hasil rekomendasi perbaikan terhadap IDFIF v2

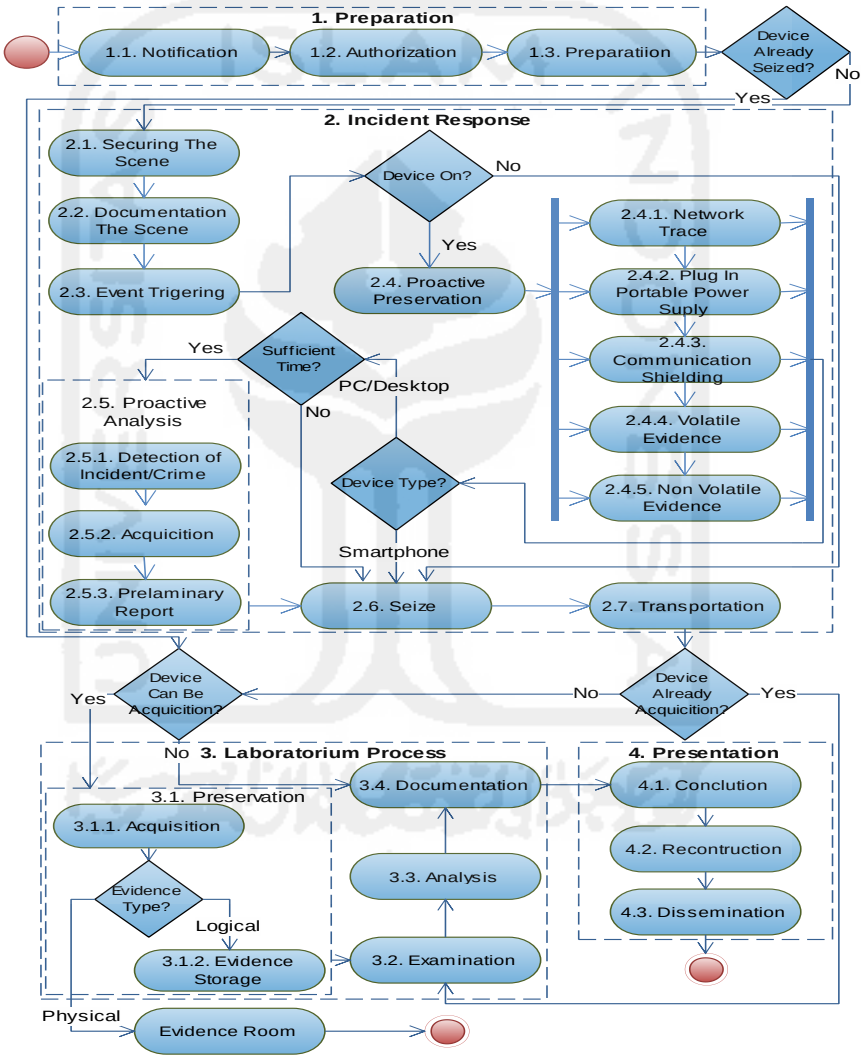
Model IDFIF v2	Rekomendasi	Hasil Perbaikan
Notification		
Authorization		
Preparation	Setelah *preparation* itu harus ada *decision process* untuk menentukan proses investigasi yang akan dilakukan. Jika belum dilakukan proses investigasi, maka tim investigasi harus menuju lapangan untuk memeriksa seluruh kejadian namun apabila tim investigasi sebelumnya telah melakukan proses penyitaan terhadap barang bukti digital tersebut, maka proses selanjutnya adalah poses analisa yang dilakukan di laboratorium forensic.	Penambahan *decision process* untuk menentukan proses investigasi selanjutnya
Securing The Scene	-	-
Documentation The Scene	-	-
Event Trigering	-	-

Lanjutan Tabel 4.4. Hasil rekomendasi perbaikan terhadap IDFIF v2

Model IDFIF v2	**Rekomendasi**	**Hasil Perbaikan**
Proactive Preservation	Setelah melakukan tahapan *proactive preservation*, harus ada *decision process* untuk menentukan jenis barang bukti dan proses analisa barang bukti yang telah ditemukan. Apabila memungkinkan untuk dilakukan analisa di tempat maka berlanjut ke proses *proactive analysis* namun apabila waktunya tidak memungkinkan, maka barang bukti tersebut harus langsung disita untuk di bawa ke laboratorium.	Penambahan *decision process* untuk menentukan jenis barang bukti dan proses analisa barang bukti digital yang telah ditemukan
Proactive Analysis	-	-
Seize	-	-
Transportation	Setelah proses *transportation*, *decision process* selanjutnya adalah untuk menentukan proses penanganan barang bukti digital ke tahapan berikutnya. Jika barang bukti digital yang telah ditemukan tersebut telah dilakukan proses akuisisi di tempat, maka tahapan berikutnya adalah ke proses *examination*. Namun apabila belum dilakukan akuisisi, maka proses berikutnya adalah *preservation*.	Penambahan *decision process* untuk menentukan proses analisa barang bukti digital di laboratorium forensika digital
Preservation	Setelah proses *acquicition* pada tahap *preservation* harus ada *decision process* untuk menentukan proses penyimpanan barang bukti ke *evidence room* dan penyimpanan bukti digital ke *evidence storage*.	Penambahan *decision process* untuk proses penyimpanan barang bukti ke *evidence room* dan penyimpanan bukti digital ke *evidence storage*.
Examinitation	-	-
Analysis	-	-
Documentation	-	-
Conclution	-	-
Recontruction	-	-
Dissemination	-	-

1.7. Tahap 7 SSM: *Action To Improve The Problem Situation*

Berdasarkan hasil rekomendasi perbaikan pada tahapan sebelumnya, maka pada tahapan IDFIF v2 inti ditambahkan 4 decision proses untuk penanganan barnag bukti digital tersebut sehingga model IDFIF v2 ini menjadi lebih fleksible saat diterapkan pada proses penanganan barang bukti digital di lapangan berdasarkan barang bukti yang telah ditemukan. Adapun hasil perbaikan IDFIF v2 tersebut dapat dilihat pada gambar 4.5.



Gambar 4.5. Model IDFIF v2

1.8. *Case Study*

Skenario penanganan barang bukti digital difokuskan pada proses penanganan *smartphone* menggunakan model IDFIF v1 dan model IDFIF v2.

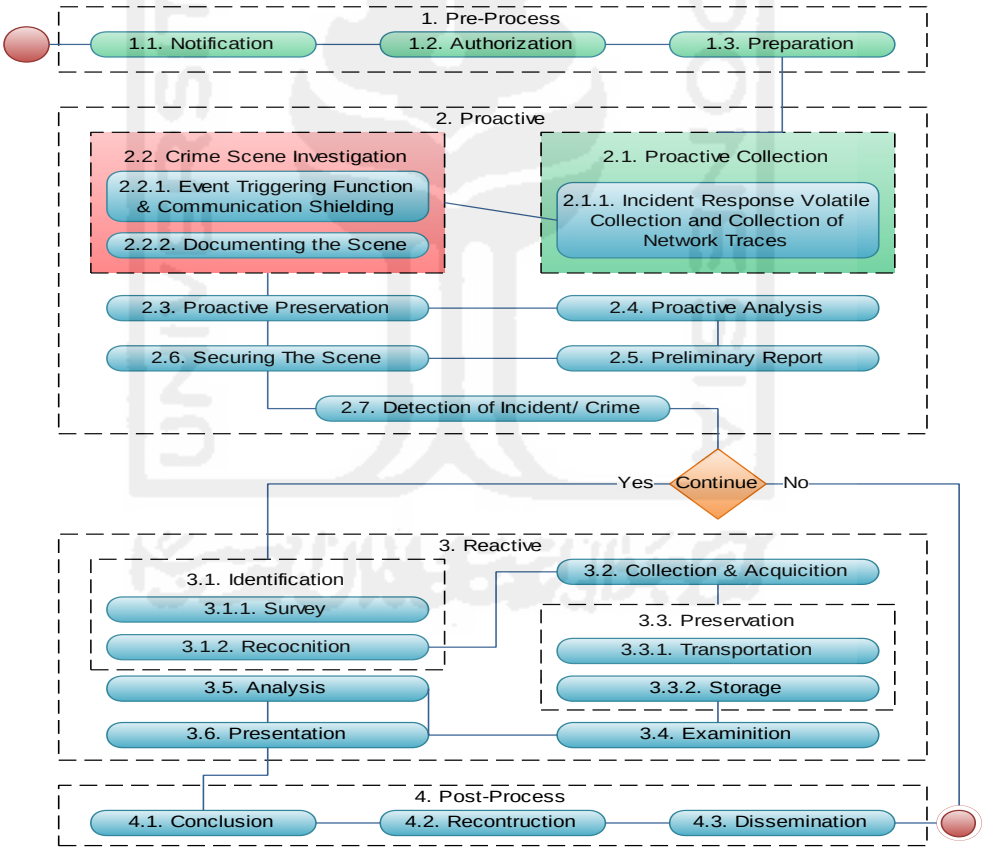
Pengujian kedua model tersebut dilakukan oleh tim yang terdiri dari 2 orang yang masing-masing memilik tugas dan fungsinya selama melakukan pengujian model tersebut, adapaun tim yang tergabung dalam dalam pengujian kedua model tersebut dapat dilihat pada tabel 4.5.

Tabel 4.5. Daftar Tim Penguji Model IDFIF v1 dan IDFIF v2

No	Nama	Keterangan
1	Agus Supriatman, ST.	Melakukan pengujian IDFIF v1 dalam penanganan perangkat *Smartphone*
2	Dian Hermawan, ST.	Melakukan pengujian IDFIF v2 dalam penanganan perangkat *Smartphone*

1.8.1. Model IDFIF v1

Proses penanganan barang bukti digital terhadap *smartphone* mennggunakan model IDFIF v1 dapat dilihat pada gambar 4.6.



Gambar 4.6. Proses penanganan *smartphone* menggunakan model IDFIF v1

Keterangan Warna Tahapan:

: Tahapan IDFIF v1
: Tahapan yang digunakan untuk penanganan *smartphone*
: Tahapan yang tidak dapat digunakan untuk penanganan *smartphone*

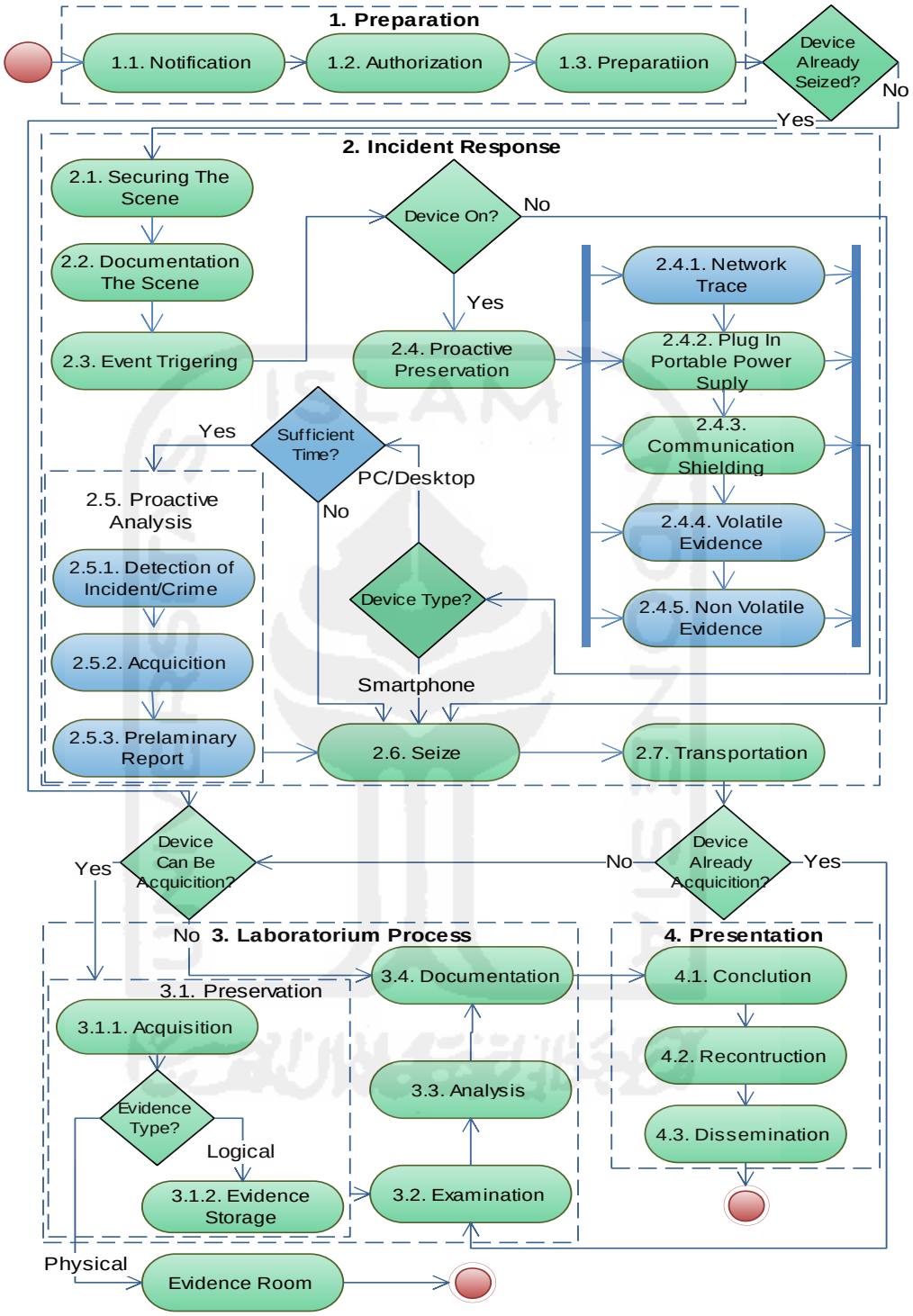
Proactive process merupakan proses olah tempat kejadian perkara untuk mendapatkan semua bukti-bukti yang terkait dengan kejahatan yang telah dilakukan oleh pelaku. Seharusnya proses yang pertama dilakukan dalam olah tempat kejadian perkara adalah *securing the scene*. *Securing the scene* merupakan sebuah mekanisme untuk mengamankan tempat kejadian perkara dan melindungi integritas barang bukti yang ada.

Proses penanganan barang bukti digital *smartphone* menggunakan model ini hanya dapat dilakukan sampai dengan proses *crime scene investigation* karena untuk proses pemeriksaan smartphone harus dilakukan di laboratoium digital forensic sehingga keamanan data yang ada dalam smartphone tersebut dapat terjamin.

Selanjutnya, pada model IDFIF ini tidak ada proses *plug in portable power supply* yang merupakan proses pengamanan *smartphone* dari habisnya sumber daya baterai karena *smartphone* yang di dapatkan di tempat kejadian perkara tidak selalu dalam kondisi penuh. Sedangkan untuk penanganan *smartphone* itu apabila ditemukan dalam keadaan "*on*" maka harus tetap "*on*" dan apabila smartphone tersebut ditemukan dalam keadaan "*off*" harus tetap "*off*".

1.8.2. Model IDFIF v2

Proses penanganan barang bukti digital terhadap *smartphone* mennggunakan model IDFIF v2 dapat dilihat pada gambar 4.7. Tahapan *Pre-Process* pada model IDFIF v1 memiliki persamaan dengan tahapan *Preparation* pada model IDFIF v2 dan tahapan *Post-Process* pada IDFIF v1 memiliki persamaan dengan tahapan *Presentation* pada IDFIF v2 sehingga focus pengujian model IDFIF v2 ini hanya dilakukan pada tahapan *Incident Response* (*Securing the Scene, Documentation the Scene, Event Triggering, Proactive Preservation, Plug in Portable Power Supply, Communication Shielding* dan *Transportation*) dan pada tahapan *Labolatorium Process*.



Gambar 4.7. Proses penanganan *smartphone* menggunakan model IDFIF v2

Keterangan Warna Tahapan:

: Tahapan yang digunakan untuk penanganan komputer
: Tahapan yang digunakan untuk penanganan *smartphone*

Incident Response sama halnya dengan *proactive collection* yaitu merupakan proses olah tempat kejadian perkara untuk mendapatkan semua bukti-bukti yang terkait dengan kejahatan yang telah dilakukan oleh pelaku. Namun ada beberapa tahapan yang harus dilakukan dalam *incident response* untuk penanganan barang bukti *smartphone* yaitu *securing the scene, documentation the scene, event triggering, proactive preservation, plug in portable power supply, communication shielding, seize* dan *transportation*.

1. ***Securing the scene***

   Tahapan pertama yang harus dilakukan dalam pelaksanaan olah tempat kejadian perkara(*Incident Response*) adalah menjaga lokasi kejadian dari orang-orang yang tidak memiliki kepentingan dalam proses investigasi sehingga integritas barang bukti digital dapat dijamin keasliannya.

2. ***Documentation the scene***

   Setelah pengamanan tempat kejadian perkara adalah melakukan dokumentasi terhadap wilayah sekitar dan barang yang berpotensi sebagai barang bukti dengan cara memotrek TKP dan barang bukti secara fotografi forensic (foto umum, foto menengah dan foto *close up*).

3. ***Event triggering***

   Melakukan proses analisa awal terhadap suatu kejadian yang telah terjadi di tempat kejadian perkara.

4. ***Proactive preservation***

   Merupakan 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 forensik.

Gambar 4.9. *Plug in portable power supply*

Plug in portable power supply merupakan proses *charging* terhadap barang bukti *smartphone* menggunakan *portable power supply* karena kondisi daya baterai pada *smartpone* yang di temukan adalah 49% 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 merupakan tahapan 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.

Gambar 4.10. *Isolating* menggunakan *faraday bag*

5. *Seize*

Setelah proses pengamanan daya baterai dan isolasi, pada tahapan selanjutnya adalah proses penyitaan(*seize*) barang bukti *smartphone* untuk diperiksa di laboratorium digital forensic.

6. *Transportation*

Tahapan berikutnya adalah proses pemindahan barang bukti yang telah di temukan dari tempat kejadian perkara menuju laboratorium digital forensic. Ketika dalam proses *transportation*, barang bukti *smartphone* harus benar-benar dijaga keadaannya supaya tidak ada yang berubah sedikitpun dan mengurangi integriatas barang bukti tersebut.

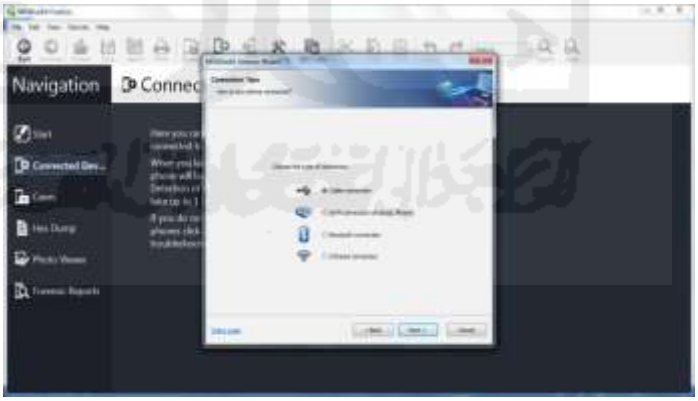
Tahapan selanjutnya adalah *laboratorium process* yang merupakan proses pemeriksaan *smartphone* di laboratorium digital forensik. Adapun tahapan yang dilakukan dalam proses pemeriksaan di laboratorium digital forensic yaitu *preservation, acquicition, storage, examination, analysis* dan *documentation*.

1. *Preservation*

Preservation dalam *laboratorium process* merupakan proses pengamanan barang bukti *smartphone*. Kondisi *smartphone* ketika dalam proses akuisisi harus dalam keadaan terputus dari komunikasi data yang ada seperti pada gambar 4.11.

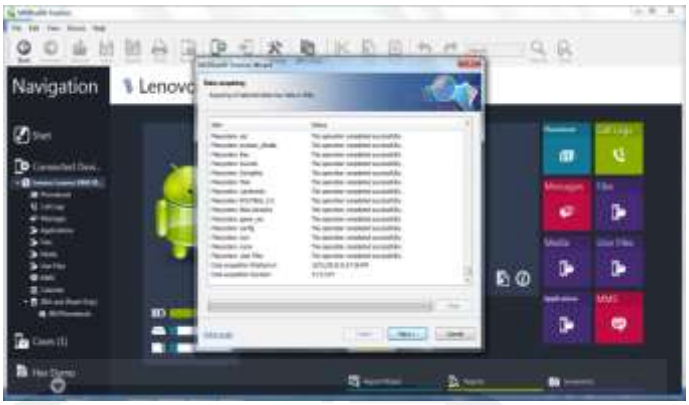
Gambar 4.11. Tampilan *layar smartphone*

Proses *acquicition* merupakan hal pertama yang harus dilakukan di laboratorium digital forensic terhadap perangkat *smartphone* yang telah ditemukan di tempat kejadian perkara..



Gambar 4.12. Proses menghubungkan *smartphone* dengan *notebook*

Gambar 4.12 memperlihatkan proses penghubungan barang bukti *smartphone* dengan *notebook* dengan memanfaatkan koneksi kabel data.



Gambar 4.13. Proses akuisisi *smartphone*

Proses akuisisi data pada *smartphone* ini menggunakan tool *mobiledit 7.5* seperti yang terlihat pada gambar 4.13. 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 merupakan proses penyimpanan barang bukti *smartphone* ke tempat yang 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.

2. *Examination*

Examination merupakan proses pengolahan barang bukti digital untuk menemukan keterkaitanya dengan kejadian kejahatan yang telah dilakukan oleh pelaku terhadap korban

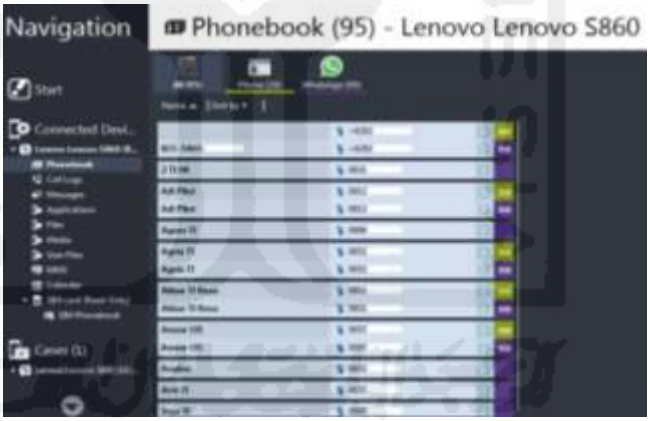
3. *Analysis*

Analysis merupakan proses kajian teknis dalam pemeriksaan barang bukti *smartphone* dan merangkai keterkaitan antara temuan-temuan yang ada. Setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan diatas, selanjutnya data tersebut dianalisis secara detail dan komprehensit untuk dapat membuktikan kejahatan apa yang terjadi dan

kaitannya pelaku dengan kejahatan tersebut. Hasil analisis terhadap data digital tadi selanjutnya disebut sebagai barang bukti digital yang harus dapat dipertanggungjawabkan secara ilmiah dan hukum di Pengadilan.

Gambar 4.14. Hasil akuisisi *smartphone*

Gambar 4.14 merupakan tampilan awal dari hasil akuisisi smartphone. Pada gambar tersebut 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*.



Gambar 4.15. Daftar kontak pada *smartphone*

Gambar 4.15 menampilkan daftar kontak yang terdapat pada *smartphone* yang telah diakuisisi. Selain itu, terlihat juga daftar kontak yang terdapat pada *WhatApp.*

Gambar 4.16. Daftar telepon keluar pada *smartphone*

Gambar 4.16 menampilkan catatan telepon keluar. Dari catatan tersebut dapat dilihat nama orang yang ditelepon, nomor telepon dan waktu melakukan panggilan keluar

Gambar 4.17. Daftar telepon keluar pada *smartphone*

Gambar 4.17 menampilkan catatan telepon masuk. Dari catatan tersebut dapat dilihat nama orang yang menelepon, nomor telepon dan waktu menerima panggilan dari luar.

Gambar 4.18. Daftar pesan pada *smartphone*

Gambar 4.18 menampilkan catatan percakapan melalui pesan singkat. Dari catatan tersebut dapat dilihat nama penerima dan pengirim pesan singkat, nomor telepon dan waktu penerimaan dan pengiriman pesan singkat.

Gambar 4.19. Daftar aplikasi pada *smartphone*

Gambar 4.19 menampilkan seluruh jenis dan daftar aplikasi yang digunakan pengguna pada *smartphone* tersebut.

Gambar 4.20. Daftar *file system* pada *smartphone*

Gambar 4.20 menampilkan seluruh file system yang terdapat pada *smartphone* yang telah diakuisisi.

Gambar 4.21. Daftar *user file* pada *smartphone*

Gambar 4.21. menampilkan seluruh aplikasi pada *smartphone* yang digunakan oleh *user*.

Gambar 4.22. Data *simcard* pada *smartphone*

Gambar 4.22 menampilkan informasi yang terdapat pada simcard diantaranya 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*). MCC untuk Indonesia yaitu 510, sedangkan MNC untuk operator-operator yang ada di Indonesia dapat dilihat pada tabel 4.6.

Tabel 4.6. Daftar kode operator(MNC) di Indonesia

No	MCC	MNC	Operator	Perusahaan
1.	510	00	PSN	PT Pasifik Satelit Nusantara (ACeS)
2.	510	01	INDOSAT	PT Indonesian Satellite Corporation Tbk (Indosat)
3.	510	03	StarOne	PT Indonesian Satellite Corporation Tbk (Indosat)
4.	510	07	TelkomFlexi	PT Telkom
5.	510	08	AXIS	PT Natrindo Telepon Seluler
6.	510	09	SMART	PT Smart Telecom
7.	510	10	Telkomsel	PT Telekomunikasi Selular
8.	510	11	XL	PT XL Axiata Tbk
9.	510	20	TelkomMobile	Pt Telcom Indonesia TBK
10.	510	21	IM3	PT Indonesian Satelite Corporation Tbk (Indosat)
11.	510	27	Ceria	PT Sampoerna Telekomunikasi Indonesia
12.	510	28	Fren/Hepi	PT Mobile-8 Telecom
13.	510	89	3	PT Hutchison CP Telecommunications
14.	510	99	Esia	PT Bakrie Telecom

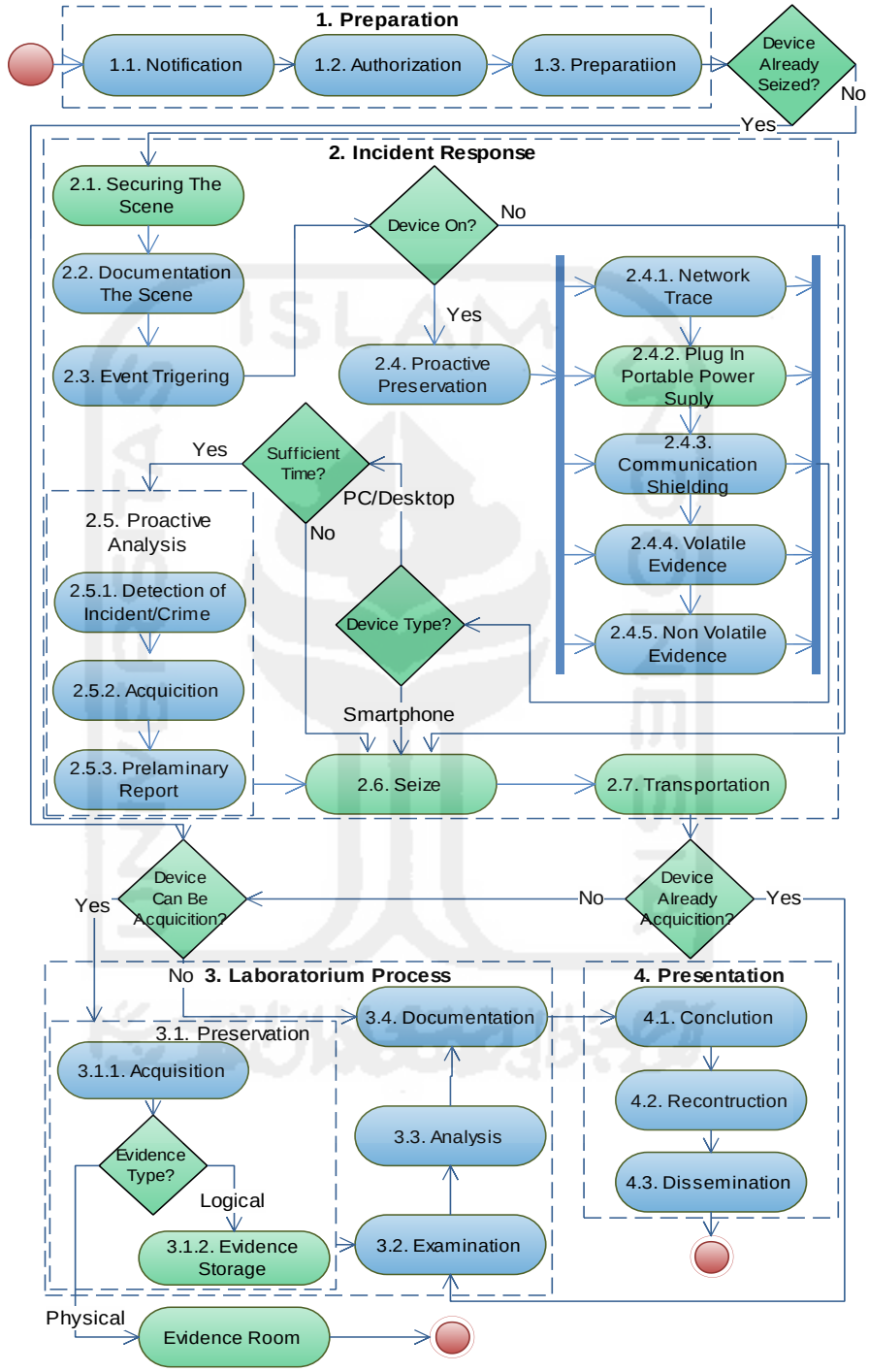
4. *Documentation*

Dokumentation merupakan proses pembuatan laporan tertulis tentang kegiatan investigasi barang bukti *smartphone* yang dilakukan dari awal pemeriksaan hingga akhir pemeriksaan yang nantinya laporan tersebut akan dijadikan sebagai bahan pertimbangan oleh hakim di pengadilan dalam proses pengambilan keputusan.

1.9. *Evaluation Result*

Proses evaluasi terhadap IDFIF v2 dilakukan dengan cara memberikan lembar kuesioner tentang *framework* tersebut kepada para ahli dan kemudian membandingkan model IDFIF v2 dengan IDFIF v1. Adapun hasil dari kuesioner tersebut dapat dilihat pada lampiran 20.

Perbedaan tahapan IDFIF v2 dengan IDFIF v1 dapat dilihat pada gambar 4.23.



Gambar 4.23. Perbedaan IDFIF v1 dengan IDFIF v2

Keterangan Warna Tahapan:

: Tahapan awal IDFIF
: Tahapan yang ditambahkan/diperbaiki

Perbedaan model IDFIF v2 dengan IDFIF v1 dapat dilihat pada tabel 4.7.

Tabel 4.7. Perbedaan Model IDFIF v2 dengan Model IDFIF v1

Tahapan			IDFIF		Keterangan
			v1	v2	
1	*Preparation*		√	√	
	1.1	*Notification*	√	√	
	1.2	*Authorization*	√	√	
	1.3	*Preparation*	√	√	Pada IDFIF v1 setelah tahapan ini tidak ada proses *decition* apabila barang bukti telah disita
2	*Incident Response*		√	√	
	2.1	*Securing The Scene*	√	√	Pada IDFIF v1 tahapan ini diletakkan setelah proses *Preliminary Report*
	2.2	*Documentation The Scene*	√	√	
	2.3	*Event Trigering*	√	√	
	2.4	*Proactive Preservation*	√	√	Pada IDFIF v1 setelah tahapan ini tidak ada proses *decition* penanganan bararang bukti berdasarkan *device type* yang ditemukan
		2.4.1 *Network Trace*	√	√	
		2.4.2 *Plug In Portable Power Suply*	X	√	
		2.4.3 *Communication Shielding*	√	√	
		2.4.4 *Volatile Evidence*	√	√	
		2.4.5 *Non Volatile Evidence*	X	√	
	2.5	*Proactive Analysis*	√	√	
		2.5.1 *Detection Of Incident Crime*	√	√	
		2.5.2 *Acquicition*	√	√	
		2.5.3 *Prelaminary Report*	√	√	
	2.6	*Seize*	X	√	
	2.7	*Transportation*	√	√	

Lanjutan Tabel 4.7. Perbedaan Model IDFIF v2 dengan Model IDFIF v1

Tahapan			IDFIF		Keterangan
			v1	v2	
3	*Laboratorium Process*		√	√	
	3.1	*Preservation*	√	√	
		3.1.1 *Acquicition*	√	√	
		3.1.2 *Evidence Storage*	√	√	
	Evidence Room		X	√	
	3.2	*Examination*	√	√	
	3.3	*Analysis*	√	√	
	3.4	*Documentation*	√	√	
4	*Presentation*		√	√	
	4.1	*Conclution*	√	√	
	4.2	*Recontruction*	√	√	
	4.3	*Dissemination*	√	√	

Setelah dilakukan perbandingan IDFIF v1 dan IDFIF v2 menggunakan tabel, maka untuk mengetahui perbedaan jumlah tahapan pada kedua model tersebut sehingga dapat diketahui nilai perbedaanya dilakukan dengan cara memberikan nilai 0 untuk tahapan yang tidak ada pada model tersebut dan memberikan nilai 1 untuk tahapan yang ada pada model tersebut. Setelah mengetahui nilai dari setiap tahapan tersebut, maka tahapan selanjutnya adalah melakukan perhitungan sehingga dapat diketahui nilai persentase tahapannya mengunakan cara seperti dibawah ini:

1. Nilai Persentase IDFIF v1:

$$NI_1 = \frac{\sum TI_1}{\sum TT} \text{ X } 100\%$$

Keterangan:

$\sum TI_1$: Jumlah Tahapan IDFIF v1

$\sum TT$: Jumlah Tahapan Total

NI_1 : Nilai Persentase Tahapan IDFIF v1

$$\frac{28}{32} \text{ X } 100\% = 87{,}5\%$$

Nilai persentase tahapan IDFIF v 1 berdasarkan hasil perhitungan tersebut adalah 87,5% dari seluruh tahapan yang ada.

2. Nilai Persentase IDFIF v2:

$$NI_2 = \frac{\sum TI_2}{\sum TT} \text{ X } 100\%$$

Keterangan:

$\sum TI_2$: Jumlah Tahapan IDFIF v2

$\sum TT$: Jumlah Tahapan Total

NI_2 : Nilai Persentase Tahapan IDFIF v2

$$\frac{32}{32} \text{ X } 100\% = 100\%$$

Nilai persentase Tahapan IDFIF v 2 berdasarkan hasil perhitungan tersebut adalah 100% dari seluruh tahapan yang ada.

3. Selisih Nilai Persentase Tahapan IDFIF v2 dan IDFIF v1

Selanjutnya adalah melakukan perhitungan untuk mengetahui rentan perbedaan tahapan antara kedua model tersebut dengan cara melakukan perhitungan seperti dibawah ini:

$$NI_2 - NI_1 = 100\% - 87{,}5\% = 12{,}5\%$$

Berdasarkan perhitungan tersebut, maka nilai persentase perbedaan tahapan antara model IDFIF v1 dan model IDFIF v2 adalah 12,5%.

1.10. *Analysis and Evaluation*

Setiap *digital forensic model* memiliki tahapan yang berbeda-beda dalam setiap penanganan barang bukti digital yang ditemukan sehingga untuk penanganan barang bukti yang berbeda memerlukan *digital forensic model* yang berbeda juga. Seharusnya *digital forensic model* tersebut dapat diterapkan terhadap seluruh barang bukti digital yang ditemukan di lapangan. Perbedaan setiap model tersebut dapat dilihat pada tabel 4.8.

Tabel 4.8. Perbandingan *Digital Forensic Model* untuk *Smartphone*

IDFIF v2	**WMFPM**	**SSFPM**	**ACPO**	**SFIPM**	**ISO/IEC 27041**	**NIST**	**HDFIP**
Notification					√		√
Authorization			√		√		√
Preparation	√	√		√	√	√	√
Securing The Scene	√		√	√		√	
Documentation The Scene	√		√		√	√	
Event Trigering	√				√	√	√
Proactive Preservation	√		√	√	√	√	√
Proactive Analysis				√			√
Seize			√			√	
Transportation			√		√	√	
Preservation		√	√	√	√	√	√
Examinitation	√	√	√	√	√	√	√
Analysis	√	√	√	√	√	√	√
Documentation	√		√	√	√	√	√
Conclution	√	√		√			√
Recontruction							
Dissemination							

Berdasarkan tabel 4.5, model IDFIF v2 memiliki tahapan penanganan barang bukti digital yang lebih lengkap dari NIST, ACPO, ISO 27041, SFIPM, SSFPM, HDFIP dan WMDFM.

Setiap *digital forensic model* juga memiliki kelebihan dan kekurangan dalam proses penanganan barang bukti digital. Adapun kelebihan dan kekurangan setiap model tersebut dapat dilihat pada tabel 4.9.

Tabel 4.9. Perbedaan *Digital Forensic Model* untuk Penanganan *Smartphone*

Nama Pembuat	Nama Model	Kelebihan	Kekurangan
Ruuhwan	*Integrated Digital Forensic Investigation Framework v2*	Memiliki tahapan yang fleksible ketika digunakan dalam proses investigasi komputer dan *smartphone*	Belum bisa digunakan untuk proses investigasi *network* dan *cloud*
Rahayu	*Integrated Digital Forensic Investigation Framework*	Dapat mengakomodir seluruh tahapan pada DFIF yang ada	Tidak dapat digunakan untuk proses investigasi *smartphone*
NIST	*Smartphone Forensic Investigation*	Memiliki tahapan yang lengkap untuk penanganan *smartphone*	Tidak ada proses penanganan barang bukti digital di tempat kejadian. Seluruh barang bukti diperiksa di laboratorium.
ACPO	*Good Practice Guide For Computer Based Electronic Evidence Internet*	4 prinsip ACPO dapat mengakomodir seluruh barang bukti elektronik	3 dari 4 prinsip ACPO tidak dapat diterapkan pada penanganan barang bukti *smartphone*
ISO	*Smartphone Forensic Investigation(*ISO 27041)	Memiliki tahapan yang lengkap untuk penanganan barang bukti digital secara umum	Tidak ada proses pengamanan tempat kejadian.
Goel, Tyagi & Agrawal	*Smartphone Forensic Investigation Process Model*	Memiliki tahapan yang lengkap untuk penanganan *smartphone*	Dokumentasi hanya dilakukan setelah pemeriksaan barang bukti *smartphone*
Mohtasebi & Dehghantanha	*Symbian Smartphones Forensic Process Model*	Memiliki tahapan yang lengkap untuk penanganan *smartphone*	Semua tahapan tersebut dilakukan di tempat.
Raymond & Venter	*Harmonised Digital Forensic Investigation Process*	Memiliki tahapan yang lengkap untuk penanganan barang bukti digital secara umum	Tidak ada proses pengamanan tempat kejadian dan dokumentasi di tempat kejadian.
Anup Ramabhadran	*Windows Mobile Device Forensic Model*	Tahapannya cukup spesifik untuk penanganan *smartphone*	Semua tahapan tersebut dilakukan di tempat.

Berdasarkan tabel 4.6, model IDFIF v2 memiliki tahapan penanganan barang bukti digital yang lebih *fleksible* ketika digunakan dalam proses investigasi komputer dan *smartphone*.