ANALISIS *DIGITAL EVIDENCE GLOBAL POSITIONING SYSTEM* BERBASIS *SMARTPHONE* ANDROID MENGGUNAKAN METODE *HYBRID EVIDENCE INVESTIGATION*

TESIS

Disusun Sebagai Salah Satu Syarat untuk
memperoleh Gelar Magister Komputer
Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Oleh

I PUTU EKA WARMAYUDHA

NPM : 2019210007

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA & KOMPUTER - LIKMI
BANDUNG
2020

ANALISIS *DIGITAL EVIDENCE GLOBAL POSITIONING SYSTEM* BERBASIS *SMARTPHONE* ANDROID MENGGUNAKAN METODE *HYBRID EVIDENCE INVESTIGATION*

Oleh

I PUTU EKA WARMAYUDHA

NPM : 2019210007

Bandung, 27 Oktober 2020
Menyetujui,

Prof. Dr. Ana Hadiana, M.Eng. Sc.
Pembimbing

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA & KOMPUTER - LIKMI
BANDUNG

2020

Dipersembahkan untuk

Keluarga Tercinta

Bapak Nyoman *dan* **Ibu Ketut**

Istri ku Yunantari, anak ku Galih Kanaka,

& **Juna Nayaka**

Serta

Kepolisian Republik Indonesia

ABSTRAK

ANALISIS DIGITAL EVIDENCE GLOBAL POSITIONING SYSTEM BERBASIS SMARTPHONE ANDROID MENGGUNAKAN METODE HYBRID EVIDENCE INVESTIGATION

I Putu Eka Warmayudha

NPM : 2019210007

Global Positioning System (GPS) merupakan salah satu *digital evidence* yang tidak pernah mendapatkan perhatian dari tim investigator atau pihak penegak hukum. GPS merupakan *software* yang terpasang didalam *smartphone* dan satnav (sistem navigasi satelit), berfungsi untuk alat bantu dari tim penyidik sebagai alat lacak dari keberadaan tersangka tindak kriminalitas. *Digital evidence* yang bersumber dari GPS merupakan hal penting dalam hal keberhasilan pengungkapan kasus kriminalitas, Para pelaku kriminalitas juga menggunakan GPS untuk saling berkomunikasi perihal lokasi yang menjadi target operasi. Pelaku kriminalitas juga menyimpan berbagai data penting seperti peta atau foto yang merupakan lokasi sasaran.

Hybrid Evidence mengacu pada physical evidence dan digital evidence, menambahkan kemungkinan physical evidence tersebut dapat memiliki hidden digital evidence, karakteristik harus dikondisikan dalam penyelidikan kasus kriminalitas. Sebagai contoh, Ballpoint yang kamera mikro ataupun mikrofon yang digunakan untuk merekam video dan suara, contoh lainnya yaitu selembar kertas yang memiliki chip RFID yang berisi informasi pelacakan. Hybrid model dapat digunakan dalam penyelidikan, yang hanya menggunakan physical evidence atau digital evidence yang tersedia. Model Hybrid Evidence Investigation terdapat 4 utama dan 12 tahapan sekunder, yaitu: Preparation, Crime Scene Investigation, Laboratory Examination, Conclusion atau dikenal dengan istilah HEI.

Hasil analisis terhadap smartphone yang dilakukan menghasilkan beberapa data yaitu SMS, Call Logs, Phone Book, file image, calendar dan note, juga mengambil semua informasi telepon, seperti IMEI, sistem operasi, firmware termasuk rincian SIM (IMSI), ICCID dan yang terakhir digunakan BTS. Metode Hybrid Evidence Investigation dapat diimplementasikan pada proses penyelidikan, karena dengan menggunakan metode Hybrid Evidence Investigation, physical evidence dan digital evidence dapat dilakukan secara bersamaan, tanpa harus mengganggu bukti yang lainnya.

Kata Kunci: *Digital Evidence, Global Positioning System, Smartphone, Hybrid Evidence Investigation*

ABSTRACT

DIGITAL EVIDENCE GLOBAL POSITIONING SYSTEM BASED ON ANDROID SMARTPHONE USING HYBRID EVIDENCE INVESTIGATION METHOD
I Putu Eka Warmayudha
NPM : 2019210007

Global Positioning System (GPS) is digital evidence that has never been noticed by the investigator team or law enforcement officials. GPS is software installed in smartphones and satnav (satellite navigation system), which functions as a tool for the investigation team as a means of tracking the whereabouts of criminal suspects. Digital evidence sourced from GPS is important in terms of the successful disclosure of criminal cases. Criminals also use GPS to communicate with each other about the locations targeted by operations. Criminals also store various important data such as maps or photos of the target location.

Hybrid Evidence refers to physical evidence and digital evidence, adding the possibility that physical evidence can have hidden digital evidence, characteristics that must be conditioned in the investigation of criminal cases. For example, a Ballpoint, which is a micro camera or microphone that is used to record video and sound, another example is a sheet of paper that has an RFID chip containing tracking information. Hybrid models can be used in investigations, which only use available physical evidence or digital evidence. The Hybrid Evidence Investigation model has 4 main and 12 secondary stages, namely: Preparation, Crime Scene Investigation, Laboratory Examination, Conclusion, or known as HEI.

The results of the analysis of smartphones carried out produce some data, namely SMS, Call Logs, Phone Book, image files, calendars, and notes, also retrieve all phone information, such as IMEI, operating system, firmware including SIM details (IMSI), ICCID and most recently used. BTS. The Hybrid Evidence Investigation method can be implemented in the investigation process, because by using the Hybrid Evidence Investigation method, physical evidence, and digital evidence can be carried out simultaneously, without having to disturb other evidence.
Keywords: *Digital Evidence, Global Positioning System, Smartphone, Hybrid Evidence Investigation*

KATA PENGANTAR

Dengan memanjatkan Puji dan Syukur Kepada Ida sang Hyang Widi Wasa atas segala Rahmat dan Karunianya pada penulis, akhirnya penulis dapat menyelesaikan penyusunan tesis yang berjudul: **ANALISIS *DIGITAL EVIDENCE GLOBAL POSITIONING SYSTEM* BERBASIS *SMARTPHONE* ANDROID MENGGUNAKAN METODE *HYBRID EVIDENCE INVESTIGATION*.**

Tesis ditulis dalam rangka memenuhi sebagai persyaratan untuk memperoleh gelar **Magister Komputer (M.Kom)** di Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI. Penulis menyadari bahwa tesis dapat diselesaikan berkat dukungan dan bantuan dari berbagai pihak, oleh karena itu penulis berterima kasih kepada semua pihak yang secara langsung maupun tidak langsung memberikan kontribusi dalam menyelesaikan Tesis ini. Selanjutnya ucapan terima kasih penulis sampaikan kepada:

1. Prof. Dr. Ana Mardiana, M.Eng. Sc. sebagai Dosen Pembimbing yang telah mengarahkan dan membimbing penulis selama penyusunan tesis ini.
2. Dr. Budi Permana, S.E., Ak., M.Sc. sebagai Ketua Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI.
3. Kepada Orang Tua Saya. Bapak Nyoman dan Ibu Ketut yang selalu mendukung dan mendoakan walaupun terbatas jarak dan pulau.
4. Istri dan Anak Saya tercinta. Yunantari dan Galih Kanaka yang selalu memberikan semangat serta motivasi tanpa henti di setiap langkah Saya.
5. Seluruh Dosen dan Staff di Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI.
6. Kepala dan Staff Kepolisian Republik Indonesia ditempat Penulis bekerja dan melakukan penelitian tesis.
7. Teman-teman Mahasiswa/i Program Pasca Sarjana Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, yang selalu mendukung dan berkonsultasi di setiap permasalahan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi Internet, pengiriman data yang berupa media digital seperti gambar, audio, video dan teks dikirimkan melalui Internet dengan sangat mudah. Namun, salah satu tantangan utama dalam berbagi dan mentransmisikan berbagai jenis informasi melalui saluran publik yaitu keamanan data. Oleh karena itu, beberapa cara untuk melindungi informasi yang dikirimkan oleh seorang penyadap dan pihak yang tidak berwenang menjadi sebuah hal penting (Suryanto, 2016).

Pada era digitalisasi, *Smartphone* atau ponsel sudah beralih fungsi dari sebuah perangkat komunikasi suara menjadi alat komunikasi dengan dilengkapi berbagai macam fungsi. *Smartphone* yang beredar saat ini sudah dilengkapi dengan teknologi dan fasilitas yang dapat melakukan seperti komputer. Dampak negatif yang ditimbulkan dari perkembangan teknologi tersebut pada tahun 2010, DFAT (Digital Analis Forensik Team) Puslabfor Mabes Kepolisian Republik Indonesia berhasil memeriksa 214 *digital evidence* dari 52 kasus yang terdiri dari berbagai kasus kejahatan seperti: Pornografi, Korupsi, Perjudian, Penyuapan, Penipuan, Pencemaran Nama Baik, Narkoba dan sebagainya. Total keseluruhan dari jumlah kejahatan yang terjadi, terdapat 118 jenis *digital evidence* yang didapatkan dari *smartphone* (Al-Azhar, 2012).

Global Positioning System (GPS) merupakan salah satu *digital evidence* yang tidak pernah mendapatkan perhatikan dari Tim Investigator atau Pihak Penegak Hukum. GPS merupakan *software* yang terpasang didalam *smartphone* dan satnav (sistem navigasi satelit), berfungsi untuk alat bantu dari tim penyidik sebagai alat lacak dari keberadaan tersangka tindak kriminalitas. Perusahaan para pengembang *software* yang diperuntukkan untuk GPS melakukan pengembangan sistem, pada ranah *computer forensic* dalam hal pengembangan produk navigator satelit yang dilengkapi dengan alat dan teknologi untuk memperoleh *digital evidence* (Chen, 2013).

Digital evidence yang bersumber dari GPS merupakan hal penting dalam hal keberhasilan pengungkapan kasus kriminalitas. Sebagai contoh: aktivitas pelaku kriminalitas, pelaku menggunakan *smartphone* bertujuan untuk saling berkomunikasi, tukar menukar bahkan menyimpan informasi yang terkait dengan kriminalitas yang dilakukan. Pelaku kriminalitas menggunakan *smartphone* untuk berkomunikasi dengan pelaku lainnya dari tim atau grup kriminal yang dibentuk. Para pelaku kriminalitas juga menggunakan GPS untuk saling berkomunikasi perihal lokasi yang menjadi target operasi. Pelaku kriminalitas juga menyimpan berbagai data penting seperti peta atau foto yang merupakan lokasi sasaran.

Osama bin Laden berhasil ditemukan di Pakistan oleh pasukan AS dengan cara pelacakan *call logs* dari panggilan menggunakan satelit yang dilakukan oleh pengawalnya (Goel, 2012). Kasus lainnya yang terungkap karna GPS yaitu empat tersangka bersenjata dituduh merampok Bank di Inggris, dihukum karna pelaku mempunyai kendaraan dengan fasilitas satnav sehingga menjadi bukti yang memberatkan, termasuk alamat Bank, alamat dari tiga pelaku lainnya (Chen, 2013).

Proses investigasi yang terkait *digtal evidence* yang dilakukan oleh Divisi Forensik Kepolisian Republik Indonesia saat ini hanya menggunakan 2 tahapan, yaitu tahap *collection/examination* dan tahap *reporting*. Berdasarkan hal tersebut, penulis menggunakan metode *hybrid evidence investigation* dalam pengungkapan suatu kasus kriminalitas.

1.2 Rumusan Masalah

Berdasarkan pada batasan masalah, dan agar permasalahan tidak terlalu melebar, penulis merinci bagian permasalahan sebagai berikut:

1. Bagaimana melakukan analisis dari kumpulan *digital evidence* yang bersumber dari *Global Positioning System* yang terdapat pada *smartphone* pelaku tindak kriminalitas.

2. Bagaimana menerapkan model *Hybrid Evidence Investigation* untuk proses investigasi *digital evidence* yang didapatkan dari proses olah TKP (Tempat Kejadian Perkara).

1.3 Tujuan Penelitian

Tujuan dari dilakukan penelitian ini adalah mengetahui proses investigasi *mobile forensic* berbasis *Global Positioning System* di *smartphone* Android, mengetahui potensi bukti data digital yang terdapat pada *smartphone* Android dan melakukan investigasi *digital evidence* pada *smartphone* Android menggunakan metode *Hybrid Evidence Investigation*.

1.4 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini adalah analisis d*igital evidence* yang disesuaikan dari data GPS (*Global Positioning System)* yang terdapat pada *smartphone* pelaku tindak kriminalitas, *smartphone* yang digunakan dalam penelitian ini berbasis Android dan dilakukan proses penyidikan perangkat *smartphone* pelaku kriminalitas dengan mencari bukti berupa percakapan *digital* melalui pesan teks dan aplikasi *messenger* dan dilakukan GPS *Extraction*, GPS *Conversion* dan GPS *Presentation* di *smartphone* pelaku.

1.5 Sistematika Penelitian

Usulan tesis ini disusun untuk mempermudah pembahasan dengan sistematika sebagai berikut :

BAB 1 PENDAHULUAN

Bab Pendahuluan berisi Latar Belakang, Identifikasi Masalah, Tujuan Riset, Ruang Lingkup Riset, Metodologi Riset, Sistematika Penelitian.

BAB II LANDASAN TEORI

Bab Landasan Teori berisi teori pendukung penelitian ini, diantaranya: *Digital Forensic, Digital Forensic Investigation Famework* (DFIF), Investigasi Forensika, *Mobile Forensic*, Barang Bukti, *Global Positioning System* (GPS), *Digital Evidence, Hybrid Evidence Investigation*, Arsitektur GPS, Teknologi GPS disertai dengan A-GPS *Smartphone,* Mengukur Posisi Geografis, Data *Latitude* dan Data *Longtitude*, Kesesuaian Data untuk *Digital Forensic*.

BAB III OBJEK DAN METODOLOGI PENELITIAN

Bab Objek dan Metodologi Penelitian berisi metode yang digunakan pada penelitian ini yang berupa penerapan model *Hybrid Evidence Investigation* berbasis *smartphone* android*.*

BAB IV HASIL DAN PEMBAHASAN

Bab Hasil dan Pembahasan berisi Penerapan *Framework* Dalam Proses Investigasi Bukti Digital GPS Pada *Smartphone* Android, r*esources, preparation, communication Shielding, Data Acquistion, Analysis (*GPS *Extraction, GPS Conversion, reporting,* GPS *Presentation, Archiving.*

BAB V KESIMPULAN DAN SARAN

Bab Kesimpulan dan Saran berisi hasil yang didapatkan berdasarkan hasil yang telah dilakukan juga saran yang bertujuan agar penelitian dapat diimplementasikan untuk pengungkapan kasus kriminalitas dengan menggunakan *digital evidence* GPS berbasis *smartphone*.

BAB II

LANDASAN TEORI

2.1 *Digital Forensic*

Digital Forensic merupakan aplikasi *sains* atau ilmu pengetahuan yang digabungkan dengan teknologi komputer bertujuan untuk pemeriksaan dan melakukan analisis terhadap *electronics evidence* dan *digital evidence* untuk melihat hubungannya dengan tindak kriminalitas (Al Azhar, 2012). Menurut EC Council (2006), *Digital Forensic* adalah suatu aplikasi ilmu komputer yang bertujuan untuk pencarian kepastian hukum yang diperuntukkan bagi tindak kriminalitas (Al Azhar, 2012).

Menurut (Miller, 2006) definisi *digital forensic* : "Penggunaan metode yang diturunkan dan terbukti secara ilmiah untuk preservasi, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber digital untuk memfasilitasi rekonstruksi peristiwa atau membantu mengantisipasi tindakan ilegal yang terbukti menggangu prosedur yang direncanakan." Penggunaan metode secara ilmiah terhadap preservasi, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi yang berasal dari bukti digital untuk tujuan memfasilitas dan merekontruksi terhadap tindak kejahatan dan terhadap tindakan tidak sah terhadap suatu operasi yang telah direncanakan. (Miller, 2006).

Menurut Muh. Azhar seorang ahli *digital forensic*, *digital forensic* bertujuan untuk memeriksa dan menganalisa dari *electronic digital evidence* untuk memastikan antara *digital evidence* ada terkait dengan bukti yang lainnya, *digital forensic* merupakan penggabungan dari teknologi komputer dengan aplikasi *science.* Peran *digital forensic* dapat mengungkap keberadaan pelaku sehingga dapat dilakukan penangkapan oleh pihak Kepolisian (Al-Azhar, 2012).

Ahli *Digital Forensic* perlu memahami prinsip dasar yang tertera pada ACPO (*Association Of Chief Police Officiers*) merupakan Biro Hukum yang berada United Kingdom (UK) bidang penegakan hukum menyatakan bahwa prinsip-prinsip dasar sebagai berikut (Williams, 2012):

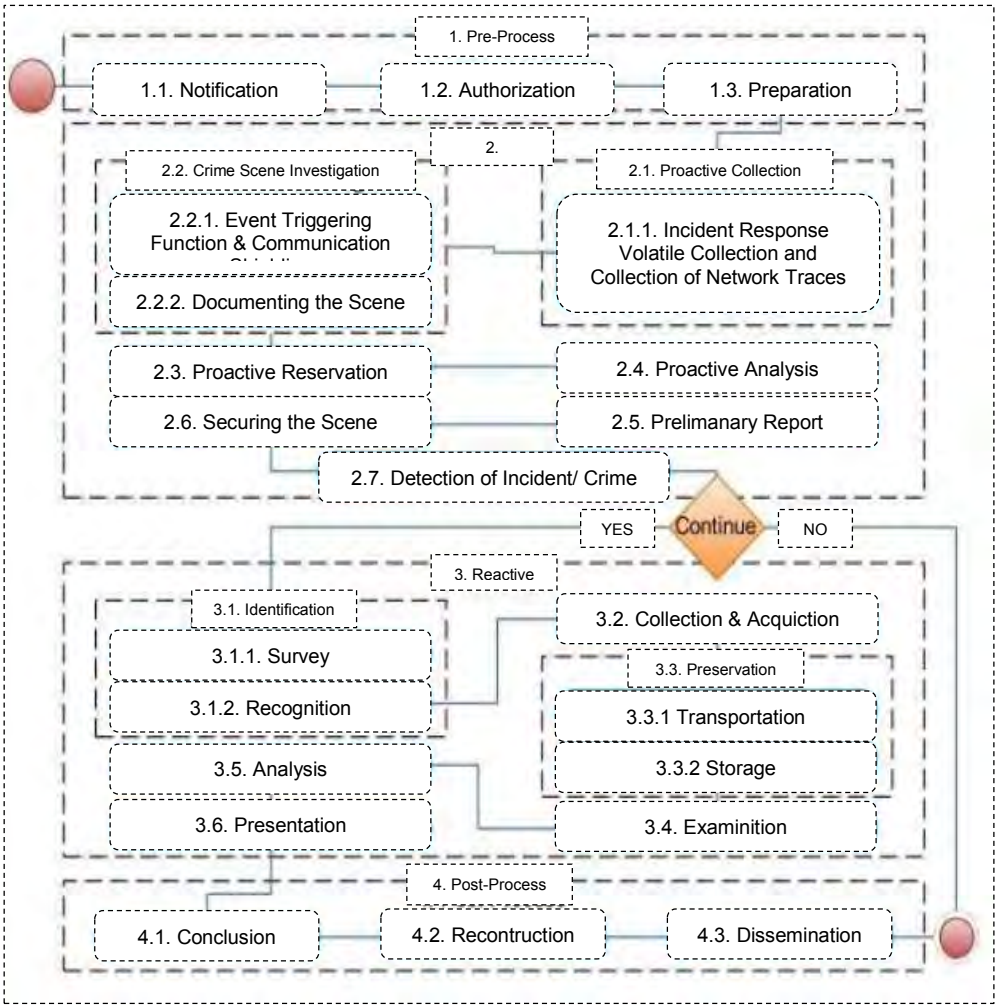
1. Tidak ada tindakan dari lembaga penegak hukum atau agen untuk mengubah data yang telah disimpan di *personal computer* atau *storage* yang selanjutnya dapat diandalkan di pengadilan;
2. Dalam keadaan apapun data asli dapat diakses oleh seseorang yang disimpan di *personal computer* atau *storage*, pengguna harus ahli terkait dalam memberikan bukti yang dapat menjelaskan implikasi dan hubungan dari tindakan yang dilakukan;
3. Penerapan jejak audit atau catatan proses pada *electronic evidence* berbasis *personal computer* dibuat dan dipelihara atau dirawat. Pihak ketiga yang independen harus dapat memeriksa proses-proses tersebut dan mencapai hasil yang sama;
4. Orang yang bertanggung jawab atas penyelidikan (petugas kasus) bertanggungjawab sepenuhnya untuk meninjau bahwa hukum dan kaidah penyelidikan ditaati.

Empat prinsip dapat disimpulkan bahwa Lembaga atau Penegak Hukum dilarang merubah data digital yang nantinya akan dipertanggungjawabkan di pengadilan, bahwa seseorang yang mempunyai kewenangan terhadap barang bukti digital dipastikan kompetensinya dan dapat menjelaskan tindakan serta analisis terhadap barang bukti digital.

Beberapa catatan teknis terhadap langkah-langkah yang telah di lakukan ini untuk menjaga bila pihak ketiga mengakses barang bukti digital akan memperoleh hasil yang sama dan yang terakhir adalah seseorang yang telah melakukan pemeriksaan barang bukti dapat meyakinkan terkait tahapan yang dilakukan berdasarkan hukum yang berlaku sesuai prinsip-prinsip dasar dan dapat dipresentasikan dengan baik.

2.2 *Integrated Digital Forensic Investigation Framework* (DFIF)

Metode IDFIF adalah metode yang dikembangkan dari sekuensial lojik di proses utama yang terdapat di DFIF. Metode DFIF terbagi menjadi beberapa tahapan yaitu Pre-Proses, Proaktif, Reaktif, dan Post-Proses. Tahapan Pre-Proses mencakup Notifikasi, Autorisasi, Persiapan. Tahapan Proaktif terdiri dari beberapa sub-tahapan yaitu : Proaktif Pengumpulan, Investigasi Area Kejahatan, Proaktif Preservasi, Proaktif Analisa, Laporan Preliminary, Mengamankan Area, Deteksi Insiden / Kejahatan. Tahapan Reaktif adalah tahapan yang mencakup Identifikasi, Pengumpulan dan akusisi, Preservasi, Examinasi, Analisa dan Presentasi. Tahapan Post-Process adalah tahapan yang mencakup Kesimpulan, Rekonstruksi, Diseminasi (Rahayu, 2014).



Gambar 2.1 Model Investigasi IDFIF
(Rahayu, 2014)

2.3 Investigasi Forensika

Perkembangan bidang *science* mengalami kemajuan dan disesuaikan dengan kemajuan teknologi, untuk cabang ilmu forensik yang ada pada saat ini merupakan bidang ilmu yang sedang berkembang dan berhubungan erat dengan teknologi informasi (IT). Forensika merupakan proses yang dilakukan secara ilmiah dengan tujuan untuk mengumpulkan, analisis, juga menghadirkan beragam barang bukti yang digunakan didalam sidang pengadilan yang terkait suatu kasus hukum.

Forensika atau Bidang Forensika juga mengalami perkembangan terhadap teknologi komputer, Forensika Komputer merupakan proses *identification*, *Preservation*, *Analysis,* dan *using the digital evidence* menurut hukum yang berlaku. Komputer Forensik mempunyai ruang lingkup yang merupakan aktivitas terkait dengan identifikasi, pengambilan, penyaringan, pemeliharaan dan dokumentasi *evidence* komputer didalam kejahatan komputer. Tahapan tersebut dapat dilakukan analisis juga penyelidikan untuk menentukan *evidence* dengan status legal.

2.3.1 *Systematic Digital Forensic Investigation Model*

Menurut Agarwal, 2011, bahwa tahapan investigasi memerlukan pengembangan dari berkembangnya setiap kasus yang terjadi. Studi yang dilakukan untuk beberapa *investigation model* yang telah dilakukan oleh para pakar. Sebagai contohnya yaitu *investigation model* dari DFRWS (*Digital Forensic Reasearch Workshop*), pengembangan model DFRWS setelah itu diusulkan *digital forensic investigation model* baru yang disebut dengan *Systematic Digital Forensic Investigation Model* (SRDFIM). Dalam model yang telah ditemukan oleh para pakar, ada beberapa tahapan dalam proses *investigartion forensic* yaitu :

1. *Preparation*

Tahapan *Preparation* adalah tahapan yang dilakukan sebelum proses penyelidikan sebuah kasus dilakukan Kegiatan yang dilakukan seperti pembuatan ijin, dokumen-dokumen dan administrasi lainnya.

2. *Securing The Scene*

Tahapan ini bertujuan untuk mengamankan TKP, sehingga dapat menghindari terjadinya kontaminasi lokasi Tempat Kejadian Perkara.

3. *Survey and Recognition*

Tahapan ini bertujuan untuk mencari bukti awal. wawancara dengan saksi mata dilakukan pada tahapan ini, mengidentifikasi kejadian dan hal lain yang berkaitan dengan proses investigasi bukti awal.

4. *Documenting of Scene*

Tahapan *Documenting of Scene* bertujuan untuk mendokumentasi setiap kejadian, *image* lokasi TKP dan di ilmu *forensic* dikenal sebagai *chain of custody.*

5. *Communication Shielding*

Tahapan ini merupakan cara untuk mencegah komunikasi dari *physical evidence* pada pihak eksternal. Betujuan agar bukti tidak berubah kondisinya atau kehilangan daya.

6. *Evidence Collection*

Tahapan ini bertujuan untuk pencarian *physical evidence* sesuai dengan bukti awal yang telah didapatkan. Beberapa jenis bukti merupakan *volatile evidence* dan bukti yang *non-volatile evidence*.

7. *Preservation*

Tahapan *preservation* yaitu barang bukti dijaga dan diamankan sesuai prosedur. Proses preservation terdiri dari pengumpulan, penyimpanan dan hingga sampai ke laboratorium *forensic*.

8. *Examination*

Tahapan ini merupakan tahapan pemeriksaan *physical evidence* yang telah didapatkan dan dilakukan di laboratorium *forensic*.

9. *Analysis*

Tahapan ini bertujuan untuk mencari keterkaitan dari *physical evidence* yang ditemukan dengan kasus yang terjadi, Berhubungan antara keterkaitan *evidence* yang mengarahkan kepada salah satu tersangka atau terdapat temuan tersembunyi yang dapat memutar balikkan tuduhan awal sebuah kasus.

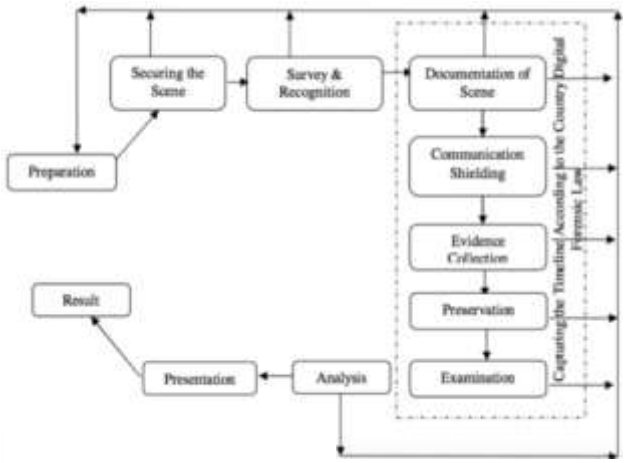
10. *Presentation*

Tahapan ini merupakan tahapan untuk melakukan penyajian laporan sesuai dengan barang bukti dan hasil analisa yang sudah dilakukan. Hasil *reporting* akan digunakan pada pengadilan. Sehingga dapat memperkuat *reporting* dan bersamaan dengan kehadiran saksi ahli untuk mengurai dan mempresentasikan hasil analisa dan pemeriksaan *physical evidence*.

11. *Result and Review*

Tahapan ini merupakan tahapan finasilsasi dari rangkaian proses investigasi. Hal ini diperlukan untuk mengambil kesimpulan yang didapatkan dari hasil analisa dan pemeriksaan. Selain itu melakukan *check* terakhir pada laporan yang dibuat.

Secara umum, SRDFIM lebih memperjelas dan proses forensik yang dikembangkan dari DFRW sehingga didapatkan model yang dapat mengakomodasi keseluruhan proses investigasi dari forensik digital, dan gambar 2.2 menjelaskan alur dari SRDFIM yang dikembangkan oleh Agarwal & Gupta, 2011.



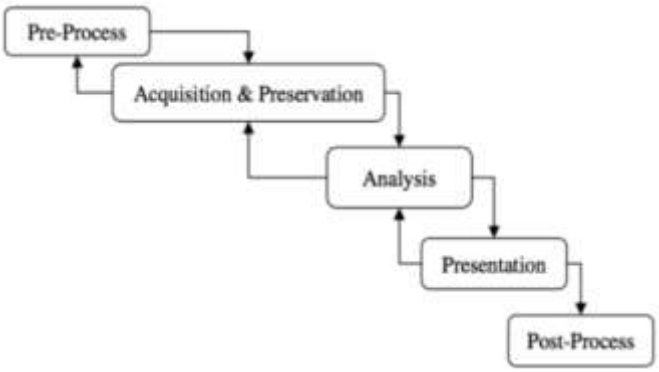
Gambar 2.2 Model Investigasi SRDFIM
(Agarwal, 2011)

2.3.2 Tahapan Umum *Computer Forensic Investigation Model*

Berbeda dengan metode *forensic* yang ditemukan oleh Agarwal, 2011. Yusoff, 2011 lebih mengutamakan sebuah metode yang dapat digunakan pada investigasi forensik. Yusoff, 2011 berpendapat bahwa semua metode forensik ujung-ujungnya mengarah pada satu titik inti yang menggambarkan keseluruhan model investigasi forensik. Menurut Yusoff, 2011 *investigation process* terdiri dari :

1. Pra Proses (*Pre-process*)
2. Akuisisi dan Pemeliharaan (*Acquisition and Preservation*)
3. Analisa (*Analysis*)
4. Penyajian (*Presentation*)
5. Pasca Proses (*Post-Process*)

Generic Computer Forensic Investigation Model (GCFIM) yang diusulkan oleh Yusoff, 2011 dapat dilihat di gambar 2.3.

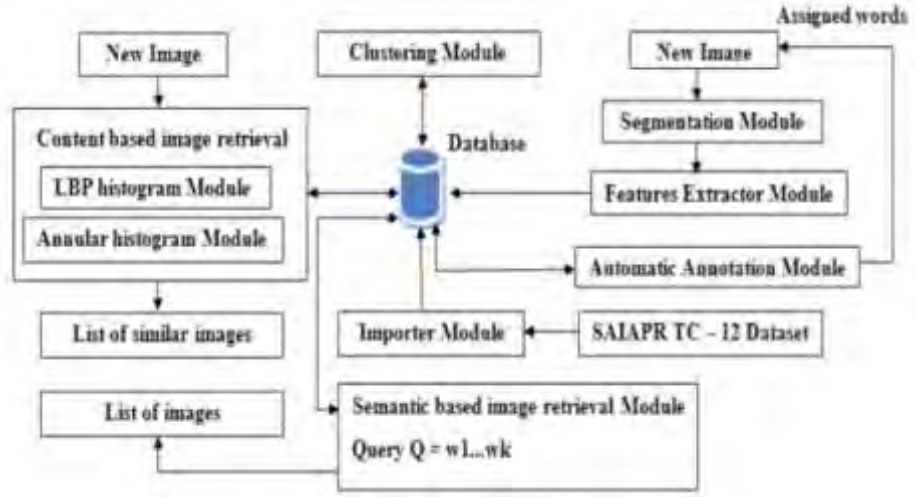


Gambar 2.3 *Generic Computer Forensic Investigation Model (GCFIM)*
(Yusoff, 2011)

Dari sisi makna, hampir sama untuk setiap model yang digunakan. Tetapi yang menjadi daya tarik adalah 4 tahapan di awal dapat berulang layaknya SDLC pada *waterfall.* Hal ini karena tidak menutup kemungkinan akan ditemukannya bukti baru. Sedangkan bagian akhir di pasca proses tidak dapat kembali lagi. Karena tahapan ini adalah tahapan pengembalian atau penghancuran *physical evidence.*

2.3.3 Model Investigasi Forensik

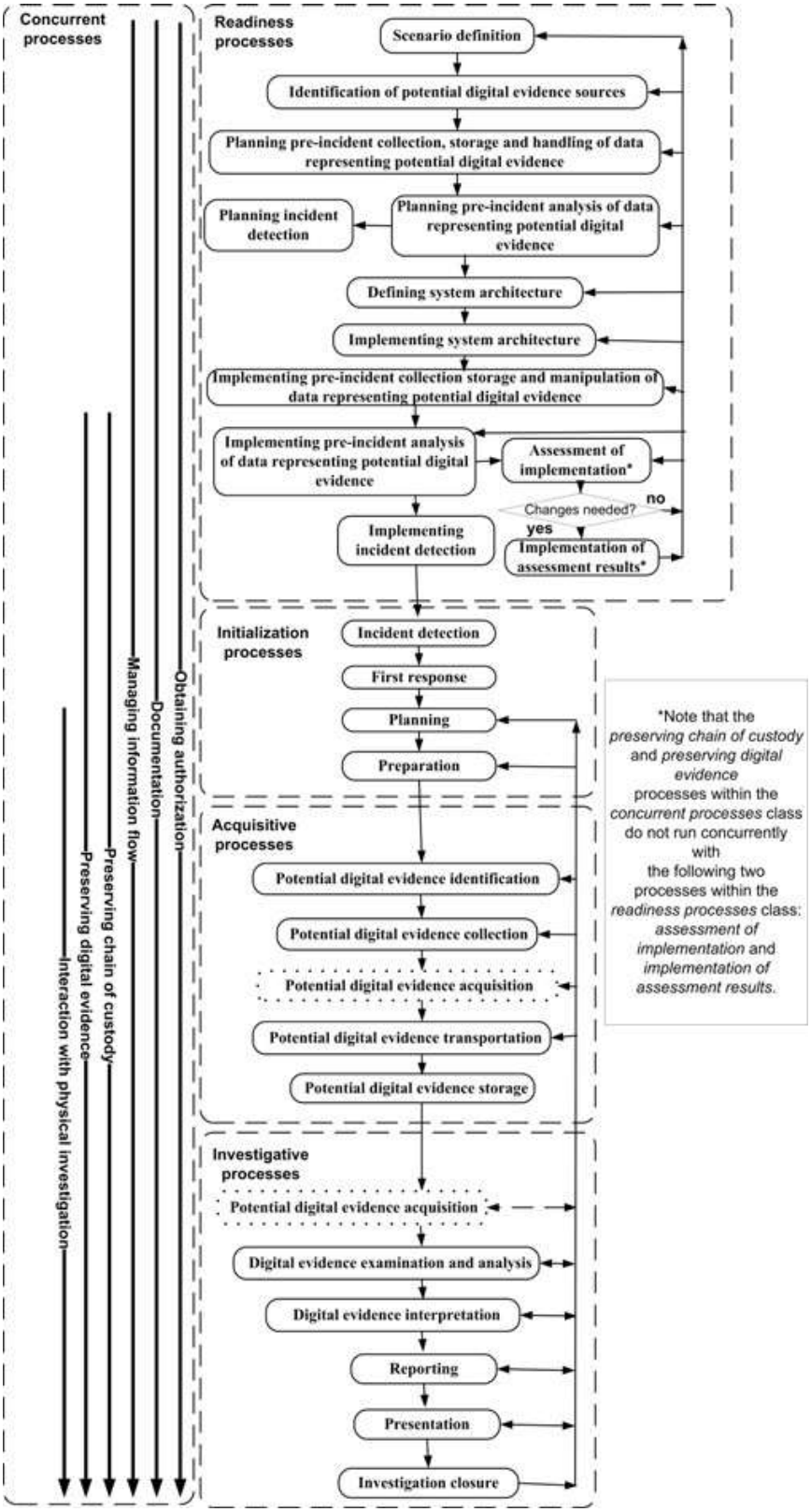
Investigation Model yang dikemukakan oleh Dieko, 2014 mengusulkan untuk menerapkan *clustering* untuk dokumen dan *evidence* yang tidak terstruktur untuk dikelompokkan yang secara otomatis terbentuk menjadi grup-grup. Sesuai dengan arsitektur yang diusulkan, dapat dijelaskan bahwa sistem yang digunakan adalah *Cross Media Relevance Model* (CWRM) menggunakan keterangan dalam sebuah *images,* sistem bekerja otomatis untuk mengenali sesuatu melalui untaian kata-kata. Kumpulan *cluster* pada wilayah *image* yang diperoleh menggunakan algoritma K-*means*, setiap *image* dari sebuah *set* di terjemahkan dengan menggunakan urutan diskrit dari kumpulan identitas. Pada *distribution process* menggunakan cara untuk melakukan *generate* kata-kata setiap *image* baru..



Gambar 2.4 *Cross Media Relevance Model* (CWRM)
(Dieko, 2014)

2.3.4 Proses Standart Investigasi Forensik Digital

Valjarevic, 2014 mengusulkan sebuah prototipe untuk membantu membimbing dan melaksanakan proses investigasi forensik yang standart, prototipe yang diusulkan oleh Valjarevic, 2014 tertera pada gambar 2.5.



Gambar 2.5 Proses Standart Investigasi Forensik Digital (Valjarevic, 2014)

2.4 *Mobile Forensic*

Cabang dari forensika digital yaitu *Mobile Forensics* terkait *digital evidence recovery* dari sebuah *smartphone*, Perangkat selular dapat berupa *smartphone* tetapi dapat dihubungkan dengan *digital device* yang memiliki memori *internal* dan kemampuan komunikasi. *Mobile device forensics* adalah ilmu yang dapat digunakan untuk proses *digital evidence recovery* dari *mobile device* menggunakan cara *forensic* (Jansen, 2007). *Mobile Forensic Device* merupakan *forensic* yang datanya diambil dari ponsel, dengan sendirinya dapat dijadikan sebagai bukti.

Bukti-bukti ini dapat menjadi acuan pada saat penyelidikan perkara oleh lembaga penegak hukum, pengembang *forensic tool* menggunakan metode yang berbeda untuk *gaining access* memori pada device (McCharthy, 2005).

International Organization of Computer Evidence (IOCE) menyatakan bahwa bukti digital adalah informasi yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan di pengadilan (Turnbull, 2000) juga menegaskan bahwa *digital evidence* dapat memastikan kejahatan telah dilakukan, dapat memberikan *relation* antara kriminalitas dan *victim* atau dapat menyediakan *link* antara kejahatan dan pelakunya. Empat *forensic key*, yaitu (Rahmadi, 2003):

1. *Identification from Digital Evicence*

Merupakan tahap paling awal *forensic* dalam teknologi informasi. Tahapan ini melakukan proses identifikasi ketika bukti itu ditemukan, *evidence* tersebut disimpan dan bagaimana cara penyimpanannya untuk mempermudah ke tahapan selanjutnya.

2. *Digital Evidence Storage*

Termasuk tahapan yang paling krusial dalam *forensic*, karena *digital evidence* pada tahapan ini dapat saja hilang karena penyimpanannya yang kurang baik.

3. *Digital Evidence Analysis*

Pengambilan, pemrosesan dan *interpretation* dari *digital evidence* adalah bagian penting untuk menganalisa *digital evidence.*

4. Presentasi bukti digital

Proses persidangan *digital evidence* diuji *authentication* dan keterkaitan dengan kasus yang ada. Tahapan yang harus dilakukan oleh investigator untuk melindungi *physical evidence* adalah *the chain of custody*. Istilah tersebut mengandung arti bahwa pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Tujuan dari *the chain of custody* adalah :

a. *Evidence* itu masih asli.
b. *Evidence* masih dapat dikatakan sama saat ditemukan pada saat persidangan. (jarak yang terjadi dari penyidikan ke persidangan relatif lama).

2.5 Barang Bukti

Barang bukti adalah hal penting untuk kasus kriminalitas, bersumber dari *hysical evidence* yang didapatkan, Tim Investigasi dan Analisis *Forensic* dapat melakukan pengungkapan kasus dengan urutan kronologis yang lengkap. Menurut Al-azhar (2012), barang bukti diklasifikasikan menjadi 2 bagian:

1. Barang bukti elektronik
2. Barang bukti digital

Menurut SWGDE yang merupakan kelompok kerja ilmiah Bukti Digital (2015), Bukti Digital adalah informasi nilai pembuktian yang disimpan atau ditransmisikan dalam bentuk biner. Berdasarkan definisi tersebut, *digital evidence* termasuk bukti pada perangkat digital apapun seperti *portable media player*, kamera digital atau perangkat telekomunikasi dan bukan hanya terbatas pada yang ditemukan di komputer. Selain itu, *digital evidence* dapat ditemukan dan digunakan sebagai bukti dan tidak dibatasi hanya untuk komputer seperti tindakan *hacking.* Terdapat 5 kriteria yang wajib dimiliki dari sifat bukti, yaitu: Keaslian, Keandalan, Kelengkapan, Kepercayaan dan dapat diterima.

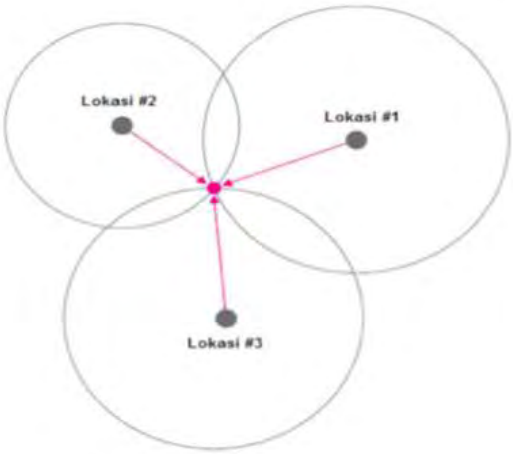
2.6 *Global Positioning System*

GPS adalah sistem yang dapat digunakan oleh pengguna di laut, darat dan udara secara *realtime* 24 jam di seluruh dunia, tanpa dibatasi oleh faktor cuaca. Bertujuan untuk menentukan titik koordinat 3D (tiga dimensi), dan juga memantau kecepatan GPS pada prinsipnya terdapat 3 bagian yaitu.

1. Segmen Luar Angkasa
2. Segmen Pengendali
3. Segmen Pengguna

GPS (*Global Positioning System*) merupakan system berbasiskan satelit yang terhubung berada di sebuah orbit yang berfungsi sebagai system navigasi. *Departement of Defense* Amerika Serikat yang pertama diperkenalkan tahun 1978, pada tahun1994 menggunakan 24 satelit. Fungsi dari *GPS reciever* yaitu menerima sinyal yang dikirim dari satelit *Global Positioning System* dan bertujuan untuk melacak koordinat dari posisi seseorang. *Way-point* merupakan koordinat dari posisi yang telah dilakukan pengubahan menjadi titik yang selanjutnya menjadi titik-titik koordinat lintang dan bujur yang merupakan letak seseorang atau lokasi.

GPS menggunakan kumpulan satelit yang mengorbit bumi sebanyak 27 satelit, Satelit tersebut mengirimkan informasi kepada *Global Positioning System receiver* yang bertugas untuk menerima informasi yang berasal dari tiga atau lebih satelit. Gambar 2.6, merupakan trileterasi dalam GPS untuk menentukan posisi. Penentuan posisi mengharuskan *GPS receiver* dan ketiga satelit tersebut dalam *line-of sight* (LoS), sehingga *outdoor positioning* merupakan posisi ideal untuk penggunaan GPS. Aplikasi yang terdapat di perangkat target atau *client* setelah mendapatkan *request* dari pelacak atau *server*, setelah itu *client* akan melakukan *request* koordinat posisinya pada *Global Positioning System* dan selanjutnya akan dikirimkan ke pelacak atau *server*.



Gambar 2.6 Trilaterasi dalam Global Positioning System (GPS)
(Ary Mazharuddin S, S.Kom., M.Kom.Sc., Surabaya, Januari:2011)

Pada tahun 1980, GPS digunakan untuk keperluan militer mulai terbuka untuk publik. Meskipun satelit-satelit tersebut diperkirakan senilai ratusan juta USD, tetapi dapat digunakan secara gratis oleh setiap orang. Satelit-satelit ini mengorbit di ketinggian sekitar 12.000 mil dari permukaan bumi, dan posisi ini sangat ideal karena dapat menjangkau area *coverage* yang lebih luas. Satelit-satelit yang telah mengorbit akan selalu berada diposisi yang dapat menjangkau area *coverage* di atas permukaan bumi sehingga meminimalkan terjadinya *blank spot* atau zona yang tidak terjangkau oleh satelit.

Waktu yang diperlukan oleh satelit untuk mengelilingi bumi adalah 12 jam, dan sangat cepat sehingga selalu dapat menjangkau posisi di atas permukaan bumi. GPS *reciever* terdiri dari beberapa *integrated circuit* (IC). GPS dapat digunakan untuk berbagai keperluan, misalnya kendaraan (pesawat terbang, mobil, kapal), dan untuk pertanian yang di integrasikan dengan komputer maupun laptop. (Sunyoto, 2013:). Berikut beberapa contoh perangkat GPS *reciever*:

Gambar 2.7 Perangkat GPS
(Sunyoto, 2013)

2.6.1 Cara Kerja *Global Positioning System* (GPS)

Jangkauan zona dapat terjangkau oleh 3 sampai 4 satelit, 12 *chanel* satelit dapat diterima oleh setiap GPS sekaligus. Kondisi pemandangan yang cerah dan tanpa halangan membuat GPS dengan mudah untuk menerima sinyal yang dikirimkan oleh satelit. Tingkat akurasi GPS dipengaruhi oleh jumlah satelit yang diterima oleh GPS

Cara kerja GPS secara sederhana ada 5 langkah, yaitu :

1. Menggunakan "*triangulation*" yang bersumber dari satelit.
2. GPS melakukan pengukuran *travel time* sinyal radio untuk perhitungan "*trianggulation*".
3. GPS memerlukan tingkat akurasi waktu yang tinggi untuk pengukuran *travel time*.
4. Posisi satelit dan ketinggian orbitnya diperlukan untuk penghitungan jarak.
5. *Delay* sinyal *travel time* di atmosfer dilakukan koreksin hingga diterima *reciever*.

Gambar 2.8 Cara Satelit Menentukan Posisi
(Sunyoto, 2013)

Satelit GPS berputar mengelilingi bumi selama 12 jam di dalam orbit yang akurat dan mengirimkan sinyal informasi ke bumi. Penghitungan "*triangulation*" yang menghitung *user location* dengan akurat dilakukan untuk pengambilan informasi yang dilakukan oleh GPS *reciever*. GPS *reciever* melakukan perbandingan *time signal* di kirim dengan *time signal* tersebut di terima. Berdasarkan informasi yang telah diperoleh, maka dapat diketahui berapa jarak satelit. Perhitungan dan menentukan posisi *user* dan menampilkan dalam peta elektronik dapat dilakukan dengan perhitungan jarak GPS *reciever*.

Gambar 2.9 Tampilan GPS Reciever
(Sunyoto, 2013)

2.6.2 Cara Satelit Menetukan Posisi Lokasi

Menghitung *travel time* dilakukan berdasarkan lokasi sinyal yang dikirimkan oleh satelit ke GPS, dan dikenal sebagai *Time of Arrival* (TOA). Menurut prinsip fisika, bahwa waktu dikalikan dengan cepat rambat sinyal merupakan cara untuk mengukur jarak. Sehingga, prinsip fisika tersebut dapat digunakan untuk menemukan jarak antara satelit ke GPS. Satelit berisi informasi yang sangat detail (waktu, orbit satelit, hambatan di atmosfir) yang akan dikirimkan oleh satelit dalam bentuk sinyal. (Sunyoto, 2013).

Satuan waktu yang paling akurat yang digunakan satelit adalah jam atom. Tiga satelit minimal dibutuhkan untuk dapat melakukan penentuan posisi dari sebuah GPS dalam bentuk 2 dimensi (jarak). Empat buah satelit minimal dibutuhkan untuk dapat melakukan penentuan lokasi ketinggian dari sebuah GPS dalam bentuk 3 dimensi. GPS receiver bertugas untuk menerima sinyal yang dipancarkan oleh setiap satelit. (Sunyoto, 2013).

Jari-jari lingkaran dari jangkauan masing-masing satelit didapatkan dari sinyal yang kemudian dihitung jarak dari masing-masing satelit ke GPS. Penentuan lokasi dari GPS di permukaan bumi didapatkan dari perpotongan setiap lingkaran jangkauan satelit dan juga didapatkan dari perhitungan matematis yang rumit. (Sunyoto, 2013).

2.7 *Digital Evidence*

Pasal 5 undang-undang No.11 Tahun 2008 Tentang Informasi dan Trasaksi Eletronik Ayat 1 berbunyi, Informasi dan Eletronik dan/atau Dokumen eletronik dan/atau hasil cetakan merupakan alat bukti hukum yang sah. Dijelaskan di Ayat 2 Pasal 5 UUD No. 11 Tahun 2008 Bahwa informasi eletronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Ayat 3 Pasal 5 UUD No. 11 Tahun 2008 menjelaskan bahwa

Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. Ayat 4 Pasal 5 UUD No.11 Tahun 2008 Tentang ITE Hal tersebut diperkuat Pasal 44 Huruf B UUD No.11 Tahun 2008 Tentang ITE bahwa informasi eletronik dan dokumen eletronik merupakan alat bukti lain, selain alat bukti yang dimaksud dalam ketentuan perundang–undangan.

GPS *evidence* merupakan *digital evidence* yang menentukan lokasi *geografis* dengan akurasi yang telah teruji. Lokasi geografis yang didapatkan akan langsung ke salah satu lokasi pengguna *smartphone* sehingga dapat untuk ditemukan, begitupun dengan *user* tertentu yang dicari dalam suatu kasus kejahatan. Bukti GPS berupa *data latitude* dan *data longitude*.

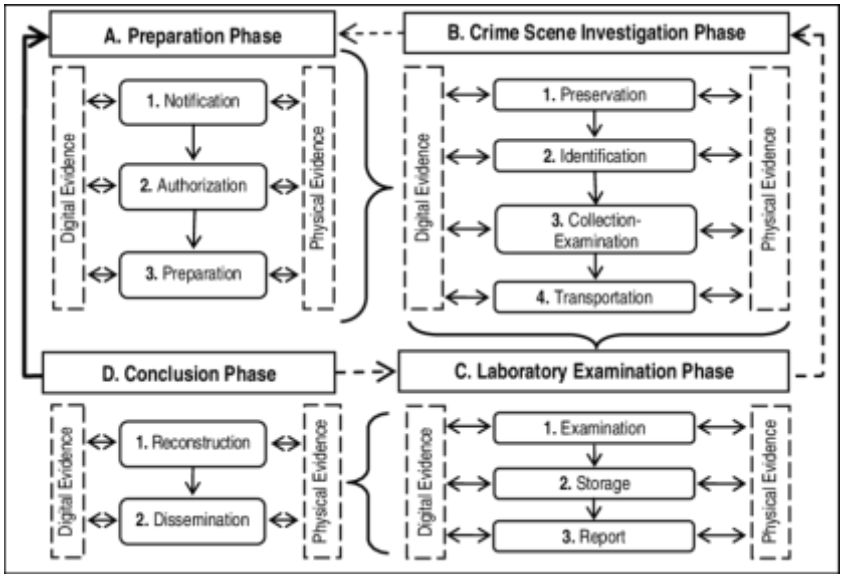
2.8 *Hybrid Evidence Investigation*

Hybrid Evidence mengacu pada bukti fisik dan bukti digital, menambahkan kemungkinan bukti fisik tersebut dapat memiliki *hidden digital evidence,* karakteristik harus dikondisikan dalam penyelidikan kasus kriminalitas. Sebagai contoh, *Ballpoint* yang kamera mikro ataupun mikrofon yang digunakan untuk merekam video dan suara, contoh lainnya yaitu selembar kertas yang memiliki *chip* RFID yang berisi informasi pelacakan. *Hybrid model* dapat digunakan dalam penyelidikan, yang hanya menggunakan bukti fisik atau *digital evidence* yang tersedia.

Model *Hybrid Evidence Investigation* terdapat 4 tahapan utama dan 12 tahapan sekunder, yaitu: *Preparation* → *Crime Scene Investigation* → *Laboratory Examination* → *Conclusion* atau dikenal dengan istilah HEI.

1. Tahap *Preparation* = (*Notification* → *Authorization* → *Preparation*).
2. Tahap *Crime Scene Investigation* = (*Preservation* → *Identification* → *Collection Examination* → *Transportation*).
3. Tahap *Laboratory Examination* = (*Examination* → *Storage* → *Report*).
4. Tahap *Conclusion* = (*Reconstruction* → *Dissemination*).

Gambar 2.10 adalah model hybrid evidence investigation yang digunakan sebagai acuan untuk melakukan penyidikan dari suatu kasus kriminalitas.



Gambar 2.10
Model *Hybrid Evidence Investigation*
(K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, 2012)

Tahapan utama yang terdiri dari 4 tahapan memiliki fungsi dan tujuan, yaitu:

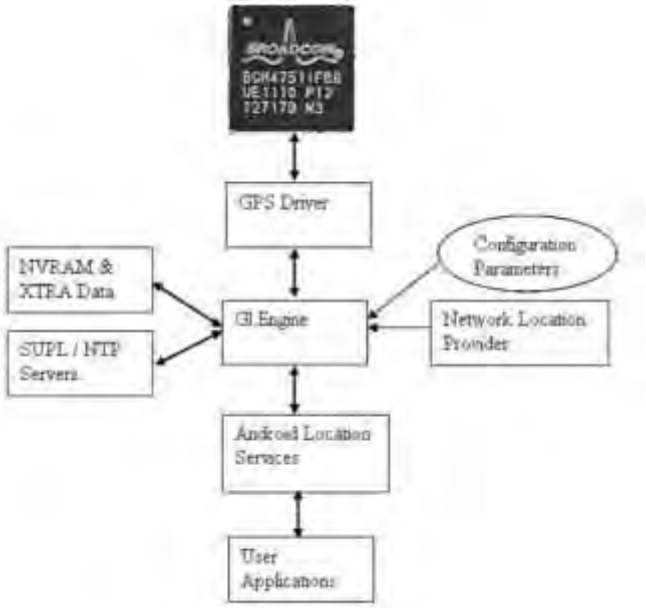
a. Tahap *Preparation* merupakan tahapan persiapan dari sebuah investigasi yang terkait dengan hak akses dan tool atau perangkat yang akan digunakan.
b. Tahap *Crime Scene Investigation* merupakan tahapan dari tindakan oleh TKP dengan tujuan untuk menggali fakta yang terdapat di TKP.
c. Tahap *Laboratory Examination* merupakan tahapan yang melakukan proses dari penggalian fakta terkait pada barang bukti yang didapatkan dari olah TKP.
d. Tahap *Conclusion* merupakan tahapan dokumentasi dan evaluasi yang dilakukan setelah seluruh tahap atau proses investigasi yang telah dilakukan oleh Tim Penyidik atau Tim Analis *Forensic*.

2.9 Teknologi GPS dan A-GPS pada *Smartphone*

Posisi tanpa halangan, GPS receiver dan satelit merupakan tiga komponen untuk proses dalam penentuan posisi melalui GPS. Bertujuan agar perangkat GPS dapat menerima sinyal dengan maksimal, perangkat harus berada di *outdoor*, dan juga tanpa halangan. Jika perangkat berada bawah gedung, dibawah pohon atau didalam kendaraan,

dapat menyebabkan penurunan dari kekuatan sinyal. Sinyal hampir dapat dipastikan menghilang kalau perangkat GPS masuk ke dalam gedung (Tohid, 2012).

A-GPS dikembangkan untuk meningkatkan kinerja GPS. *Server* bantuan akan memberikan informasi pendukung ke *device* yang dapat membantu dalam perhitungan lokasi. *Server* bantuan sebagai penyedia data informasi satelit yang dibutuhkan oleh A-GPS didukung oleh jaringan operator dikarenakan tower BTS memiliki unit GPS *receiver* dan secara *non-stop* akan men*download* data informasi data satelit dan kemudian memprosesnya (Tohid, 2012). Gambar 2.11 adalah gambar komponen-komponen yang ada pada GPS android.



Gambar 2.11
Arsitektur Chip GPS Pada Android
(Arsitektur Chip GPS pada Android. 2013)

2.10 Mengukur Posisi Geografis

Smartphone yang didukung dengan teknologi GPS, A-GPS dan WLAN, maka dapat dipastikan letak posisi cukup akurat. Jika A-GPS, maka geodata akan dikirimkan ke *smartphone* dengan sistem lintang atau bujur koordinat yang menampilkan lokasi dalam derajat dari 180° BB hingga 180° timur sepanjang khatulistiwa dan 90° utara melalui 90° selatan sepanjang meridian utama. [-] dd, [-] hh merupakan format deskripsi dalam derajat desimal untuk sebelah selatan dan sebelah barat dengan angka negatif. (Paseban, 2013).

Tabel 2.1
Akurasi Sistem *Positioning* Pada *Smartphone*

Positioning Method	***Accuracy***
GPS	± 8m
Assited GPS (aGPS)	5-50 m
Cell-id	100 – 3000 m
GSM Cell Tower Triangulation	± 25 m
WLAN Positioning System	20– 30 m

2.11 *Data Latitude* dan *Data Longtitude*

Latitude atau lintang (garis horizontal) merupakan *distance* dari sudut, dengan bentuk *degree, minute*, dan *second* dari titik utara atau selatan dari Khatulistiwa. Sedangkan *longitude* atau bujur (garis vertikal) merupakan *distance* dari sudut, dengan bentuk derajat, menit, dan detik, dari titik timur atau barat Meridian. Data dua format data *latitude* dan *longitude*, yaitu *Decimal format* dan *Degrees Minutes Seconds format*. Contoh, untuk data Longlat lokasi tertentu adalah: -6.191067, 106.829607. *Decimal Formated* : -6.191067, 106.829607. Jika di konversi ke *Degrees Minutes Seconds Formated* menjadi: -6° 11′ 27.8412″, 106° 49′ 46.5846″.

Format *Degrees Minutes Seconds* adalah, angka sebelum . (titik) yang diartikan sebagai *degrees* atau derajat. Nilai Negatif yang berarti *South* atau *latitudes* dan *West* atau *longitudes* sedangkan nilai positif berarti arah sebaliknya. Bertujuan untuk mendapatkan presisi, derajat bujur dan lintang telah dibagi menjadi *minute* (‘) dan *second* (“) Ada 60 *minute* dalam setiap *degree*. Setiap *minute* dibagi menjadi 60 detik. Maka itu, akan selalu

lebih kecil dari 60. Setiap detik dibagi lagi menjadi sepersepuluh, seperseratus, atau bahkan seperseribu.

Format *Decimal* lebih kompleks, terutama untuk angka setelah titik. Angka depan sebelum titik sama artinya *degrees*/derajat. Nilai Negatif berarti *South* (*latitudes*) atau *West* (*longitudes*) sedangkan nilai positif berarti arah sebaliknya. Sebaiknya dikonversi terlebih dahulu data *Latitude Longitude* ke dalam format *Degrees Minutes Seconds Formated* (GPS Tracker, 2013).

Gambar 2.12
Garis Lintang Dan Bujur
(GPS Tracker, 2013)

2.12 Relevansi Data untuk *Digital Forensic*

Peningkatan selama dua tahun terakhir dari jumlah *smartphone* menyebabkan perkembangan aplikasi yang membutuhkan informasi *location* dari pengguna perangkat tersebut. Untuk *platform smartphone* android yang ditargetkan sebuah penelitian terbaru dari hampir 50.000 aplikasi menunjukkan bahwa 25% dari aplikasi membutuhkan akses ke informasi *location*. 15% dari aplikasi mempunyai fitur yang dapat memberikan informasi posisi dari pengguna perangkat. (Stefan, 2011).

1. *Smartphone* muncul dengan dilengkapi *map* atau *navigation system.*
2. *Smartphone* juga memiliki *built-in* kamera. Bagian dari metadata gambar dari hasil kamera *smartphone* diperoleh jika *geo-tagging* diaktifkan.
3. Aplikasi dengan fitur *location based* menjadi sangat populer. *Foursquare*, aplikasi untuk menjelajahi kota dan berbagi lokasi, memiliki 6,5 juta pemakai di bulanFebruari 2011.

Facebook, berbasis lokasi layanan *places* pada bulan Agustus 2010. Twitter juga menambahkan informasi lokasi sebagai *optional* untuk *tweets* sejak 2010 (Stefan, 2011).

2.13 Software X

Perangkat lunak (*software*) yang digunakan di penelitian ini menggunakan *software* yang berbeda disesuaikan dengan kebutuhan proses investigasi. Proses *acquisition data* menggunakan Sistem Operasi Linux khusus *forensic* sebagai *tools* untuk melakukan *acquisition data* dari *smartphone* pelaku kriminalitas.

Proses pemeriksaan *file*, penulis menggunakan *software* yang memiliki fitur untuk membaca nilai *hexadecimal* dari sebuah *file* dan juga memiliki fitur untuk membandingakan antara *hexadecimal* dari *file* asli dengan *hexadecimal* dari *file* yang telah dilakukan modifikasi.

Proses GPS *Extraction*, penulis menggunakan *software* yang memiliki fitur untuk melakukan ektraksi data dari *database* yang diambil langsung dari *smartphone* pelaku kriminalitas. *Software* yang digunakan untuk proses GPS *Extraction* juga memiliki fitur ekstraksi file dengan ekstensi .log, *software* yang digunakan juga memiliki fitur melakukan ekstraksi data *satellite* GPS yang tersimpan dalam *database* berada dalam direktori /root/GPS.log.

Proses GPS *Conversion*, penulis menggunakan *software* yang memiliki fitur untuk melakukan ekstraksi *file* gambar dan memiliki fitur untuk melakukan *conversion file* gambar yang di investigasi sehingga dapat menampilkan koordinat data *latitude* dan data *longtitude* GPS. Hasil conversion yang telah dilakukan menggunakan *software* dapat dijadikan sebagai *digital evidence* dan memastikan bahwa foto atau gambar yang telah dilakukan investigasi merupakan foto atau gambar yang diambil langsung menggunakan kamera yang ada di *smartphone* pelaku kriminalitas dan bukan dari kiriman seseorang atau *download* dari media internet.

Proses *reporting* atau GPS Presentation, penulis menggunakan Google Map untuk melakukan pelacakan lokasi yang bersumber dari data *latitude* dan data *longtitude* GPS yang telah didapatkan dari *acquisition data*, proses pemeriksaan, proses GPS *Extraction* dan proses GPS *Conversion.* Data *latitude* dan data *longtitude* GPS di inputkan kedalam *textbox* yang ada di Google Map untuk dilakukan pencarian lokasi.

Software X yang digunakan dari *acquisition data*, proses pemeriksaan, proses GPS *Extraction* dan proses GPS *Conversion* memiliki spesifikasi minimum untuk menjalankan sistem operasi Linux *Forensic* dan Microsoft Windows yaitu dengan menggunakan perangkat komputer dengan RAM 512 MB, Processor 700MHz, Resolusi Layar 1024x768 dan *Disk Space* 5GB.

2.14 Penelitian terdahulu

Penelitian terdahulu ini sebagai referensi penulis untuk melakukan penelitian sehingga penulis dapat memperdalam teori yang digunakan untuk mengkaji penelitian yang akan dilakukan. Berdasarkan penelitian terdahulu, penulis tidak menemukan penelitian dengan judul yang sama seperti judul penelitian penulis. Namun penulis telah mengambil beberapa penelitian sebagai referensi dalam memperdalam bahan kajian pada penelitian penulis. Tabel 2.2 merupakan penelitian terdahulu berupa beberapa jurnal terkait dengan penelitian yang dilakukan penulis.

Tabel 2.2
Penelitian Terdahulu
(Hasil Kajian Penulis, 2020)

Nama Peneliti	Judul Penelitian	Hasil Penelitian	Perbedaan
Ankit Agarwal, Megha Gupta, Saurabh Gupta, Subhash Chandra Gupta, (2011).	*Systematic Digital Forensic Investigation Model*	Penelitian dimulai dengan diskusi tentang teknologi *digital forensic* kemudian diskusi beralih ke model investigasi *digital forensic*. Beberapa masalah mengenai penelitian *digital forensic* telah diidentifikasi dan dihasilkan Model investigasi *digital forensic* Sistematik	Penelitian yang dilakukan oleh Ankit Agarwal, Megha Gupta, Saurabh Gupta, Prof. (Dr.) Subhash Chandra Gupta hanya menghasilkan sebuah model investigasi *digital forensic* dan tidak melakukan *Tracking GPS* yang bersumber dari *smartphone* pelaku tindak kriminalitas.

Nama Peneliti	Judul Penelitian	Hasil Penelitian	Perbedaan
		beserta investigasi *digital forensic*.	
Anton Yudhana, Imam Riadi, Ikhwan Anshori, (2017).	*Analysis of Digital Evidence on Facebook Messenger Using the NIST Method*	Text percakapan, gambar dan audio yang telah didapatkan dari proses investigasi pada aplikasi *Facebook Messenger* dan hasil dari analisis dilaporkan sebagai barang bukti.	Penelitian yang dilakukan oleh Anton Yudhana, Imam Riadi, Ikhwan Anshori hanya melakukan investigasi text percakapan, gambar dan audio pada aplikasi *Facebook Messenger* saja dan tidak melakukan proses *Tracking* GPS dari *smartphone* yang digunakan oleh pelaku kriminalitas.
Muhammad Kukuh Tri Haryanto, Imam Riadi, Yudi Prayudi, (2018).	*Forensics Analysis of Sqlite Database on Android-Based IMO Applications*	Menemukan struktur folder dan isinya di aplikasi IMO, proses investigasi menunjukkan bahwa terdapat 6 folder didalam aplikasi IMO yaitu *lib, catche, database, files, no back_up, dan shared_pref* dari keenam folder tersebut hanya *folder catche* dan database yang memiliki *subfolder*. *Subfolder* tersebut berisi kumpulan file gambar dan video dari aktifitas pengguna aplikasi IMO.	Penelitian yang dilakukan oleh Muhammad Kukuh Tri, Imam Riadi, Yudi Prayudi Haryanto hanya berfokus ke pencarian direktori dari sebuah aplikasi yang kemudian dilakukan proses ekstraksi data yang terdapat didalam folder dan file yang telah didapatkan pada proses investigasi dan Penelitian *database SQlite* pada aplikasi IMO berbasis Android hanya menemukan *Log_video call.* Penelitian tersebut tidak melakukan *Tracking GPS* yang bersumber dari *smartphone* pelaku kriminalitas.
K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, (2012).	*A Model for Hybrid Evidence Investigation*	Bukti digital dan bukti fisik dapat diselidiki bersamaan, dan menjadi tantangan utama dalam penyelidikan. Selain itu, peneliti meninjau pilihan model investigasi untuk bukti fisik / digital, peneliti	Penelitan yang dilakukan oleh K. Vlachopoulos, E. Magkos and V. Chrissikopoulos tidak menggunakan *Smartphon*e dan *Tracking* GPS, penelitian tersebut hanya menghasilkan sebuah model pengabungan untuk

Nama Peneliti	Judul Penelitian	Hasil Penelitian	Perbedaan
		memperkenalkan istilah bukti *hybrid* dan mengusulkan model untuk investigasi bukti *hybrid*.	proses investigasi bukti fisik dan bukti digital.

Berdasarkan penelitian terdahulu yang tercantum pada Tabel 2.2, dapat dilihat bahwa belum ada penelitian di bidang *Digital Forensic* dan *Forensic Investigation*, yang membahas *Tracking GPS* dengan menggunakan *Hybrid Evidence Investigation*. Sehingga hasil penelitian ini dapat berkontribusi dalam hal Investigasi *Forensic* dengan metode *Hybrid Evidence Investigation.*

BAB III

OBJEK DAN METODOLOGI PENELITIAN

3.1 Penentuan Posisi GPS

Penggunaan GPS *System* yaitu untuk memberikan informasi mengenai kecepatan, posisi dan waktu secara *global* secara *realtime* tanpa ada batasan cuaca dan waktu. Pada tahun 1978, Satelit GPS pertama kali diluncurkan. Tahun 1994, GPS *System* dioperasikan. Tiga segmen utama yang ada di GPS *System* yaitu *space segment*, *control system segment*, dan *user segment* (Awaluddin, 2007).

1. *Space segment*

Space segment merupakan satelit GPS yang mengorbit di angkasa yang digunakan sebagai stasiun radio (Awaluddin, 2007). Satelit GPS dilengkapi dengan antena dengan tujuan untuk dapat *sending* dan *receive wave*. *Wave* dipancarkan ke bumi dan diterima oleh GPS *receiver* yang ada di bumi dan digunakan untuk penentuan informasi waktu, kecepatan dan posisi. Satelit GPS terdiri dari 24 satelit yang menempati 6 bidang orbit dengan periode orbit 10 jam 58 menit, pada ketinggian ± 20.200 km di atas permukaan bumi (*www.coremap.or.id*). Pada setiap waktu, paling sedikit 4 satelit dapat di amati di setiap lokasi di permukaan bumi. Hal ini memungkinkan pengguna GPS untuk dapat menghitung posisi di permukaan bumi.

2. *Control System Segment*,

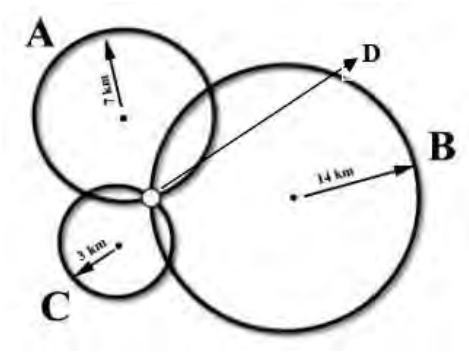
Control System Segment GPS adalah inti dari GPS (Awaluddin, 2007). Tugas dari *Control System Segment* yaitu mengatur semua satelit GPS yang ada agar berfungsi sebagaimana mestinya serta mengirimkan beberapa informasi seperti sinkronisasi waktu, prediksi orbit satelit, informasi cuaca di angkasa dan monitor kesehatan satelit. Pihak Amerika Serikat mengoperasikan sistem ini dari Sistem Kontrol Utama di *Falcon Air Force Base* di Colorado Springs, Amerika Serikat. Segmen sistem kontrol ini juga termasuk 4 stasiun monitor yang berlokasi menyebar di seluruh dunia.

3. *User Segment*

User Segment adalah user dari satelit GPS, GPS *receiver* yang dapat menerima dan memproses sinyal yang dipancarkan oleh satelit GPS. *Receiver* GPS yang dijual di pasaran sangat bervariasi, dari segi bentuk, merk, harga, jenis, berat dan ketelitian yang diberikan. Klasifikasi GPS receiver dapat dilakukan berdasarkan penggunaannya, fungsi, jumlah kanal dan data yang direkam.

Penentuan posisi oleh GPS *receiver* dapat dibedakan tiga jenis, yaitu tipe geodetik, tipe pemetaan, tipe navigasi, (Awaluddin, 2007). Tipe geodetik adalah tipe yang paling dapat memberikan ketelitian posisi yang lebih tinggi hingga orde mm, tipe pemetaan dapat memberikan ketelitian posisi hingga orde 1m – 5m, GPS *receiver* tipe navigasi yang sering juga disebut *handheld receiver* mempunyai ketelitian yang lebih rendah dibandingkan tipe pemetaan dan geodetik (sampai orde 10m – 100m).

Pengamatan jarak antara GPS *receiver* dengan beberapa satelit GPS digunakan GPS untuk menentukan lokasi (Sillhouete, 2007). Gambar 3.1 merupakan prinsip penentuan GPS *position*, Satelit GPS ditunjukan dengan titik A, B, dan C dan GPS receiver ditunjukan dengan titik D. Langkah pertama yaitu dilakukan adalah pengukuran terhadap *distance* dari *receiver* GPS dengan satelit A, kemudian *distance* dari GPS *receiver* dengan satelit B, kemudian *distance* dari GPS *receiver* dengan satelit C. Melakukan penggabungkan data *distance* dan posisi tiga satelit sebagai acuan, posisi dari GPS *receiver* dapat diketahui.

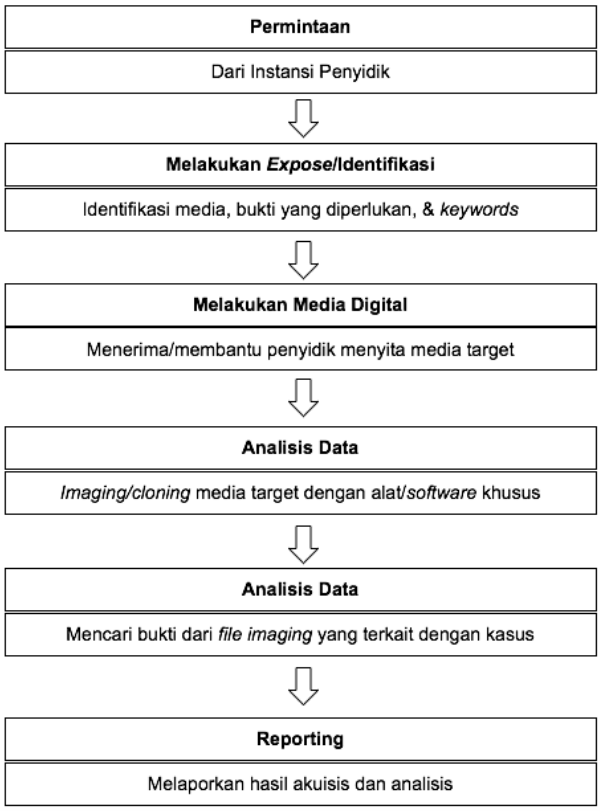


Gambar 3.1 Prinsip Penentuan GPS *Position*
(Sillhouete, 2007)

Untuk dapat menghitung GPS *receiver coordinate*, minimal ada 4 satelit yang teramati (Awaluddin, 2007). GPS akan memberikan posisi 3 dimensi (x, y, z ataupun ϑ, λ, h).

3.2 Mekanisme Bantuan Pemeriksaan *Computer Forensic*

Mekanisme bantuan pemeriksaan *computer forensic* yang dilakukan oleh Divisi Forensik Kepolisian Republik Indonesia, memiliki 6 tahap yang terdiri dari permintaan, melakukan *expose*/identifikasi, menerima media digital, *data acquistion*, analisis data dan reporting. enam tahap tersebut memiliki fungsi dan tugas masing-masing, gambar 3.2 merupakan alur detail dari mekanisme bantuan pemeriksaan komputer forensik di Divisi Forensik Kepolisian Republik Indonesia.



Gambar 3.2
Mekanisme Bantuan Pemeriksaan Komputer Forensik
(Divisi Forensik Kepolisian Republik Indonesia)

Dalam Pasal 1 angka 2, Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 tentang Tata Cara Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara Dan Laboratoris Kriminalistik Barang Bukti Kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia, menyebutkan :

> "Laboratorium Forensik adalah satuan kerja Kepolisian Republik Indonesia meliputi Pusat Laboratorium Forensik dan Laboratorium Forensik Cabang yang bertugas membina dan menyelenggarakan fungsi Laboratorium Forensik/Kriminalistik dalam rangka mendukung penyidikan yang dilakukan oleh satuan kewilayahan, dengan pembagian wilayah pelayanan (area service) sebagaimana ditentukan dengan Keputusan Kepala Kepolisian Republik Indonesia."

Pasal 1 angka 4 Peraturan Kepala Kepolisian Republik Indonesia Nomor 10 Tahun 2009 menetukan juga pengertian dari tempat kejadian perkara, bahwa: "Tempat Kejadian Perkara (TKP) adalah tempat suatu tindak pidana dilakukan atau terjadi dan tempat-tempat lain dari tersangka dan/atau korban dan/atau barang-barang bukti yang berhubungan dengan tindak pidana tersebut dapat ditemukan."

Berdasarkan Keputusan Kepala Kepolisian Republik Indonesia No. Pol.: Kep/30/VI/2003 tanggal 30 Juni 2003, tentang Perubahan atas Keputusan KaKepolisian Republik Indonesia No. Pol.: Kep/53/X/2002 tanggal 17 Oktober 2002, Tentang Organisasi dan Tata Kerja Satuan Organisasi pada Tingkat Markas Besar Kepolisian Negara Republik Indonesia, Pusat Laboratorium Forensik Kepolisian Republik Indonesia mempunyai kedudukan, tugas pokok, dan fungsi sebagai berikut :

1. Kedudukan

   Pusat Laboratorium Forensik Kepolisian Republik Indonesia disingkat Puslabfor Kepolisian Republik Indonesia adalah unsur pelaksana Badan Reserse Kriminal yang berkedudukan di bawah dan bertanggung jawaban kepada Kepala Bagian Reserse Kriminal (Bareskrim Kepolisian Republik Indonesia).

2. Tugas Pokok

   Puslabfor Kepolisian Republik Indonesia mempunyai tugas membina fungsi kriminalistik atau forensik dalam lingkungan Kepolisian Republik Indonesia dan menyelenggarakan fungsi kriminalistik atau forensik Kepolisian pada tingkat pusat.

3. Fungsi

   Dalam melaksanakan tugasnya, Puslabfor Kepolisian Republik Indonesia berfungsi :

   a. Perumusan dan pengembangan petunjuk dan prosedur pelaksanaan fungsi kriminalistik atau forensik Kepolisian.
   b. Penyelenggaran pengawasan dan pemberi arahan dalam rangka menjamin terlaksananya tugas sesuai petunjuk dan prosedur pelaksanaan fungsi kriminalistik atau forensik Kepolisian Republik Indonesia.
   c. Pemberi dukungan dalam pelaksanaan fungsi kriminalistik atau forensik Kepolisian pada tingkat kewilayahan.
   d. Penyelenggara pemeriksaan teknis kriminalistik TKP dan analisis Laboratoris barang bukti berkaitan dengan pelaksanaan penyelidikan, penyidikan, penuntutan, dan peradilan.
   e. Pemberi bantuan keahlian kriminalistik atau forensik dalam proses penegakan hukum.

f. Pengkaji dan pengembang ilmu dan teknologi kriminalistik atau forensik Kepolisian.
g. Pelaksana dalam melakukan analisa dan evaluasi pelaksanaan dan kinerja Pengembangan fungsi kriminalistik atau forensik Kepolisian.
h. Pengadaan koordinasi dan kerjasama dengan Badan-badan di dalam dan di luar Kepolisian Republik Indonesia untuk kelancaran pelaksanaan tugasnya.

4. Organisasi

Struktur organisasi berdasarkan keputusan kaKepolisian Republik Indonesia No.Pol.: Kep/9/V/2001 Puslabfor Kepolisian Negara Republik Indonesia Berkedudukan di bawah Badan Reserse Kriminal (Bareskrim) Kepolisian Republik Indonesia. Berikut ini adalah *Areal Service* Labfor Kepolisian Republik Indonesia:

a. Puslabfor Bareskrim Kepolisian Republik Indonesia (Jakarta) : Kepolisian Daerah Metro Jaya, Kepolisian Daerah Jawa Barat, Kepolisian Daerah Banten, dan Kepolisian Daerah Kalimantan Barat.
b. Labfor Cabang Medan : Kepolisian Daerah Aceh, Kepolisian Daerah Sumatera Utara, Kepolisian Daerah Sumatera Barat, Kepolisian Daerah Riau, dan Kepolisian Daerah Kepulauan Riau.
c. Labforcab Surabaya : Kepolisian Daerah Jawa Timur, Kepolisian Daerah Kalimantan Tengah, Kepolisian Daerah Kalimantan Selatan, dan Kepolisian Daerah Kalimantan Timur.
d. Labforcab Semarang : Kepolisian Daerah Jawa Tengah dan Kepolisian Daerah Daerah Istimewa Yogyakarta.
e. Labforcab Makassar : Kepolisian Daerah Sulawesi Selatan, Kepolisian Daerah Sulawesi Tenggara, Kepolisian Daerah Sulawesi Utara, Kepolisian Daerah Sulawesi Tengah, Kepolisian Daerah Gorontalo, Kepolisian Daerah Maluku, Kepolisian Daerah Maluku Utara, dan Kepolisian Daerah Papua.
f. Labforcab Palembang : Kepolisian Daerah Sumatera Selatan, Kepolisian Daerah Lampung, Kepolisian Daerah Jambi, Kepolisian Daerah Bengkulu, dan Kepolisian Daerah Bangka Belitung.

g. Labforcab Denpasar : Kepolisian Daerah Bali, Kepolisian Daerah Nusa Tenggara Barat, dan Kepolisian Daerah Nusa Tenggara Timur.

Dalam melaksanakan tugasnya, Pusat Laboratorium Forensik Kepolisian Republik Indonesia di bantu oleh 5 (lima) Departemen yang membidangi ilmu forensik di setiap bidangnya, lima Departemen adalah sebagai berikut:

1. Bidang Kimia dan Biologi Forensik (Bid Kimbiofor)
   a. Bidang Kimia Umum Forensik mencakup pemeriksaan; pemalsuan hasil-hasil industri, minyak pelumas atau oli, bahan bakar minyak, obat-obatan, kosmetik, makanan atau minuman, dan juga bahan-bahan yang tidak dikenal lainnya.
   b. Bidang Biologi Forensik mencakup pemeriksaan; Pemeriksaan cairan dan jaringan tubuh (sperma, air, darah ludah, kuku, bulu atau rambut, pemeriksaan hewan, tumbuhan dan sebagainya), serologi.
   c. Bidang Taxikologi Forensik mencakup pemeriksaan; keracunan dan peracunan yang melalui makanan atau minuman, melalui udara atau gas (Monoksida) dan air limbah sebagai pencemaran lingkungan.
2. Bidang Fisika dan Komputer Forensik (Bid Fiskomfor)
   a. Bidang Fisika Umum Forensik mencakup Pemeriksaan sabotasi, dokumen kejahatan dan sebagainya.
   b. Bidang Komputer Forensik mencakup pemeriksaan *voice*, *image, audio, video computer, mobile phones*, *cyber network* dan sebagainya.
   c. Bidang Kebakaran Forensik mencakup pemeriksaan *physical evidence* kebakaran "*on the spot*".
   d. Bidang Fisika Khusus mencakup pemeriksaan melalui *Leidetection* dan *voice detection* yang merupakan analisa kebohongan dan bekas alat atau jejak alat (*tool mark*).
   e. Bidang Instrument Forensik meliputi pemeriksaan barang bukti dengan dukungan instrument analisis.

3. Bidang Balistik dan Metallurgi Forensik (Bid Balmetfor)
    a. Bidang Senjata Api dan Peluru Forensik mencakup proses pemeriksaan partikel pecahan logam yang berasal dari senjata api dan peluru, sisa mesium, peluru dan anak peluru, juga selongsong peluru.
    b. Bidang Bahan Peledak Forensik mencakup proses pemeriksaan sumbu ledak yang merupakan barang bukti bahan peledak komersil yang berbentuk bom.
    c. Bidang Metallurgi Forensik mencakup proses pemeriksaan metallurgi umum yaitu ; perpatahan logam atau analisa kerusakan, struktur logam atau analisa spesifikasi serta pemalsuan nomor seri yang dicetak di permukaan logam (nomor rangka atau *chasis* dan nomor mesin, motor atau mobil serta peralatan cadangan lainnya).
4. Bidang Dokumen dan Uang Palsu Forensik (Bid Dokupalfor)
    a. Bidang dokumentasi Forensik mencakup proses pemeriksaan; tanda tangan, dan ketik, dan tulisan tangan.
    b. Bidang produk Cetak dan Uang palsu Forensik mencakup proses pemeriksaan; uang palsu. perangko dan bahan cetak.
    c. Bidang Fotografi Forensik mencakup proses pemeriksaan; makro dan mikro fotografi.
5. Bidang Narkotika, Psikotropika, dan obat berbahaya Forensik (Bid Narkobafor)

Bidang ini bertugas melakukan pemeriksaan yang berkaitan dengan narkotika seperti: bahan sintesa dan semi sintesa, cairan tubuh dan narkotika bahan alam, psikotropika seperti : bahan baku psikotropika, laboratorium *illegal* sepeti: bahan psikotropika dan obat atau bahan kimia obat berbahaya, prekursor, dan bahan kimia adiktif,

Divisi Forensik Kepolisian Republik Indonesia, dalam pengungkapan suatu kasus yang melibatkan penyidikan *digital evidence* menggunakan tahapan *Identification*, *Collection-Examination, Dissemination, Examination* dan *Report.* Tabel 3.1 menjelaskan perbedaan antara tahapan yang dilakukan oleh Divisi Forensik Kepolisian Republik Indonesia dengan tahapan yang ada di *Hybrid Evidence Investigation*.

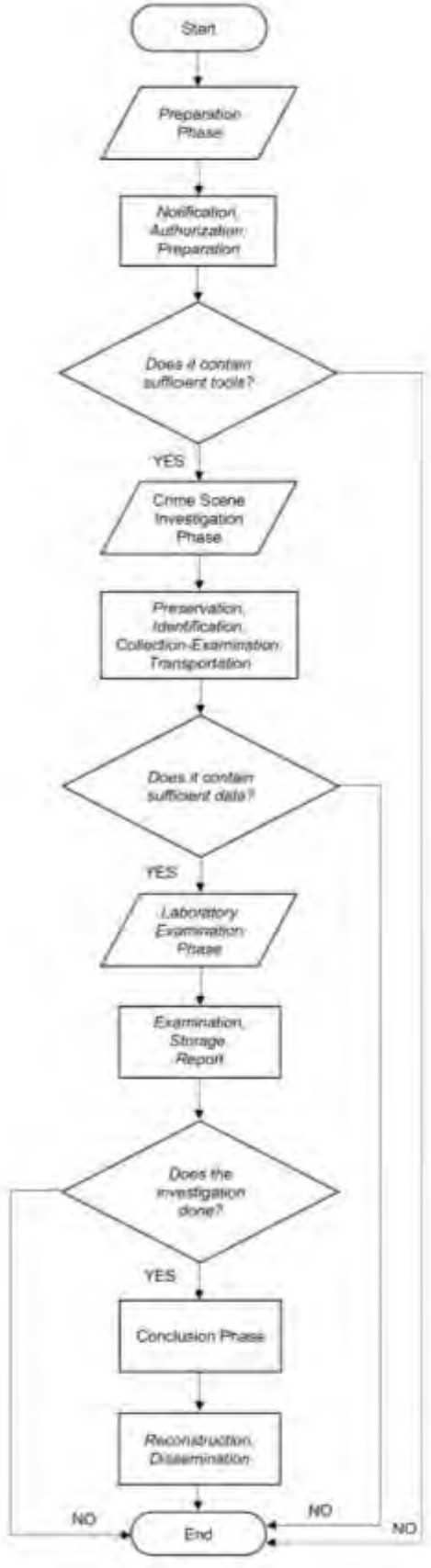
Tabel 3.1 Perbandingan Metode Divisi Forensik Kepolisian Republik Indonesia dengan *Hybrid Evidence Investigation*

No	***Hybrid Evidence Investigation***	**Metode Divisi Forensik Kepolisian Republik Indonesia**
1	*Notification*	Tidak Ada
2	*Authorization*	Tidak Ada
3	*Preparation*	Tidak Ada
4	*Preservation*	Tidak Ada
5	*Identification*	Ada
6	*Collection-Examination*	Ada
7	*Transportation*	Tidak Ada
8	*Reconstruction*	Tidak Ada
9	*Dissemination*	Ada
10	*Examination*	Ada
11	*Storage*	Ada
12	*Report*	Tidak Ada

Berdasarkan keterangan yang ada di Tabel 3.1 dapat disimpulkan bahwa metode penyidikan suatu kasus yang melibatkan pengungkapan suatu *digital evidence,* hanya menggunakan 5 tahapan. Tahapan yang digunakan Divisi Forensik Kepolisian Republik Indonesia merupakan tahapan yang langsung masuk kedalam Laboratorium Forensik untuk dilakukan penyidikan *digital evidence.*

3.3 Metodologi Penelitian

Metode *Hybrid Evidence Investigation* merupakan metodologi penelitian yang digunakan, alur dari metode *Hybrid Evidence Investigation* menggambarkan 4 fase utama yang terdiri dari *Preparation Phase, Crime Scene Investigation Phase, Laboratory Examination Phase*, *Conclusion Phase* dan 12 fase pendukung yang terdiri dari *Notification, Authorization, Preparation, Preservation, Identification, Collection Examination, Transportation, Examination, Storage, Report, Reconstruction, Dissemination.* Flowchart metode *Hybrid Evidence Investigation* dan dapat dilihat di gambar 3.3 dan masing-masing fase terdapat *output* setelah melakukan langkah-langkah dari keempat fase utama yang terdapat di model *hybrid evidence investigation*. *Output* dari tiap fase dapat dilihat di tabel 3.2.



Gambar 3.3
Flowchart *Hybrid Evidence Investigation*

Tabel 3.2
Output Fase *Hybrid Evidence Investigation*

No	***Phase***	***Output***
1	*Preparation Phase*	*Preparation phase* atau fase persiapan merupakan tahap awal dari metode *hybrid evidence investigation*, *output* fase ini adalah dibentuknya tim penyidik, tim analis dan tim ahli forensik yang akan melakukan penyidikan.
2	*Crime Scene Investigation Phase*	*Crime Scene Investigation Phase* merupakan tahap lanjutan dari *preparation phase, output* yang dihasilkan adalah didapatkannya barang bukti seperti sidik jari, *smartphone*, item yang berkaitan dengan kriminalitas, bahan biologi dan bukti fisik lainnya.
3	*Laboratory Examination Phase*	*Laboratory Examination Phase* merupakan tahap ketiga didalam metode *hybrid evidence investigation*, menghasilkan *output* berupa *metadata file* dan laporan hasil dari akusisi data dan hasil dari investigasi yang didapatkan dari *smartphone* pelaku kriminalitas.
4	*Conclusion Phase*	*Conclusion Phase* merupakan tahap akhir dari serangkaian tahapan yang terdapat didalam metode *hybrid evidence investigation* yang menghasilkan *output* berupa evaluasi dari bukti fisik yang telah didapatkan pada tahap olah TKP yang selanjutnya dilakukan investigasi untuk mendapatkan bukti *digital evidence* yang terkait dengan kasus kriminalitas.

1. *Preparation Phase* (Persiapan)

Preparation phase meliputi beberapa tahapan, yaitu:

a. *Notification*

Pemberitahuan bahwa tindak kriminalitas telah terjadi, seperti halnya dengan menggunakan nomor darurat (110) melaporkan tindak kriminal. Lembaga Penegak Hukum bertanggungjawab melakukan penyelidikan. Instansi yang bertanggungjawab

dapat ditentukan dengan kriteria geografis atau insiden dari tindak kriminal tersebut. Proses pemberitahuan ini sangat penting karena dapat digunakan untuk langkah selanjutnya.

b. *Authorization*

Otorisasi ini didapatkan dari lembaga yang bertugas untuk melakukan penyelidikan. Bentuk dan rincian otorisasi tergantung pada jenis kejahatan dan hukum acara dari suatu Negara. Setelah tindak kriminalitas ditemukan, petugas yang telah ditugaskan dapat melakukan penyelidikan dan memberikan informasi kepada pengacara yang bertugas.

c. *Preparation*

Tahapan persiapan meliputi mempersiapkan tersedianya alat-alat yang diperlukan, peralatan dan personil yang mampu melakukan penyelidikan oleh Tim Penyidik, Tim Analis dan Tim Ahli *Forensic* yang terlibat dalam kasus kriminalitas.

2. *Crime Scene Investigation Phase* (Investigasi)

Tahapan *crime scene investigation phase* terdapat beberapa proses, yaitu:

a. *Preservation*

Investigasi merupakan pengamanan Tempat Kejadian Perkara dari orang-orang yang tidak berwenang untuk mendekati, selain itu juga sumber bukti fisik dan digital terjamin keasliannya.

b. *Identification*

Tahapan identifikasi merupakan tugas yang diberikan khusus dan dilakukan oleh Tim Ahli Investigasi Kriminalitas. Bertugas untuk mengidentifikasi kemungkinan bukti yang didapatkan, secara fisik atau digital dengan item yang ada di Tempat Kejadian Perkara.

c. *Collection-Examination*

Tahapan koleksi merupakan sub fase yang menjadi faktor penting dari tahapan-tahapan yang tertera pada model ini yaitu pemeriksaan. Penyidik harus mengumpulkan

sidik jari, *smartphone* pelaku kriminalitas, *item* yang berkaitan dengan kriminalitas, bahan biologi dan bukti fisik lainnya.

d. *Transportation*

Tahapan transportasi merupakan prosedur sekunder yang memerlukan langkah-langkah khusus bertujuan untuk mencegah kerusakan bukti, Tim penyidik harus berhati-hati dengan suhu sekitar lokasi, kelembapan ruangan atau lokasi kejadian dan kemasan untuk menghindari kerusakan bukti fisik ataupun bukti digital.

3. *Laboratory Examination Phase* (Pemeriksaan Lab)

Terdapat beberapa sub fase didalam tahapan *laboratory examination phase*, yaitu:

a. *Examination*

Tahapan pemeriksaan terkait bukti yang didapatkan pada TKP (Tempat Kejadian Perkara) merupakan hal penting karena dapat memberikan informasi kepada Tim Penyidik terkait dengan bukti untuk kasus kriminalitas. Pada fase pemeriksaan, semua bukti akan benar-benar diperiksa dan dianalisis sesuai dengan sifat dan spesifikasi dari bukti yang didapatkan.

b. *Storage*

Tahap penyimpanan akan dilakukan jika tahap pemeriksaan telah selesai dilakukan, seluruh bukti yang didapatkan harus disimpan dengan baik dan dimasukkan kedalam ruangan terkunci. Setiap bukti yang telah didapatkan, diberi label dan dipisahkan untuk menghindari kontaminasi silang dan juga untuk menghindari kerusakan sehingga bukti dapat digunakan kembali untuk proses pengadilan ataupun langkah lain dari proses penyelidikan.

c. *Report*

Tahapan laporan bertujuan untuk menentukan hasil yang didapatkan dari proses pemeriksaan laboratorium, laporan lab merupakan dokumen penting yang dibutuhkan oleh Tim Penyidik dan semua pihak yang terlibat dalam kasus kriminalitas.

4. *Conclusion Phase* (Kesimpulan)

Terdapat beberapa sub fase didalam tahapan kesimpulan, yaitu:

a. *Reconstruction*

Tahapan rekonstruksi menjadi tanggungjawab dari Tim Penyidik yang melakukan evaluasi terhadap bukti yang dikumpulkan dan diperiksa, mewakili fakta seperti yang diartikan oleh analisis bukti. Jika seluruh metode yang ada di tahap rekonstruksi diterapkan maka hasil yang didapatkan akan sama.

b. *Dissemination*

Tahapan diseminasi merupakan langkah akhir dari keseluruhan model yang diusulkan, bertujuan untuk memberikan informasi kepada pihak lain yang akan melakukan investigasi serupa yang menggunakan metode dari model *Hybrid Evidence Investigation.*

BAB IV

HASIL DAN PEMBAHASAN

4.1 *Preparation Phase*

Simulasi dilakukan di Pusat Studi Forensik, Laboratorium Forensik Kepolisian Republik Indonesia. *Preparation phase* yang meliputi: *notification, authorization*, dan *preparation* tidak dilakukan di Pusat Studi Forensik Kepolisian Republik Indonesia, *preparation phase* dilakukan oleh bagian Polisi tugas umum (Polgasum) dan Polisi tugas khusus dimana terdapat tim yang bertugas 24 jam secara bergantian setiap harinya diantaranya Sabara, Reserse, Intelijen dan Propam.

Urutan *Preparation phase* dijabarkan sebagai berikut :

1. *Notification*
   a. Kasus di laporkan dengan menggunakan nomor center 110 *Call center Kepolisian Republik Indonesia* atau menggunakan sms, email, fax dan media sosial yang didukung oleh jaringan Telkom Group di Indonesia. Masyarakat yang nantinya melakukan panggilan ke nomor akses 110 akan langsung terhubung ke agen yang akan memberikan layanan berupa informasi, pelaporan (kecelakaan, bencana, kerusuhan, dan sebagainya) dan pengaduan (penghinaan, ancaman, tindak kekerasan dan sebagainya).
   b. Menggunakan aplikasi PolisiKu, Aplikasi PolisiKu memiliki fitur utama yaitu untuk mencari pos polisi terdekat dari posisi masyarakat. Selain itu terdapat fitur lain antara lain:
      1) Melakukan panggilan telepon *call center* 110 melalui jaringan internet atau VOIP (*Voice Over Internet Protocol).*
      2) Mencari pos polisi dan teleponnya di seluruh Indonesia.
      3) Melakukan pengaduan masyarakat.
      4) Serta sebagai sarana penyaluran informasi dari Humas Kepolisian Republik Indonesia kepada masyarakat.
      5) Memberikan aspirasi melalui fitur Halo Polisiku.

6) Fitur layanan publik seperti SKCK Online dan SIM Online.

2. *Authorization*

Dari hasil tahapan *notification,* Divisi Kepolisian bidang teknologi informasi akan mengkonfirmasi kebenaran dan legalitas dari laporan pelapor / korban berdasarkan *notification* tersebut dan jika laporan terbukti benar akan dilakukan proses *Authorization* dengan melacak posisi pelapor menggunakan identitas nomor telephone , Mobile Station International Subscriber Directory Number (MSISDN) atau disebut juga nomor seluler, Mobile Equipment Identity (IMEI) dan GPS dari perangkat / *smartphone* pelapor untuk mendapatkan posisi tempat kejadian perkara (TKP) serta mempermudah tim Kepolisian terdekat untuk mendatangi TKP dan selanjutnya tim akan membantu dalam pembuatan laporan polisi

Jika *notification* terbukti palsu akan ditindak lanjuti kembali dengan melacak posisi pelapor menggunakan identitas nomor *telephone* , MSISDN (nomor seluler), IMEI dan GPS dari perangkat atau *smartphone* pelapor (dan akan dilakukan proses hukum lebih lanjut sehingga akan memudahkan polisi dalam penanganan kasus laporan palsu

3. *Preparation*

Tahapan ini merupakan tahapan setelah proses *notification* dari pelapor dan *authorization* dilakukan, tim akan turun ke lokasi TKP dengan berdasarkan hasil *authorization* nomor telephone , MSISDN (nomor seluler), IMEI dan GPS dari perangkat / *smartphone* pelapor, dengan adanya tahapan *Preparation* maka tim yang turun akan mempersiapkan sumberdaya dan *tools* sesuai dengan kasus di TKP

4.2 *Crime Scene Investigation Phase*

1. *Preservation*

Pengamanan dan olah tempat kejadian perkara dilakukan oleh tim kepolisian yang sudah melalui *Preparation phase,* tahapan pengamanan dan olah tempat kejadian perkara sebagai berikut :

a. Penanganan Tempat Kejadian Perkara dengan melakukan Tindakan Pertama di Tempat Kejadian Perkara (TPTKP), yaitu tindakan yang harus dilakukan segera

untuk melakukan pertolongan atau perlindungan pada korban, penutupan dan pengamanan Tempat Kejadian Perkara guna penyidikan lebih lanjut.

b. melakukan pengamanan dan penutupan Tempat Kejadian Perkara dengan mempertahankan *status quo*, yaitu seperti memasang garis polisi (*police line*) yang berfungsi melarang siapapun masuk ke TKP kecuali penyidik atau petugas polisi lainnya, dan membuat batas Tempat Kejadian Perkara dengan tujuan agar keaslian Tempat Kejadian Perkara tetap terjaga guna kelancaran penyidikan selanjutnya.

2. *Identification*

Pada Tindakan Pertama di Tempat Kejadian Perkara (TPTKP) ini penyidik melakukan *Identification* untuk memperoleh bukti, Berdasarkan dari *Identification* akan ditemukannya bukti, antara lain : Pertama, Dari korban, pelaku, alat yang dipakai di TKP. Kedua, Pelaku, TKP dan alat yang dipakai pada korban. Ketiga,Dari korban, TKP dan alat yang dipakai pada korban. Keempat, Dari korban, TKP dan pelaku pada alat yang dipakai.

3. *Collection-Examination*

Salah satu tindakan yang dilakukan petugas di Tempat Kejadian Perkara adalah mencari barang bukti. Terdapat beberapa metode didalam melakukan pencarian barang bukti. Metode Pertama, menggunakan metode spiral yaitu, beberapa orang petugas bergerak beriringan dengan jarak tertentu, mengikuti bentuk spiral berputar kearah dalam. Metode kedua yang digunakan adalah metode strip ganda (*strip and double method*), yaitu 3 petugas berdampingan dengan jarak tertentu, bergerak bersama-sama secara serentak dari sisi lebar ke sisi lain TKP, dan dapat berputar kearah semula. Metode ketiga, menggunakan Metode *Zone (Zone Method)* yaitu dengan cara daerah dibagi menjadi beberapa bagian untuk menggeladahnya. Metode keempat, menggunakan metode Roda dalam hal ini, tempat atau ruangan dianggap sebagai suatu lingkaran, caranya adalah beberapa petugas bergerak bersama-sama kearah luar dimulai dari titik tengah tempat kejadian

Dalam metode *Hybrid Evidence Investigation* petugas akan mengembangkan kembali hasil *Preparation phase* yaitu tahapan *notification* dan *authorization* dengan menemukan alat bukti digital yang berisi *Serial Number, IMEI, Owner Phone Number, Operator, Unlocking Pattern, Cell Tower Position, Resolved Cell Tower Position, IMSI, ICCID , GPS* dan di cocokan dari hasil *notification* dan *authorization.* Selanjutkan akan dilakukan penanganan barang bukti objektif dan subyektif antara lain :

a. Penanganan Bukti-Bukti Objektif

   Bukti Obyektif adalah bukti-bukti mati atau bukti-bukti fisik yang ditemukan di TKP. Dalam metode *Hybrid Evidence Investigation* baran bukti elektronik dan digital akan menjadi target utama selain bukti fisik lain yang digunakan pelaku / korban sehingga penanganan dari barang bukti bukti elektronik dan digital akan berbeda dengan penangan alat bukti lainya, penanganan barang bukti bukti elektronik dan digital khususnya *Smartphone* adalah sebagai berikut :

   1) Usahakan *Smartphone* tetap hidup / *on* dengan menyiapkan *charger* atau sumber daya baterai cadangan.
   2) Isolasi dari jaringan komunikasi / *Network* dengan mempersiapkan *faraday bag, box* atau ruangan isolasi.
   3) Dokumentasi menggunakan kamera digital sebagai bahan analisis awal dan setelah alat bukti digital dalam proses *Laboratory Examination Phase.*

b. Penanganan Bukti-Bukti subjektif

   Penanganan bukti subjektif merupakan keterangan dari saksi dan tersangka, cara penanganan yang dilakukan polisi yaitu Pertama, bertanya langsung atau wawancara (*interview*) terhadap orang-orang yang diduga melihat, mendengar, mengetahui tindak pidana disekitar TKP.

4. *Transportation*

   Tahapan ini adalah proses pengamanan dari TPTKP sampai dengan *Laboratory Examination Phase*, pengantaran dari barang bukti digital harus di jaga secara ketat karena perubahan / koneksi jaringan telekomunikasi, daya tahan batrei dan kondisi dilapangan akan mempengaruhi barang bukti digital tersebut.

4.3 *Laboratory Examination Phase*

Penulis melakukan penelitian dimulai dari *crime scene investigation phase.* Penulis menggunakan perangkat *smartphone* berbasis android yang digunakan oleh pelaku kriminalitas yang telah didapatkan di *crime scene investigation phase* dan perangkat *smartphone* yang digunakan bertujuan untuk proses investigasi yaitu pengumpulan *digital evidence* yang bersumber dari *smartphone* pelaku, perangkat *smartphone* dilakukan installasi *software* yang digunakan untuk investigasi *digital forensic* dan terkait *policy* yang diterapkan di Pusat Studi Forensik Kepolisian Republik Indonesia.

Penulis akan menyamarkan *software* atau aplikasi yang digunakan dan beberapa identitas yang dianggap penting didalam investigasi forensika, seperti *Serial Number, IMEI, Owner Phone Number, Operator, Unlocking Pattern, Cell Tower Position, Resolved Cell Tower Position, IMSI, ICCID,* dan identitas lainnya yang bersifat rahasia, hanya diketahui oleh Tim Forensik dan hanya dipergunakan untuk investigasi *digital forensic* yang bersumber dari *smartphone* pelaku kriminalitas. *Laboratory examination phase* merupakan tahapan yang menghasilkan *output* berupa metadata *file* dan laporan hasil dari *data acquisition* dan hasil dari investigasi yang telah didapatkan dari *smartphone* pelaku kriminalitas. *Laboratory examination phase* yang dilakukan meliputi *Acquisition process,* Proses Pemeriksaan, GPS *Extraction,* GPS *Conversion.*

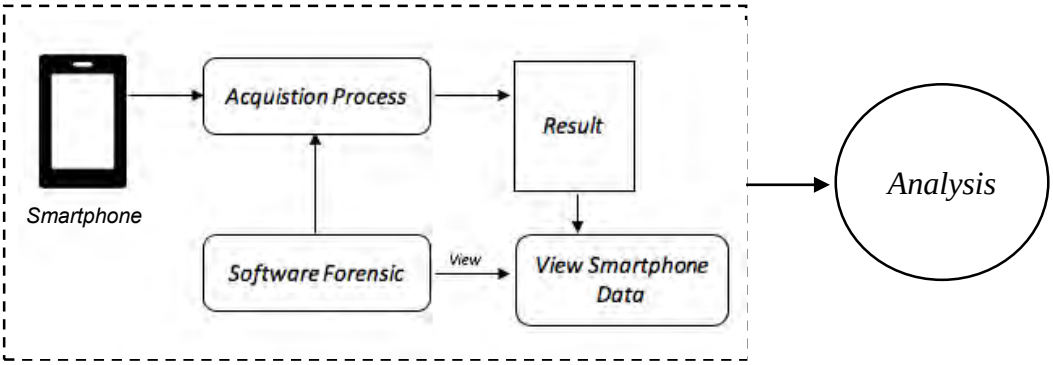
4.3.1 *Acquisition Process*

Acquisition process atau dikenal dengan istilah *imaging process* yang bertujuan untuk mendapatkan data yang bersumber dari perangkat *smartphone* pelaku kriminalitas, *Acquisition Process* memiliki teknik khusus yang dikenal dengan teknik ekstraksi. Teknik ekstraksi yang digunakan pada *Acquisition process* terdiri dari: *physical extraction, logical extraction* dan *file system extraction.* masing-masing teknik yang terdapat di *Acquisition process* memiliki fungsi dan peran yang berbeda tetapi saling terkait.

Physical extraction adalah duplikasi *bit by bit* yang didapatkan dari *flash memori* perangkat *smartphone,* teknik *physical extraction* memungkinkan akuisisi menyeluruh terhadap *file* yang disembunyikan atau yang telah terhapus. *Logical extraction* adalah akuisisi yang dilakukan di perangkat *smartphone* dengan *bit for bit* pada *logical storage*

yang meliputi file dan direktori yang terdapat di *logical storage* (*file system*), *Acquisition process* menyebabkan struktur data sistem lebih mudah untuk dilakukan ekstraksi. *File System Extraction* adalah akuisisi sebuah file yang terdapat didalam memori perangkat *smartphone,* teknik ini *file system extraction* bertujuan untuk mendapatkan akses dari semua file yang terdapat di memori perangkat *smartphone* yang dikenal dengan istilah *allocated space*, termasuk *images*, video, *database file*, *file system and log* yang dapat digunakan untuk investigasi *digital evidence*.

Perangkat *smarphone* pelaku kriminalitas yang dijadikan sebagai *digital evidence* bertujuan untuk memperoleh data duplikat tanpa merusak *digital evidence* sehingga tidak merusak kualitas *digital evidence* dan tidak menghambat dari proses investigasi*,* proses *Acquisition process* dapat dlihat di Gambar 4.1.



Gambar 4.1
Acquisition Data Process

Tahap awal *Acquisition Process* yaitu proses duplikasi memori internal perangkat *smartphone* kedalam *Secure Digital Card* atau yang dikenal dengan *sdcard*, setelah proses duplikasi memori internal dilakukan, proses selanjutnya yaitu melakukan *create file* 'dd' untuk memastikan bahwa *Acquisition process* atau *imaging process* yang dilakukan dapat terjamin keasliannya yang didapatkan dari *back-up file* dengan nilai *hash* yang tertera di tabel 4.1, penulis menutupi sebagian informasi untuk MD5 dikarenakan *policy* yang ada di Laboratorium *Forensic* Kepolisian Republik Indonesia.

Tabel 4.1
Nilai *Hashing* Perangkat *Smartphone*

No	***Name***	***Info***
1	*File Dump*	Path *Smartphone* Sony Xperia Z5 Size(bytes) 46.529.452.73 MD591728330***5e6281924bc92a3***53c2

Berdasarkan hasil yang didapatkan dari *Acquisition process* menggunakan sistem operasi Linux khusus *forensic* dan aplikasi *forensic* yang dimiliki oleh Laboratorium *Forensic* Kepolisian Republik Indonesia, untuk *digital evidence* yang bersumber dari perangkat *smartphone* yang digunakan oleh pelaku kriminalitas menunjukkan tidak ada kendala atau masalah, karena Sistem Operasi Linux khusus *forensic* membaca penuh *driver* USB. Hasil Ekstrak yang diperoleh yaitu beberapa *folder* seperti: *lib folder, files folder, no back-up folder*, dan *shared-pref folder* yang dapat digunakan untuk investigasi.

Folder yang merupakan hasil ekstraksi dari *Acquisition process,* terdapat *folder* yang terdiri dari *sub-folder* dan ada yang tidak memiliki *sub-folder.* Terdapat *folder* yang tidak memiliki *lib folder, files folder, no back-up folder*, dan *shared-pref folder, folder* yang memiliki *sub-folder* yaitu *cache folder* dan *database folder.* Tabel 4.2 merupakan tabel direktori dari masing-masing *folder*.

Tabel 4.2
Directory Folder

No	***Folder Name***	***Content***
1	*lib*	-
2	*cache*	*exocache, com.android.renderscript.cache, image_manager_disk_cache, webviecacheChromium, webviewcacheChromiumStaging* Terdapat 26 *file image*
3	*database*	*com.google.android.gsm.ads.db* Terdapat 6 file *database*
4	*files*	-
5	*no_backup*	-
6	*shared_pref*	-

Tabel 4.2 menjelaskan bahwa *cache folder* dan *database folder* merupakan folder yang dapat dilakukan investigasi lebih mendalam, karena *cache folder* dan *database folder* berisi file dari aktifitas yang dilakukan oleh pelaku kriminalitas seperti *image* dan *video*. 26

file *image* ditemukan didalam *cache folder*, dan *cache folder* memiliki *exocache* yang merupakan *sub-folder* dan ditemukan 14 file *video*.

Proses investigasi *digital evidence* yang bersumber dari perangkat *smartphone* pelaku kriminalitas memperoleh hasil yang bermanfaat untuk penyidikan, ditemukannya data yang berisi *file name, file location*, *size file*, dan *time stamp* yang memberikan informasi mengenai detail *file image* dibuat.

Image detail yang telah ditemukan dapat dilihat di tabel 4.3 dan *video file detail*, dapat dilihat di tabel 4.4. Tabel 4.3 dan tabel 4.4 merupakan hasil dari proses *aquisition data* yang merupakan tahap awal dari rangkaian proses investigasi *digital evidence* yang terdapat di *smartphone*

Tabel 4.3 adalah *image detail* yang didapatkan dari folder *Cache* dan merupakan hasil dari investigasi *digital evidence* yang telah dilakukan, berikut ini adalah penjelasan dari tabel 4.3:

1. *File Name*

   File Name adalah Nama *File Image* yang telah berhasil didapatkan dari proses investigasi *digital evidence*.

2. *File Type*

   File Type adalah Tipe atau Jenis *File* yang digunakan oleh *File* yang digunakan oleh file yang di investigasi, *File Type* menggunakan .opus yang merupakan format *File Type* dari aplikasi WhatsApp.

3. *Total Size*

   Total Size adalah Ukuran file yang dari file image yang telah dilakukan investigasi, terdapat perbedaan antara *Total size* dengan *Size on Disk* karena *Total Size* merupakan *size file* dan *Size on Disk* merupakan ruang di media penyimpanan *smartphone.*

4. *Size on Disk*

   Size on Disk adalah ukuran file di ruang media penyimpanan *smartphone*.

5. *Last Modification*

   Last Modification adalah keterangan waktu yang menunjukkan *file image* telah dilakukan perubahan atau *editing* yang kemudian di simpan ke *smartphone*.

6. *Last Access*

   Last Access adalah keterangan waktu yang menunjukkan aktifitas terakhir dari *file image.*

Tabel 4.4 adalah *image detail* yang yang didapatkan dari folder *Exocache dan* merupakan hasil dari investigasi *digital evidence* yang telah dilakukan, berikut ini adalah penjelasan dari tabel 4.4:

1. *File Name*

   File Name adalah Nama *File Image* yang telah berhasil didapatkan dari proses investigasi *digital evidence*.

2. *File Type*

   File Type adalah Tipe atau Jenis *File* yang digunakan oleh *File* yang digunakan oleh file yang di investigasi, *File Type* menggunakan .MPEG4 yang merupakan format *File Type* dari video.

3. *Total Size*

   Total Size adalah Ukuran file yang dari file image yang telah dilakukan investigasi, terdapat perbedaan antara *Total size* dengan *Size on Disk* karena *Total Size* merupakan *size file* dan *Size on Disk* merupakan ruang di media penyimpanan *smartphone.*

4. *Size on Disk*

   Size on Disk adalah ukuran file di ruang media penyimpanan *smartphone*.

5. *Last Modification*

   Last Modification adalah keterangan waktu yang menunjukkan *file image* telah dilakukan perubahan atau *editing* yang kemudian di simpan ke *smartphone*.

6. *Last Access*

   Last Access adalah keterangan waktu yang menunjukkan aktifitas terakhir dari *file image* yang terdapat di *smartphone* pelaku kriminalitas.

Tabel 4.3
Cache Folder

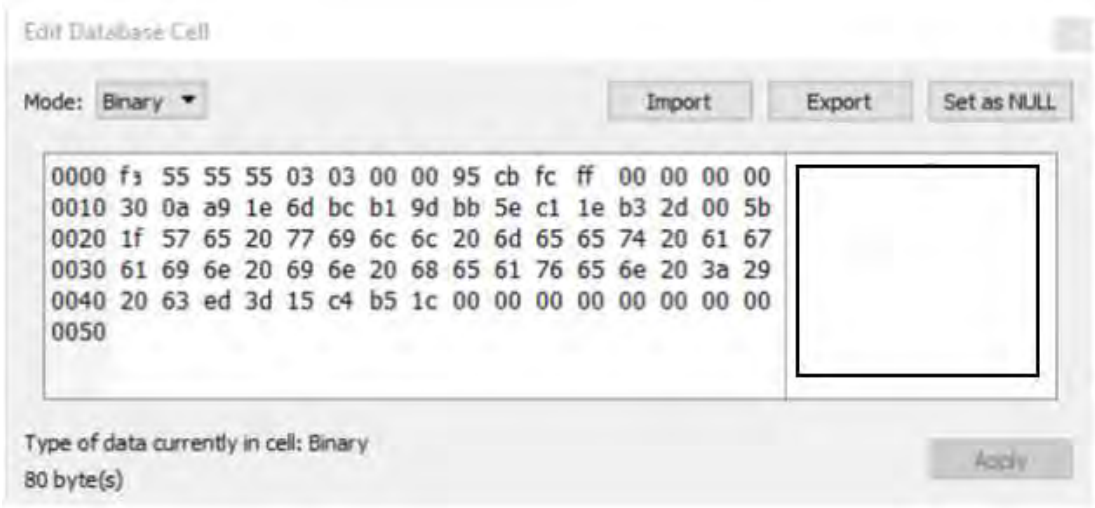
No	*File Name*	*File Type*	*Total Size*	*Size on Disk*	*Last Modification*	*Last Access*
1	IMG_200190133_20450_0	.opus	64.0KB	66.0KB	31/12/19 07:20	02/02/20 11:55
2	IMG_200190149_40720_0	.opus	54.6KB	56.0KB	31/12/19 07:56	02/02/20 13:20
3	IMG_200190166_11330_0	.opus	77.3KB	78.0KB	31/12/19 11:33	16/02/20 16:44
4	IMG_200190133_60725_1	.opus	79.5KB	82.0KB	31/12/19 11:47	16/02/20 16:58
5	IMG_200190133_15680_2	.opus	43.2KB	46.0KB	31/12/19 12:58	25/02/20 20:50
6	IMG_200190166_80832_1	.opus	43.6KB	46.0KB	31/12/19 16:36	27/02/20 19:15
7	IMG_200190166_45930_2	.opus	73.7KB	74.0KB	31/12/19 16:36	05/03/20 21:26
8	IMG_200190166_39128_3	.opus	83.9KB	86.0KB	31/12/19 16:12	11/03/20 10:41
9	IMG_200190149_66720_1	.opus	34.5KB	36.0KB	31/12/19 20:46	11/03/20 11:06
10	IMG_200190149_83229_2	.opus	87.2KB	88.0KB	31/12/19 20:56	15/03/20 14:22
11	IMG_200190149_30380_3	.opus	63.6KB	64.0KB	31/12/19 21:40	15/03/20 14:50
12	IMG_200190133_44921_3	.opus	73.5KB	76.0KB	31/12/19 22:10	15/03/20 17:10
13	IMG_200190133_20450_2	.opus	64.8KB	66.0KB	31/12/19 22:16	20/04/20 19:11
14	IMG_200190133_20450_2	.opus	89.2KB	92.0KB	31/12/19 23:20	27/04/20 18:29
15	IMG_200190133_53820_3	.opus	84.0KB	96.0KB	31/12/19 23:46	27/04/20 22:16
16	IMG_200200159_70290_0	.opus	54.0KB	56.0KB	01/01/20 00:36	08/05/20 12:40
17	IMG_200200177_66250_1	.opus	74.7KB	76.0KB	01/01/20 00:50	14/05/20 09:20
18	IMG_200200128_40690_4	.opus	87.2KB	88.0KB	01/01/20 01:32	14/05/20 11:23
19	IMG_200200177_30280_0	.opus	89.6KB	88.0KB	01/01/20 01:57	20/05/20 14:27
20	IMG_200200177_22389_3	.opus	53.5KB	56.0KB	01/01/20 02:10	20/05/20 15:30
21	IMG_200200128_77290_0	.opus	73.5KB	76.0KB	01/01/20 02:40	03/06/20 08:10
22	IMG_200200128_11957_1	.opus	73.9KB	74.0KB	01/01/20 02:55	10/06/20 23:45
23	IMG_200200177_55922_2	.opus	83.1KB	86.0KB	01/01/20 04:07	10/06/20 01:19
24	IMG_200200159_88283_2	.opus	44.0KB	46.0KB	01/01/20 04:16	17/06/20 02:46
25	IMG_200200128_38028_3	.opus	63.8KB	66.0KB	01/01/20 04:32	17/06/20 03:12
26	IMG_200200159_91628_1	.opus	83.6KB	84.0KB	01/01/20 04:47	17/06/20 04:20

Tabel 4.4
Exocache Folder

No	*File Name*	*File Type*	*Total Size*	*Size on Disk*	*Last Modification*	*Last Access*
1	0.1.2044369866548	MPEG-4	12MB	12MB	31/12/19 11:32	04/02/20 13:20
2	0.1.2318463849423	MPEG-4	30MB	30MB	31/12/19 11:46	04/02/20 15:44
3	1.1.2326461502469	MPEG-4	15MB	15MB	31/12/19 12:12	23/02/20 17:21
4	1.1.1552352461356	MPEG-4	24MB	24MB	31/12/19 15:06	16/03/20 12:52
5	1.1.1554152735349	MPEG-4	5MB	5MB	31/12/19 15:36	21/03/20 18:03
6	3.1.2550236423539	MPEG-4	17MB	17MB	31/12/19 22:20	10/04/20 22:42
7	3.1.2334209354586	MPEG-4	9MB	9MB	31/12/19 22:57	14/04/20 19:05
8	0.1.3324173520363	MPEG-4	18MB	18MB	31/12/19 23:43	26/04/20 23:06
9	2.1.3420475466349	MPEG-4	3MB	3MB	01/01/20 02:22	13/05/20 10:30
10	2.1.3303263759265	MPEG-4	5MB	5MB	01/01/20 02:45	17/05/20 14:58
11	1.1.1523274466355	MPEG-4	7MB	7MB	01/01/20 03:09	22/05/20 14:27
12	0.1.1526383572469	MPEG-4	13MB	13MB	01/01/20 03:57	27/05/20 20:50
13	3.1.2332266034743	MPEG-4	6MB	6MB	01/01/20 04:17	02/06/20 07:13
14	3.1.2354720645135	MPEG-4	10MB	10MB	01/01/20 04:55	08/06/20 09:20
15	2.1.3023456278159	MPEG-4	2MB	2MB	01/01/20 06:25	12/06/20 16:02
16	2.1.1535638352168	MPEG-4	6MB	6MB	01/01/20 06:40	20/06/20 16:55

4.3.2 Proses Pemeriksaan

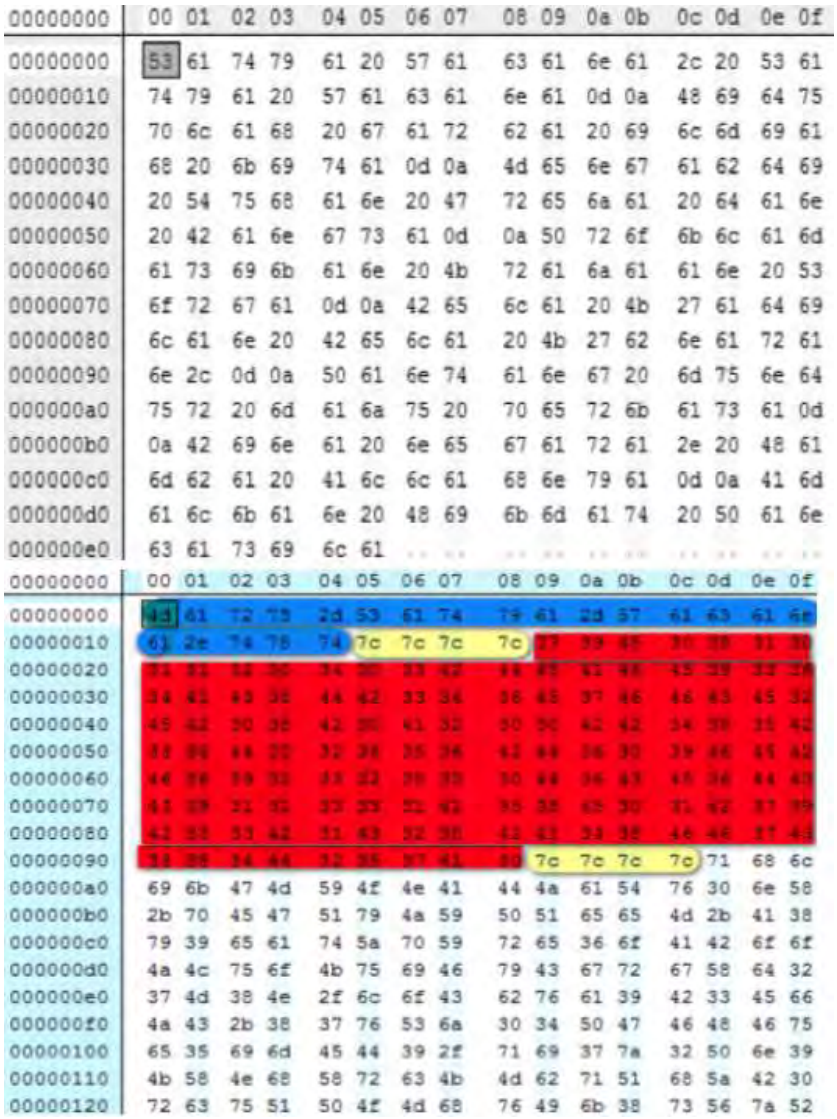
Proses pemeriksaan yang dilakukan dengan aplikasi yang dimiliki oleh Divisi Forensik Kepolisian Republik Indonesia, dengan menggunakan teknik manual *browsing* yaitu dengan cara memeriksa tipe data dari isi barang bukti digital melalui nilai *hexadecimal* yang menunjukan tipe data. Jika ditemukan salah satu huruf atau angka dari nilai *hexadecimal* tersebut berubah, maka isi dari file tersebut sudah berubah atau dimodifikasi. Gambar 4.2 merupakan hasil pemeriksaan isi file dari *smartphone*:



Gambar 4.2
Hasil Pemeriksaan *File*

Gambar 4.2 merupakan hasil pemeriksaan *file* yang telah dilakukan menggunakan *software* yang dimiliki oleh Divisi Forensik Kepolisian Republik Indonesia, dapat dilihat di gambar 4.2 terdapat *hexadecimal* dari sebuah *file*. dan di bagian yang tertutup kotak, terdapat informasi yang berupa teks asli dari *file* yang dilakukan pemeriksaan. Penulis tidak menampilkan isi dari *file* yang telah didapatkan setelah melalui proses pemeriksaan dikarenakan aturan dari Divisi Forensik Kepolisian Republik Indonesia.

Proses pemeriksaan melakukan pengambilan file kemudian mendapatkan *hexadecimal* dari sebuah *file*, bertujuan untuk melihat isi dari *file* yang telah didapatkan dengan menggunakan *software* yang dimiliki oleh Divisi Forensik Kepolisian Republik Indonesia. Gambar 4.3 merupakan proses membandingkan *file* asli dengan *file* yang telah dimodifikasi dengan melihat perubahan yang terjadi di *hexadecimal file.*



00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	53	61	74	79	61	20	57	61	63	61	6e	61	2c	20	53	61
00000010	74	79	61	20	57	61	63	61	6e	61	0d	0a	48	69	64	75
00000020	70	6c	61	68	20	67	61	72	62	61	20	69	6c	6d	69	61
00000030	68	20	6b	69	74	61	0d	0a	4d	65	6e	67	61	62	64	69
00000040	20	54	75	68	61	6e	20	47	72	65	6a	61	20	64	61	6e
00000050	20	42	61	6e	67	73	61	0d	0a	50	72	6f	6b	6c	61	6d
00000060	61	73	69	6b	61	6e	20	4b	72	61	6a	61	61	6e	20	53
00000070	6f	72	67	61	0d	0a	42	65	6c	61	20	4b	27	61	64	69
00000080	6c	61	6e	20	42	65	6c	61	20	4b	27	62	6e	61	72	61
00000090	6e	2c	0d	0a	50	61	6e	74	61	6e	67	20	6d	75	6e	64
000000a0	75	72	20	6d	61	6a	75	20	70	65	72	6b	61	73	61	0d
000000b0	0a	42	69	6e	61	20	6e	65	67	61	72	61	2e	20	48	61
000000c0	6d	62	61	20	41	6c	6c	61	68	6e	79	61	0d	0a	41	6d
000000d0	61	6c	6b	61	6e	20	48	69	6b	6d	61	74	20	50	61	6e
000000e0	63	61	73	69	6c	61	..	..	..	..	..	..	..	..	..	..

00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	43	61	72	73	2d	53	61	74	79	61	2d	57	61	63	61	6e
00000010	61	2e	74	78	74	7c	7c	7c	7c	27	39	45	30	38	31	30
00000020	31	31	32	36	34	30	33	42	44	45	41	46	45	39	33	38
00000030	34	41	43	38	44	42	33	34	36	45	37	46	46	63	45	32
00000040	45	42	30	38	42	30	41	32	30	30	42	42	34	38	31	42
00000050	38	34	44	32	32	36	35	34	43	44	36	30	39	46	45	42
00000060	44	36	39	33	33	32	39	39	30	44	36	43	45	36	44	43
00000070	41	39	31	35	33	33	31	43	39	38	65	30	31	42	37	39
00000080	42	33	33	42	31	43	32	38	43	43	33	38	46	46	37	44
00000090	38	39	34	44	32	35	37	41	30	7c	7c	7c	7c	71	68	6c
000000a0	69	6b	47	4d	59	4f	4e	41	44	4a	61	54	76	30	6e	58
000000b0	2b	70	45	47	51	79	4a	59	50	51	65	65	4d	2b	41	38
000000c0	79	39	65	61	74	5a	70	59	72	65	36	6f	41	42	6f	6f
000000d0	4a	4c	75	6f	4b	75	69	46	79	43	67	72	67	58	64	32
000000e0	37	4d	38	4e	2f	6c	6f	43	62	76	61	39	42	33	45	66
000000f0	4a	43	2b	38	37	76	53	6a	30	34	50	47	46	48	46	75
00000100	65	35	69	6d	45	44	39	2f	71	69	37	7a	32	50	6e	39
00000110	4b	58	4e	68	58	72	63	4b	4d	62	71	51	68	5a	42	30
00000120	72	63	75	51	50	4f	4d	68	76	49	6b	38	73	56	7a	52

Gambar 4.3
Hexadecimal File Asli dan *Hexadecimal File* yang telah diubah

Gambar 4.3 menampilkan perbedaan *hexadecimal* yang sangat jelas antara file asli dengan file yang telah diubah atau dimodifikasi isi dari *file* tersebut. Setiap huruf atau angka yang telah terjadi perubahan, maka dapat dipastikan isi dari *file* juga mengalami perubahan. Hasil dari proses pemeriksaan *file* dapat dijadikan *digital evidence*, yang akan dilampirkan pada saat proses persidangan.

4.3.3 GPS *Extraction*

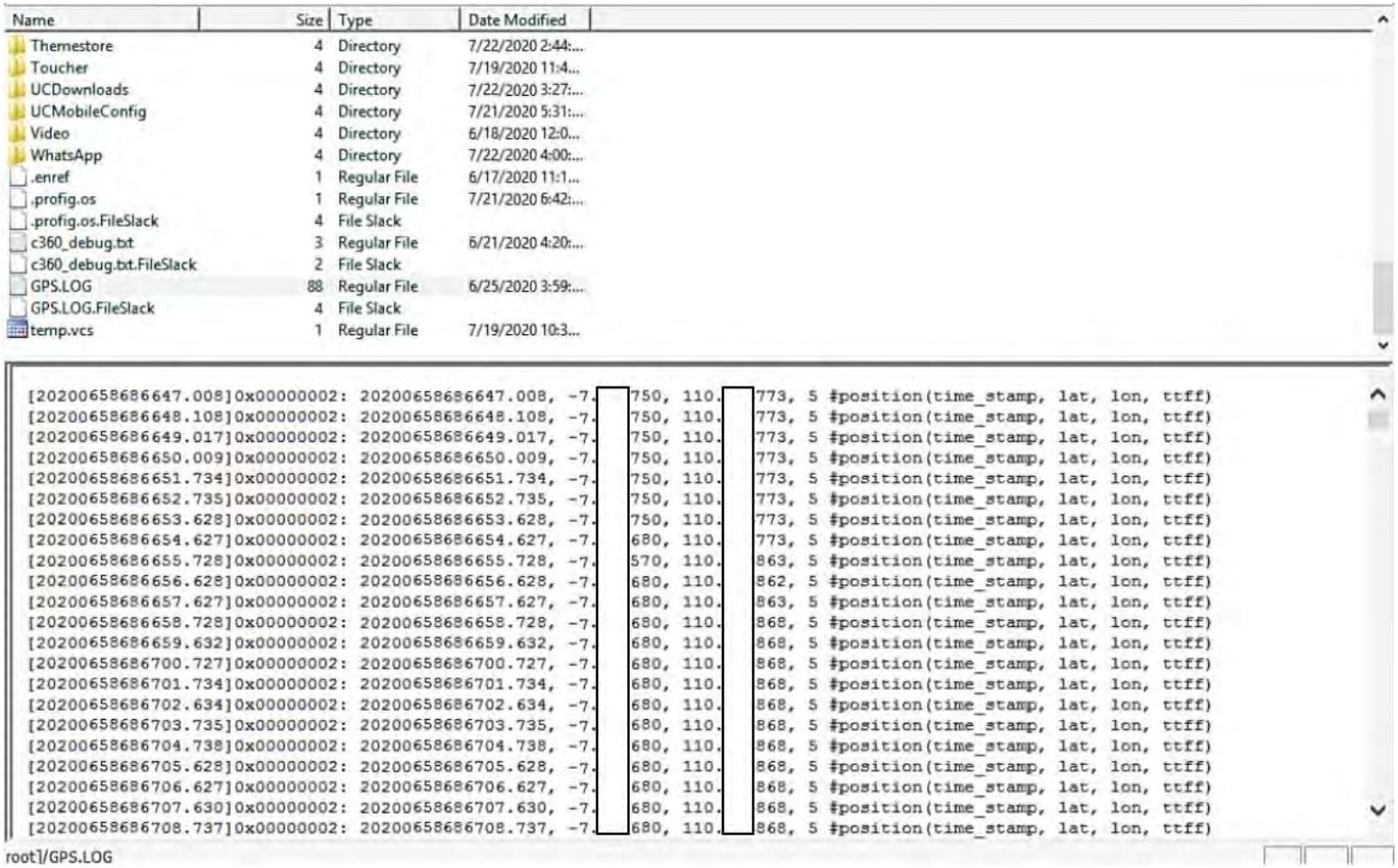
GPS *Extraction* adalah proses ekstraksi dari file yang ada pada file .dd. Informasi data GPS disimpan dalam *database* dan secara otomatis diurutkan. Dalam penelitian ini ditemukan sesuatu yang baru, media penyimpanan *database* khusunya data GPS pada Sony Z5 tidak menggunakan *database* dengan *extension* .db ataupun .sqllite, temuan pada penelitian ini membuktikan bahwa *database* pada *smartphone* android selain menggunakan .db dan .sqllite juga menggunakan .log. Data *satellite* GPS yang tersimpan dalam *database* berada dalam direktori /root/GPS.log, detail hasil ekstraksi dapat dilihat pada gambar 4.4 dan tabel 4.5. merupakan deskripsi hasil ekstraksi.

Tabel 4.5
Deskripsi Hasil Ekstraksi

No	Nama	Keterangan
1	*Time Stamp*	20200658688847
2	*Latitude*	-7.xxx750
3	*Longtitude*	110.xxx773
4	TTFF	20200658688847

Keterangan:

1. *Time Stamp* merupakan urutan karakter atau informasi yang dikodekan mengidentifikasi ketika peristiwa tertentu terjadi, biasanya memberikan tanggal dan waktu (Maus. 2011).
2. *Latitude* merupakan garis yang melintang di antara kutub utara dan kutub selatan, yang menghubungkan antara sisi timur dan barat bagian bumi. Garis *Latitude* memiliki posisi membentangi bumi seperti garis *equator* (khatulistiwa), garis lintang yang dijadikan ukuran dalam mengukur sisi utara-selatan koodinat suatu titik di belahan bumi (Sunyoto, 2013).
3. *Longtitude* merupakan garis membujur yang menghubungkan antara sisi utara dan sisi selatan bumi (kutub), garis bujur digunakan untuk mengukur sisi barat-timur koordinat suatu titik di belahan bumi (Sunyoto, 2013).
4. TTFF atau singkatan dari *time to first fix* yaitu ukuran waktu yang dibutuhkan untuk penerima GPS dalam mendapatkan sinyal satelit dan data navigasi, dan menghitung posisi (*fix*) (Maus. 2011).



Name	Size	Type	Date Modified
Themestore	4	Directory	7/22/2020 2:44:...
Toucher	4	Directory	7/19/2020 11:4...
UCDownloads	4	Directory	7/22/2020 3:27:...
UCMobileConfig	4	Directory	7/21/2020 5:31:...
Video	4	Directory	6/18/2020 12:0...
WhatsApp	4	Directory	7/22/2020 4:00:...
.enref	1	Regular File	6/17/2020 11:1...
.profig.os	1	Regular File	7/21/2020 6:42:...
.profig.os.FileSlack	4	File Slack	
c360_debug.txt	3	Regular File	6/21/2020 4:20:...
c360_debug.txt.FileSlack	2	File Slack	
GPS.LOG	88	Regular File	6/25/2020 3:59:...
GPS.LOG.FileSlack	4	File Slack	
temp.vcs	1	Regular File	7/19/2020 10:3...

```
[20200658686647.008]0x00000002: 20200658686647.008, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686648.108]0x00000002: 20200658686648.108, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686649.017]0x00000002: 20200658686649.017, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686650.009]0x00000002: 20200658686650.009, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686651.734]0x00000002: 20200658686651.734, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686652.735]0x00000002: 20200658686652.735, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686653.628]0x00000002: 20200658686653.628, -7.   750, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686654.627]0x00000002: 20200658686654.627, -7.   680, 110.   773, 5 #position(time_stamp, lat, lon, ttff)
[20200658686655.728]0x00000002: 20200658686655.728, -7.   570, 110.   863, 5 #position(time_stamp, lat, lon, ttff)
[20200658686656.628]0x00000002: 20200658686656.628, -7.   680, 110.   862, 5 #position(time_stamp, lat, lon, ttff)
[20200658686657.627]0x00000002: 20200658686657.627, -7.   680, 110.   863, 5 #position(time_stamp, lat, lon, ttff)
[20200658686658.728]0x00000002: 20200658686658.728, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686659.632]0x00000002: 20200658686659.632, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686700.727]0x00000002: 20200658686700.727, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686701.734]0x00000002: 20200658686701.734, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686702.634]0x00000002: 20200658686702.634, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686703.735]0x00000002: 20200658686703.735, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686704.738]0x00000002: 20200658686704.738, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686705.628]0x00000002: 20200658686705.628, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686706.627]0x00000002: 20200658686706.627, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686707.630]0x00000002: 20200658686707.630, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
[20200658686708.737]0x00000002: 20200658686708.737, -7.   680, 110.   868, 5 #position(time_stamp, lat, lon, ttff)
```

root]/GPS.LOG

Gambar 4.4
Ekstraksi *File* GPS.log

Gambar 4.4 merupakan hasil ekstraksi yang didapatkan dari *file* GPS.log yang ada di smartphone Sony Z5 yang digunakan oleh pelaku kriminalitas. Hasil *file* GPS.log sangat bermanfaat untuk proses penyidikan, dikarenakan *file* tersebut menyimpan *history* dari lokasi yang pernah dilalui oleh pemilik *smartphone* tersebut yang juga merupakan pelaku kriminalitas.

Hasil *file* GPS.log terdapat *Latitude, Longtitude, Time to First Fix, dan Time Stamp. Latitude* dan *Longtitude* yang berhasil didapatkan dari *file* GPS.log akan digunakan di tahap *reporting* yang merupakan presentasi GPS menggunakan Google Map dengan mengambil data *Latitude* dan *Longtitude* yang didapatkan dari hasil ekstraksi *file* GPS.log.

4.3.4 GPS *Conversion*

Metode *conversion* adalah proses membaca metada dari sebuah *file* yang berisi data gambar, video dan berbagai tipe *file* lain. Pada saat melakukan analisis di beberapa jenis file .dd yang bertujuan untuk melakukan konversi metadata dari *digital data* GPS akan mengalami kesulitan yang cukup tinggi meskipun telah dilakukan percobaan dengan menggunakan beberapa *tools*. Informasi *digital evidence* yang bersumber dari GPS, didapatkan sangat terbatas dan hanya didapatkan pada *file* yang berupa gambar (Maus. 2011). Detail *file* gambar yang ada pada file .dd dapat dilihat pada gambar 4.5.

GPS

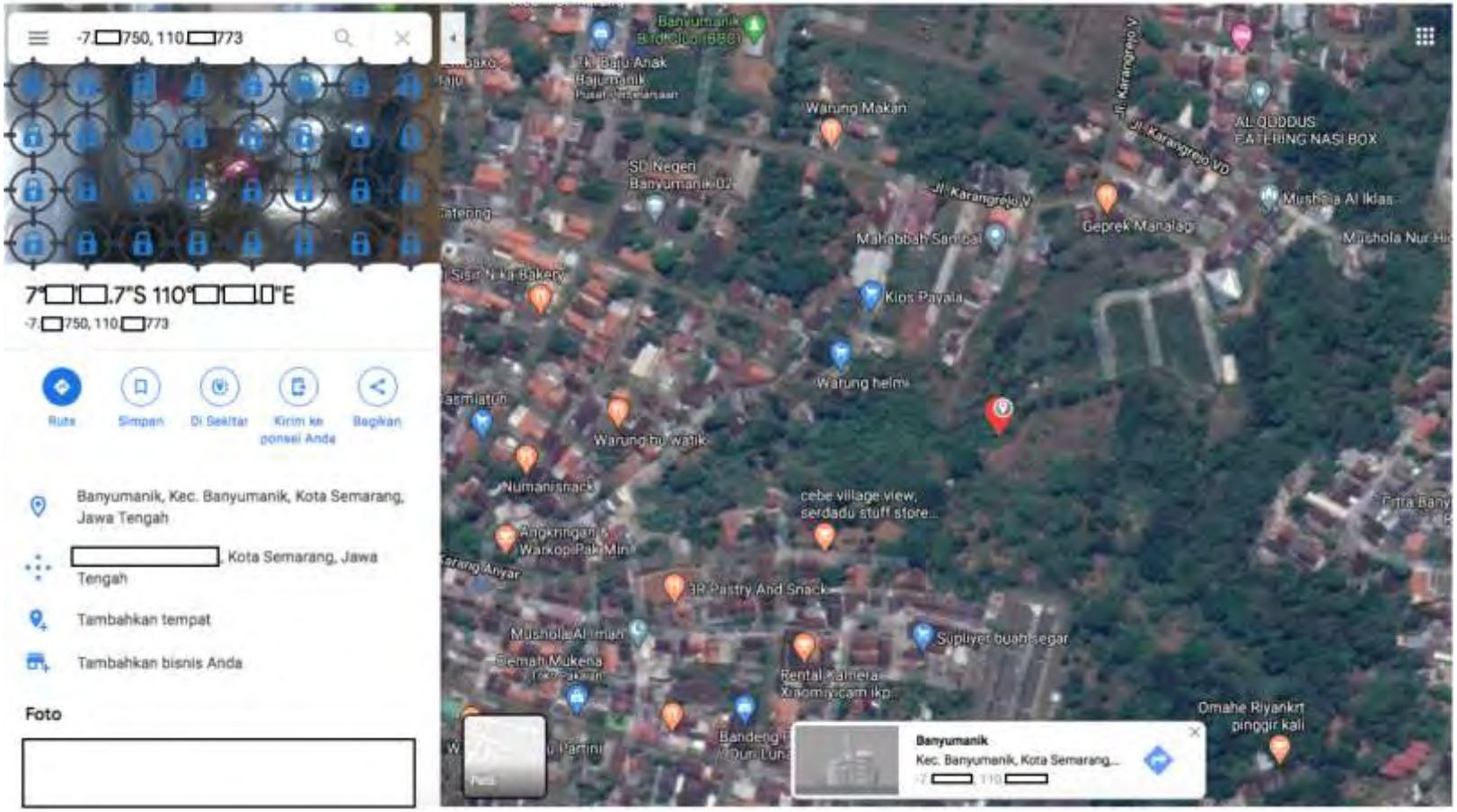
Field	Content	Tag-ID	Tag Name	Data Format
GPS tag version	Version 4.5	0000	GPSVersionID	BYTE(4)
North or South Latitude	South latitude	0001	GPSLatitudeRef	ASCII(2)
Latitude	7° [redacted] 50"	0002	GPSLatitude	RATIONAL(3)
East or West Longitude	East longitude	0003	GPSLongitudeRef	ASCII(2)
Longitude	110° [redacted] 1"	0004	GPSLongitude	RATIONAL(3)
Altitude reference	Sea level	0005	GPSAltitudeRef	BYTE
Altitude	0 m	0006	GPSAltitude	RATIONAL
GPS time (atomic clock)	15:15:03 UTC	0007	GPSTimeStamp	RATIONAL(3)
Name of GPS processing method	NETWORK	001B	GPSProcessingMet...	UNDEFINED(64)
GPS date	2020-06-20 UTC	001D	GPSDateStamp	ASCII(11)

Gambar 4.5
Detail *File* Gambar

Gambar 4.5 merupakan detail dari *file* gambar yang telah dilakukan *conversion* dengan tujuan mendapatkan data GPS ketika pemilik *smartphone* melakukan pengambilan foto atau gambar Hasil yang didapatkan dari detail *file* gambar terdapat *Latitude* dan *Longtitude* GPS yang juga sesuai dengan *Latitude* dan *Longtitude* GPS yang telah didapatkan dari proses ektraksi *file* GPS.log yang tersimpan di *smartphone* pelaku kriminalitas. Sehingga dapat dipastikan bahwa foto atau gambar yang telah dilakukan analisis terhadap detail f*ile* gambar adalah foto atau gambar yang diambil langsung menggunakan *smartphone* pelaku kriminalitas dikarenakan terdapat kesamaan data *Latitude* dan *Longtitude* hasil detail *file* gambar dengan file GPS.log.

4.3.5 *Reporting*

Reporting merupakan tahap lanjutan dari proses *extraction* dan GPS *digital evidence conversion* yang ditampilkan dalam bentuk presentasi, presentasi didalam *digital forensic* merupakan aktifitas yang dilakukan oleh Tim ahli *forensic* untuk melakukan presentasi dari hasil temuannya di pengadilan dengan tujuan untuk memberikan keterangan di suatu perkara dan untuk membantu Hakim dalam pengambilan keputusan di suatu perkara, presentasi *digital evidence* GPS dipresentasikan secara visual melalui *digital map* menggunakan google *map*, *digital evidence* GPS berupa *latitude* dan *longitude* memberikan informasi titik yang merupakan sumber pengambilan atau pembuatan sebuah dokumen. Seperti terlihat pada gambar 4.6.



Gambar 4.6
Presentasi *Digital Evidence* menggunakan *Digital Map*

Gambar 4.5 merupakan presentasi *digital evidence* menggunakan *Digital Map,* presentasi *digital evidence* dihasilkan dari serangkaian proses yang telah dilakukan oleh Tim Forensic Kepolisian Republik Indonesia. Digital Map yang digunakan untuk presentasi *digital evidence* menggunakan Google Map. Hasil dari GPS *Extraction* yang didapatkan berupa *Data Latitude* dan *Data Longtitude.*

Data Latitude dan *Data Longtitude* menunjukkan titik koordinat --7.xxx750 untuk *Data Latitude* dan 110.xxx773 untuk *Data Longtitude.* Penulis tidak menampilkan detail koordinat dari lokasi yang berhasil didapatkan dari proses hasil GPS *Extraction* dan GPS *Conversion* dikarenakan hanya untuk keperluan dari Divisi Forensik Kepolisian Republik Indonesia dan tidak diperuntukkan untuk kepentingan publik.

Titik Koordinat yang telah didapatkan dari serangkaian proses dikumpulkan untuk dilakukan proses investigasi sehingga dapat diketahui rute perjalanan atau tempat yang pernah dilewati oleh pelaku kriminalitas berdasarkan data yang didapatkan dari GPS.log *smartphone* dan hasil GPS *Extraction* dan GPS *Conversion* dari file foto atau gambar yang terdapat di *smartphone* pelaku kriminalitas.

4.4 *Conclusion Phase*

Tahap *Conclusion* merupakan tahapan dokumentasi dan evaluasi yang dilakukan setelah seluruh tahap atau proses investigasi yang telah dilakukan oleh Tim Penyidik atau Tim Analis *Forensic*. *Conclusion Phase* terdiri dari *Reconstruction* dan *Dissemination.*

1. *Reconstruction*

Rekonstruksi kejahatan merupakan tanggungjawab utama dari penyidik yang bertujuan untuk mengevaluasi bukti yang dikumpulkan selanjutnya diperiksa yang dapat dijadikan sebuah fakta temuan dan proses rekonstruksi dapat berlaku jika seluruh rangkaian forensik telah dilakukan.

2. *Dissemination*

Dissemination adalah langkah terakhir dari model *Hybrid Evidence Investigation, review* menyeluruh untuk seluruh proses investigasi dan metode *Hybrid Evidence Investigation* dapat disebarluaskan kepada pihak yang berkepentingan terkait kasus kriminalitas dalam bentuk *Digital Evidence Forensic Report,* dapat dilihat di Lampiran 20, Lampiran 21, Lampiran 22, Lampiran 23.

Tabel 4.6
Rangkuman Hasil Analisis *Digital Evidence*

No	Tahapan		*Output*	Keterangan
1	*Preparation Phase*	*Notification*	• Nomor Center 110 • Aplikasi PolisiKu	Pihak Kepolisian Divisi IT
		Authorization	• Identitas nomor telephone pelapor • *Mobile Station International Subscriber Directory Number* (MSISDN) pelapor • *Mobile Equipment Identity* (IMEI) pelapor • GPS dari perangkat / *smartphone* pelapor	Pihak Kepolisian Divisi IT
		Preparation	• Tim akan turun ke lokasi TKP • Mempermudah dalam mempersiapkan sumberdaya dan *tools* sesuai dengan kasus di TKP • GPS dari perangkat / *smartphone* pelapor	Pihak Kepolisian (tim gabungan fungsi Samapta, Reskrim, Intelijen dan Propam)
2	*Crime Scene Investigation Phase*	*Preservation*	• Melakukan pertolongan atau perlindungan pada korban, penutupan dan pengamanan Tempat Kejadian Perkara guna penyidikan lebih lanjut. • Melakukan pengamanan dan penutupan Tempat Kejadian Perkara dengan mempertahankan *status quo*.	Pihak Kepolisian (tim gabungan fungsi Samapta, Reskrim, Intelijen dan Propam)
		Identification	• Dari korban, pelaku, alat yang dipakai di TKP. • Pelaku, TKP dan alat yang dipakai pada korban. • Dari korban, TKP dan alat yang dipakai pada korban. • Dari korban, TKP dan pelaku pada alat yang dipakai.	Pihak Kepolisian fungsi Reskrim
		Collection-Examination	• Metode Spiral • Metode Strip Ganda • Metode *Zone* • Metode Roda • Barang bukti elektronik dan digital khusus *Smartphone* / telephone seluler tetap hidup / *on* • Isolasi dari jaringan komunikasi / *Network* dan data dengan mempersiapkan *faraday bag, box* • Dokumentasi	Pihak Kepolisian fungsi Reskrim khususnya labfor untuk Barang bukti elektronik dan digital *(digital evidence)*
		Transportation	• Menjaga barang bukti dari kerusakan dengan cara menjaga kelembapan dan suhu • Barang dan alat bukti digital ditempatkan pada tempat khusus terlindung dari jaringan komunikasi / *Network* dan data.	Pihak Kepolisian fungsi Reskrim khususnya labfor untuk Barang bukti elektronik dan digital *(digital evidence)*
3	*Laboratory Examination Phase*	*Examination*	• *lib folder* • *files folder* • *no back-up folder* • *shared-pref folder*	Gambar 4.1 Tabel 4.2 Tabel 4.3 Tabel 4.4 Lampiran 1 s.d lampiran 19
		Storage	• Nilai *hexadecimal* • Ekstraksi file .dd • *Latitude* • *Longtitude* • *Time to First Fix* • *Time Stamp*	Gambar 4.2 Gambar 4.3 Gambar 4.4 Gambar 4.5 Tabel 4.5
		Report	• Presentasi *digital evidence* GPS menggunakan Google Map	Gambar 4.6
4	*Conclusion Phase*	*Reconstruction*	• Evaluasi Bukti • Fakta Temuan	Pihak Kepolisian fungsi Reskrim (penyidik)
		Dissemination	• *Incoming Evidence Form* • *Evidence Chain of Custody Letter* • *Evidence Chain of Custody Form* • *Digital Evidence Forensic Report*	Lampiran 20 Lampiran 21 Lampiran 22 Lampiran 23

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Rangkaian proses pengungkapan *digital evidence* yang bersumber dari smartphone pelaku kriminalitas telah dilakukan dengan menerapkan metode *Hybrid Evidence Investigation*, diawali dari *acquisition process,* proses pemeriksaan, proses analisis (GPS *extraction*, GPS *conversion*) dan *reporting*. Penelitian dan analisa dilakukan menggunakan perangkat *smartphone* Sony Xperia Z5 dan terkait penelitian analisis *digital evidence global positioning system* berbasis *smartphone* android dapat disimpulkan sebagai berikut:

1. Proses investigasi *mobile forensic* dilakukan dari tahap *Acquisition data* yang bertujuan untuk mendapatkan data yang bersumber dari perangkat *smartphone* pelaku kriminalitas hasil dari *Acquisition data* adalah mendapatkan *Folder* yang merupakan hasil ekstraksi dari *Acquisition process,* terdapat *folder* yang terdiri dari *sub-folder* dan ada yang tidak memiliki *sub-folder.* Terdapat *folder* yang tidak memiliki *lib folder, files folder, no back-up folder*, dan *shared-pref folder, folder* yang memiliki *sub-folder* yaitu *cache folder* dan *database folder.*
2. Proses pemeriksaan file yang terdapat di *smartphone* pelaku kriminalitas, menemukan perbedaan *hexadecimal* dengan cara membandingkan *file* asli dengan *file* yang telah dimodifikasi dengan melihat perubahan yang terjadi di *hexadecimal file.*
3. Proses GPS *Extraction* menemukan *file* GPS.log yang berisi *data latitude, data longtitude*, Time Stamp, dan *Time to First Fix* yang sangat bermanfaat untuk proses penyidikan, dikarenakan *file* tersebut menyimpan *history* dari lokasi yang pernah dilalui oleh pemilik *smartphone* tersebut yang juga merupakan pelaku kriminalitas.

4. Proses GPS Presentation menggunakan Google Map berdasarkan titik Koordinat yang telah didapatkan dari serangkaian proses dikumpulkan untuk dilakukan proses investigasi sehingga dapat diketahui rute perjalanan atau tempat yang pernah dilewati oleh pelaku kriminalitas berdasarkan data yang didapatkan dari GPS.log *smartphone* dan hasil GPS *Extraction* dan GPS *Conversion* dari file foto atau gambar yang terdapat di *smartphone* pelaku kriminalitas.
5. Metode *Hybrid Evidence Investigation* dapat diimplementasikan pada proses penyelidikan,karena dengan menggunakan metode *Hybrid Evidence Investigation*, *physical evidence* dan *digital evidence* dapat dilakukan secara bersamaan, tanpa harus mengganggu bukti yang lainnya.

5.2 Saran

Saran – saran yang dapat diberikan sebagai bahan penelitian lebih lanjut adalah sebagai berikut:

1. Model *Hybrid Evidence Investigation* yang digunakan pada penelitian ini, diharapkan dapat menjadi metode yang akan menggantikan dari metode saat ini yang digunakan di Divisi Forensik Kepolisian Republik Indonesia.
2. Menggabungkan antara metode *Hybrid Evidence Investigation* dengan Algoritma Enkripsi untuk mengungkap *digital evidence* dari sebuah file yang terenkripsi.
3. Menggabungkan antara metode *Hybrid Evidence Investigation* dengan steganografi, sehingga dapat mengungkap tindak kriminalitas yang dilakukan oleh Teroris, Bandar Narkoba untuk menyembunyikan informasi atau pesan rahasia yang dikirimkan ke Organisasi atau kelompoknya.

DAFTAR PUSTAKA

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

Agarwal A, Megha, Gupta, Subhash, (2011). *Systematic Digital Forensic Investigation Model.* International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1).

Ary M, (2011). Monitoring Lokasi Anak Menggunakan Handphone ber-GPS. urusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

Asrizal, (2012). Digital Forensik. E-Dokumen Kemenag.

Atzori L., Iera A., Morabito G, (2010). *The Internet of things: A survey. Computer Networks*, 54(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010.

Awaluddin M. Teknologi *Global Positioning System* (GPS) untuk Penentuan Posisi. Diakses Juli 2020 dari www.geocities.com/

Bhosale S, Patil T., Patil P, (2015). SQLite : *Light Database System*. International Journal of Computer Science And Mobile Computing, 4(4), 882–885.

Casey E, (2011). "*Digital Evidence and Computer Crime : Forensic Science, Computer and Internet* (3rd edition)". California : Elsevier Inc.

Chip, (2013). Arsitektur Chip GPS Pada Android.

Choi J., Park J., Kim, H, (2017). *Forensic analysis of the backup database file in KakaoTalk messenger*. IEEE International Conference on Big Data and Smart Computing,BigComp,156–161. https://doi.org/10.1109/BIGCOMP.2017.7881732.

Chen, Barry, (2013). *Computer Forensics In Criminal Investigations*. http://dujs.dartmouth.edu/uncategorized/computer-forensics-in-criminal investigations.

Dieko, Alese, Thompson, Iyare, (2014). *On Forensic Investigation Models.* Proceedings of the World Congress on Engineering and Computer Science 2014 Vol I WCECS 2014, 22-24 October, 2014, San Francisco, USA.

EC-Council Press, (2010). *Investigating Data and Image Files.* USA.

E.C., Turnbull, (2000). *Digital Evidence and Computer Crime*. Academia Press.

Fauzan A., Riadi I., Fadlil A, (2017). Analisis Forensik Digital Pada Line Messeng Untuk Penanganan Cybercrime. Annual Research Seminar (ARS), 2(1), 159–163. Retrieved from http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752.

Goel, Archit., Tyagi, Anurag. Agarwal A, (2012). *Smartphone Forensic Investigation Process Model*. International Journal of Computer Science & Security (IJCSS), Volume (6) : Issue (5).

Grover J, (2013). *Android forensics: Automated data collection and reporting from a mobile device*. Digital Investigation, 10(SUPPL.). https://doi.org/10.1016/j.diin.2013.06.002.

GPSTracker. (2013). Cara Membaca Data Longtitude Latitude Alat GPS.

Haryanto T., Riadi, Prayudi, (2018). *Forensics Analysis of Sqlite Database on Android-Based IMO Applications.* International Journal of Computer Applications (0975-8887) Volume 179. No.47.

Iqbal A., Marrington, A., & Baggili, I, (2014). *Forensic artifacts of the ChatON Instant Messaging application*. Int. Workshop Syst. Approaches Digit. Forensics Eng., SADFE. https://doi.org/10.1109/SADFE.2013.6911538.

Jansen, (2007). *Guidelines on Cell Phone Forensics*. Jurnal, diterbitkan. NIST (National Institute of Standards and Technology).

Keputusan KAKEPOLISIAN REPUBLIK INDONESIA, (2001). No.Pol.: Kep/9/V/2001.

Keputusan KAKEPOLISIAN REPUBLIK INDONESIA, (2003) No. Pol.: Kep/30/VI/2003.

K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, (2012). *A Model for Hybrid Evidence Investigation*. International Journal of Digital Crime and Forensic, 4(4), 47-62. Department of Informatics, Ionian University. doi:10.4018/jdcf.201210014.

Kohar A., (2015). Analisis Kesadaran Pengguna Smartphone Terhadap Aktivitas Cybercrime. Tesis, tidak diterbitkan. Yogyakarta: Fakultas Teknologi Industri Universitas Islam Indonesia.

Kunang Y, Khristian A, (2016). Implementasi prosedur forensik untuk analisis artefak Whatsapp pada ponsel android. Annual Research Seminar, 2(1), 59–68. Retrieved from http://ars.ilkom.unsri.ac.id.

Maus, Stefan., ken, Hans., Schuba, Marko, (2011). *Forensic Analysis of Geodata in Android Smartphones*. FH Aachen, University of Applied Sciences. 52066 Aachen, Germany.

McCharthy P., (2005). *Forensic Analysis of Mobile Phones*. Tesis, diterbitkan. Australia: School of Computer and Information Science University of South Australia.

Meier R, (2012). *Professional Android 4 Application Development*. Development, 576. https://doi.org/9781118102275.

Ming J., Xie M, (2017). *Remote Live Forensics for Android Devices*. 2016 IEEE Conference on Communications and Network Security, CNS 2016, 374–375. https://doi.org/10.1109/CNS.2016.7860518.

Miller D., Grand J., Fondell, T., Anthony M, (2006). *A Road Map for Digital Forensic Research*. Journal of Animal Ecology, 75(1), 101–110. https://doi.org/10.1111/j.1365-2656.2005.01025.x.

Murphy, Cindy. (2011). *Cellular Phone Evidence Data Extraction & Documentation*. Digital Forensic Magazine. Issue 7.

Paseban. (2013). Apa Perbedaan, Kelebihan & Kekurangan Teknologi GPS vs A-GPS? Retrieved from http://portal.paseban.com/article/106052/gps-vs-a-gps-apa-kelebihan-kekurangan teknologi.

UU ITE No. 11, (2008). Pasal 112 KUHP (Kitab Undang-Undang Hukum Pidana).

Peraturan KAKEPOLISIAN REPUBLIK INDONESIA, (2010). No 21 tentang susunan organisasi dan tata kerja satker Mabes Kepolisian Republik Indonesia.

Peraturan KAKEPOLISIAN REPUBLIK INDONESIA, (2009) No 10 tentang tata cara permintaan bantuan kepada Labfor Kepolisian Republik Indonesia.

Prayogo A., Riadi, I., Luthfi, A, (2017). *Mobile Forensics Development of Mobile Banking Application using Static Forensic*. International Journal of Computer Applications, 160(1), 5–10. https://doi.org/10.5120/ijca2017912925.

Prayudi Y., Iqbal M, (2013). Analisis Forensika Digital Pada Blackberry Untuk Mendukung Penanganan Kasus *Cybercrime* Menggunakan *Smartphone*. Seminar Nasional Sistem Informasi Indonesia.

Rahayu Y., Prayudi, "Membangun *Integrated Digital Forensics Investigation Frameworks* (IDFIF) Menggunakan Metode *Sequential Logic*," in Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014), 2014, vol. 2014, no. Sentika.

Racioppo C., Murthy, N, (2012). *Android Forensics : A Case Study of the " HTC Incredible " Phone*. Proceedings of Student-Faculty Research Day, 1–8. Retrieved from http://csis.pace.edu/~ctappert/srd2012/b6.pdf.

Rahmadi, (2003). Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa Dan Bagaimana. Makalah, tidak diterbitkan.Bandung: Teknik Elektro Option Teknologi Informasi Institut Teknologi Bandung.

Riadi I., Sunardi, Firdonsyah, A, (2017). *Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework*. International Journal of Cyber- Security and Digital Forensics, 16(4), 198–205.

Sidik M, Husni M, Nur W, (2017). *Investigation Process Mobile Forensics on Smartphone iOS Based.* Jurnal Rekayasa Sistem & Industri. Volume 4, Nomor 1. Pg. 93-98.

Sillhouete. Peta Umum: Bagaimana GPS Menentukan Suatu Lokasi. Diakses Juli 2020 dari *Navigasi.net*.

Solihah S, (2014). Analisis Digital Forensik untuk File Terenkripsi dengan menggunakan Winhex dan Tools Kali Linux Autopsy. Tasikmalaya: Universitas Siliwangi.

Sunyoto, (2013). "Integrasi modul GPS Receiver dan GPRS untuk penentuan posisi dan jalur pergerakan objek. Yogyakarta: STMIK Amikom.

Suryanto, (2016). "Pengembangan dan analisis metode permutasi *chaotic* baru berbasis multiputaran mengecil dan membesar untuk enkripsi citra dengan tingkat keamanan tinggi, cepat dan tahan terhadap gangguan". Disertasi Program Doktor, Universitas Indonesia.

"The Scientific Working Group on Digital Evidence" (SWGDE), (2015). *"Information of probative value stored or transmitted in digital form".* International Journal of Digital Evidence, Springer, 2015 volume 5, Issue 3.

Tohid, (2012). *Bin Laden bodyguard's satellite phone calls helped lead US forces to hiding place.* The Christian MONITOR. Karachi, Pakistan.

Valjarevic, A., Venter, H. S., & Ingles, M. (2014). Towards a prototype for guidance and implementation of a standardized digital forensic investigation process. 2014 Information Security for South Africa. doi:10.1109/issa.2014.6950488.

Williams, J, (2012). *ACPO Good Practice Guide for Digital Evidence*, (March), 41. Retrieved from http://www.digital-detective.net/digital-forensics documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf%0Ahttp://w ww.acpo.police.uk/documents/crime/2014/Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011_Website.pdf.

Yadi I, Kunang, Y, (2014). Analisis Forensik Pada Platform Android. Konferensi Nasional Ilmu Komputer (KONIK), 141–148. https://doi.org/10.13140/RG.2.1.2967.0003.

Yudha F., (2013). *USB Analysis Tool* Untuk Investigasi Forensika Digital. Jurnal, telah diterbitkan. Yogyakarta: Fakultas Teknologi Industri Universitas Islam Indonesia.

Yudhana A, Riadi I, Anshori, (2017). *Analysis of Digital Evidence on Facebook Messenger Using the NIST Method*. Jurnal Insand Comtech, Vol. 2, No. 2.

Yusoff, Roslan, (2011). *Common Phases of Computer Forensic Investigation Models.* International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

Zamroni G., Umar R., Riadi I, (2016). Analisis Forensik Aplikasi Instant Messaging Berbasis Android. Annual Research Seminar (ARS), 2(1), 102–105.

LAMPIRAN-LAMPIRAN

Lampiran 1: *Device and Case Information*

Case Evidence Number: **9695889-689-968**

Manufacturer	Sony Xperia
Product	Z5
HW Revision	[redacted]
Platform	Android
SW Revision	7.0 (24)
Serial Number	[redacted]
Adb Backup Password	[redacted]
Unlocking Pattern	5690125
IMEI	[redacted]
Rooted	No
SIM Card	Yes
Owner Phone Number	[redacted]
Operator	[redacted]

Case Information

Case Label	Narcotics (Opioids)
Case Evidence Number	9695889-689-968
Case Evidence Details	

Device Information

Device Label	Device number #1
Device Name	Sony Xperia Z5
Device ID	
Device Evidence Number	7289029-248-901
Owner Name	[redacted]
Owner Phone Number	[redacted]
Phone Notes	

Investigator Information

Investigator Name	I Putu Eka Warmayudha
Investigator Designation	
Investigator Email	iputuekawarmayudha@gmail.com
Investigator Phone Number	+6285795078445
Permission Document	

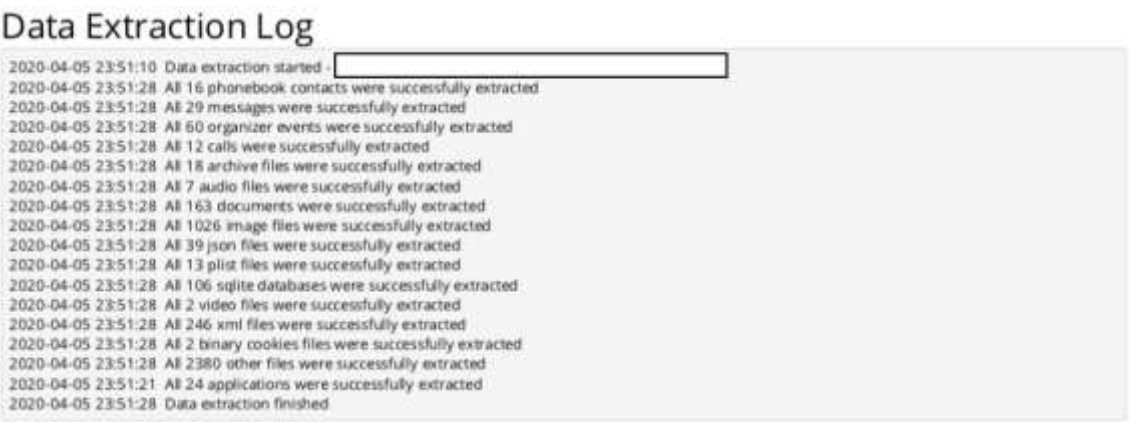
Extraction Information

Data Extraction Started	2020-04-05 23:51:10 (UTC+[redacted])
Data Extraction Finished	2020-04-05 23:51:28 (UTC+[redacted])
Extracted by	[redacted]
Report Generated by	[redacted]
Applications Analyzed by	[redacted]

Device Properties

Manufacturer	Sony Xperia
Product	Z5
HW Revision	[redacted]
Platform	Android
SW Revision	7.0 (24)
Serial Number	[redacted]
ADB Backup Password	[redacted]
Unlocking Pattern	5690125
Device Title	[redacted]
Manual Time	no
Time Zone	Indonesia
Manual Time Zone	no
IMEI	[redacted]
Cell Tower Position	MCC: [redacted] MNC: [redacted] LAC: [redacted] CID: [redacted]
Resolved Cell Tower Position	Latitude [redacted] °
	Longitude [redacted] °
Wi-Fi MAC Address	[redacted]
Bluetooth Address	[redacted]
Rooted	No
SIM Card	✓ yes
IMSI	[redacted]
SIM Card Country	Indonesia
ICCID	[redacted]
Owner Phone Number	[redacted]
Operator	[redacted]

Lampiran 2: ***Data Extraction Log***



Data Extraction Log

2020-04-05 23:51:10 Data extraction started - [redacted]
2020-04-05 23:51:28 All 16 phonebook contacts were successfully extracted
2020-04-05 23:51:28 All 29 messages were successfully extracted
2020-04-05 23:51:28 All 60 organizer events were successfully extracted
2020-04-05 23:51:28 All 12 calls were successfully extracted
2020-04-05 23:51:28 All 18 archive files were successfully extracted
2020-04-05 23:51:28 All 7 audio files were successfully extracted
2020-04-05 23:51:28 All 163 documents were successfully extracted
2020-04-05 23:51:28 All 1026 image files were successfully extracted
2020-04-05 23:51:28 All 39 json files were successfully extracted
2020-04-05 23:51:28 All 13 plist files were successfully extracted
2020-04-05 23:51:28 All 106 sqlite databases were successfully extracted
2020-04-05 23:51:28 All 2 video files were successfully extracted
2020-04-05 23:51:28 All 246 xml files were successfully extracted
2020-04-05 23:51:28 All 2 binary cookies files were successfully extracted
2020-04-05 23:51:28 All 2380 other files were successfully extracted
2020-04-05 23:51:21 All 24 applications were successfully extracted
2020-04-05 23:51:28 Data extraction finished

Lampiran 3: *Contact Analysis*

Contact Analysis (424 total, 1 deleted)

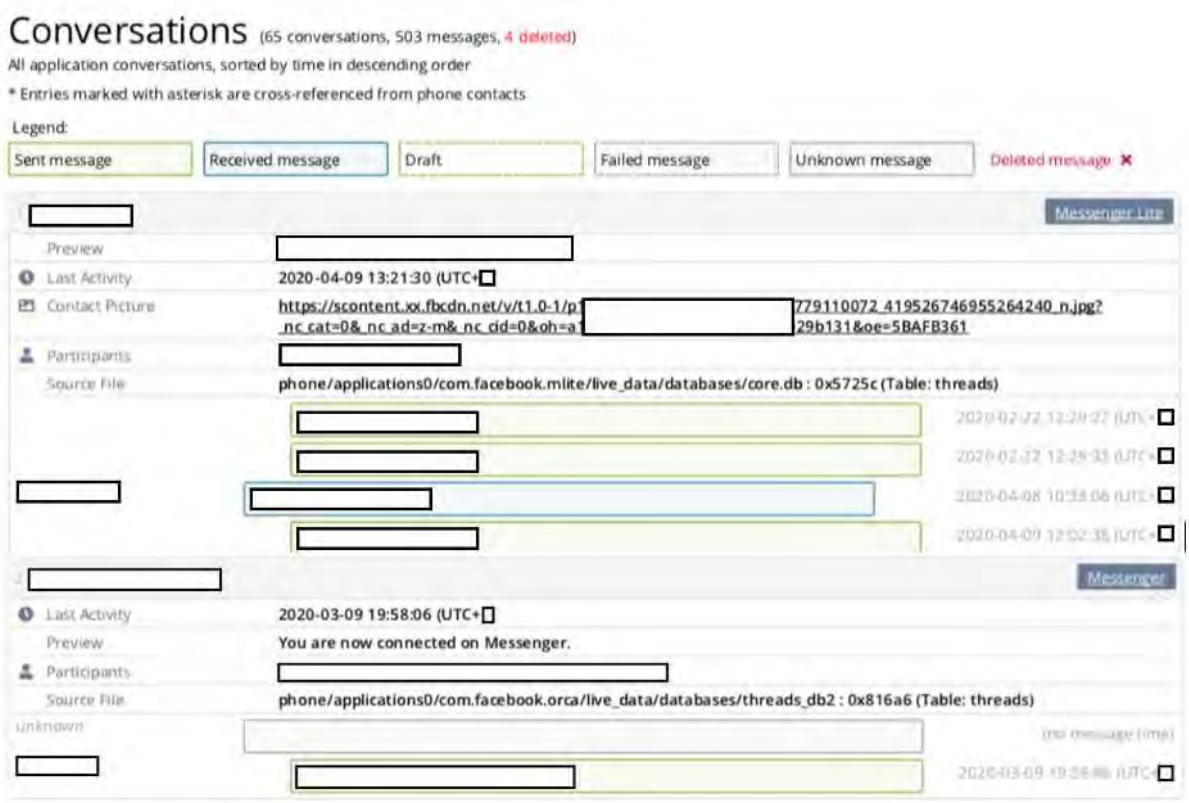
A subset of phone contacts filtered by a minimum of 1 associated events, sorted by the number of associated events in descending order

Contact	Origin	Total	Messages	Calls	Other
[redacted]	Messenger	429	Total: 384 Received: 153 Sent: 197 Other: 34 Word Count: 2768	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	45
[redacted]	Messenger	55	Total: 52 Received: 19 Sent: 33 Other: 0 Word Count: 244	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	3
[redacted]	Messenger	24	Total: 23 Received: 5 Sent: 17 Other: 1 Word Count: 101	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	23	Total: 22 Received: 12 Sent: 9 Other: 1 Word Count: 60	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 13 Sent: 7 Other: 0 Word Count: 93	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 12 Sent: 8 Other: 0 Word Count: 42	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 13 Sent: 7 Other: 0 Word Count: 148	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 12 Sent: 8 Other: 0 Word Count: 64	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 8 Sent: 12 Other: 0 Word Count: 95	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
[redacted]	Messenger	21	Total: 20 Received: 6 Sent: 14 Other: 0 Word Count: 56	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1

Lampiran 4: *Calls*

Lampiran 5: *Contact Account*

Lampiran 6: *Conversation*



Lampiran 7: *Deleted Data*

Lampiran 8: *Emails*

Email

Label	Email
Package	com.android.email
Version	5.0.0.0200
Application Type	System Application
Application Size	13.4 MB
Data Size	568.0 kB
APK File Extracted	✖ no
First Installed	2019-11-09 19:49:28 (UTC+)
Last Updated	2019-11-09 19:49:28 (UTC+)

Accounts (1)

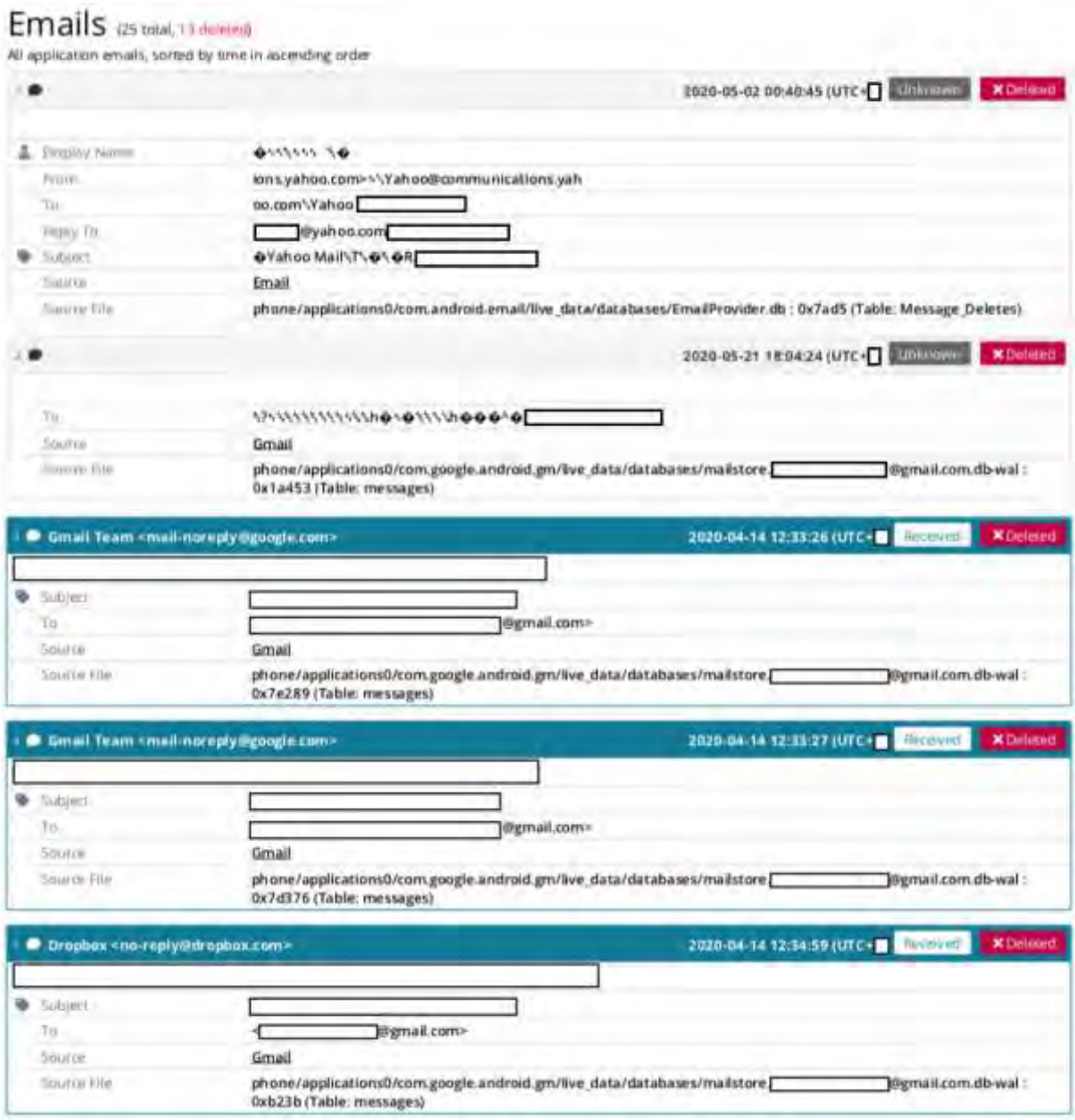
[redacted]

Email	[redacted]
Outgoing Name	[redacted]
Password Encrypted	[redacted]*Ph/3G6McEJX1Zl=
Password	[redacted]
Source file	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x14ef1 (Table: Account)

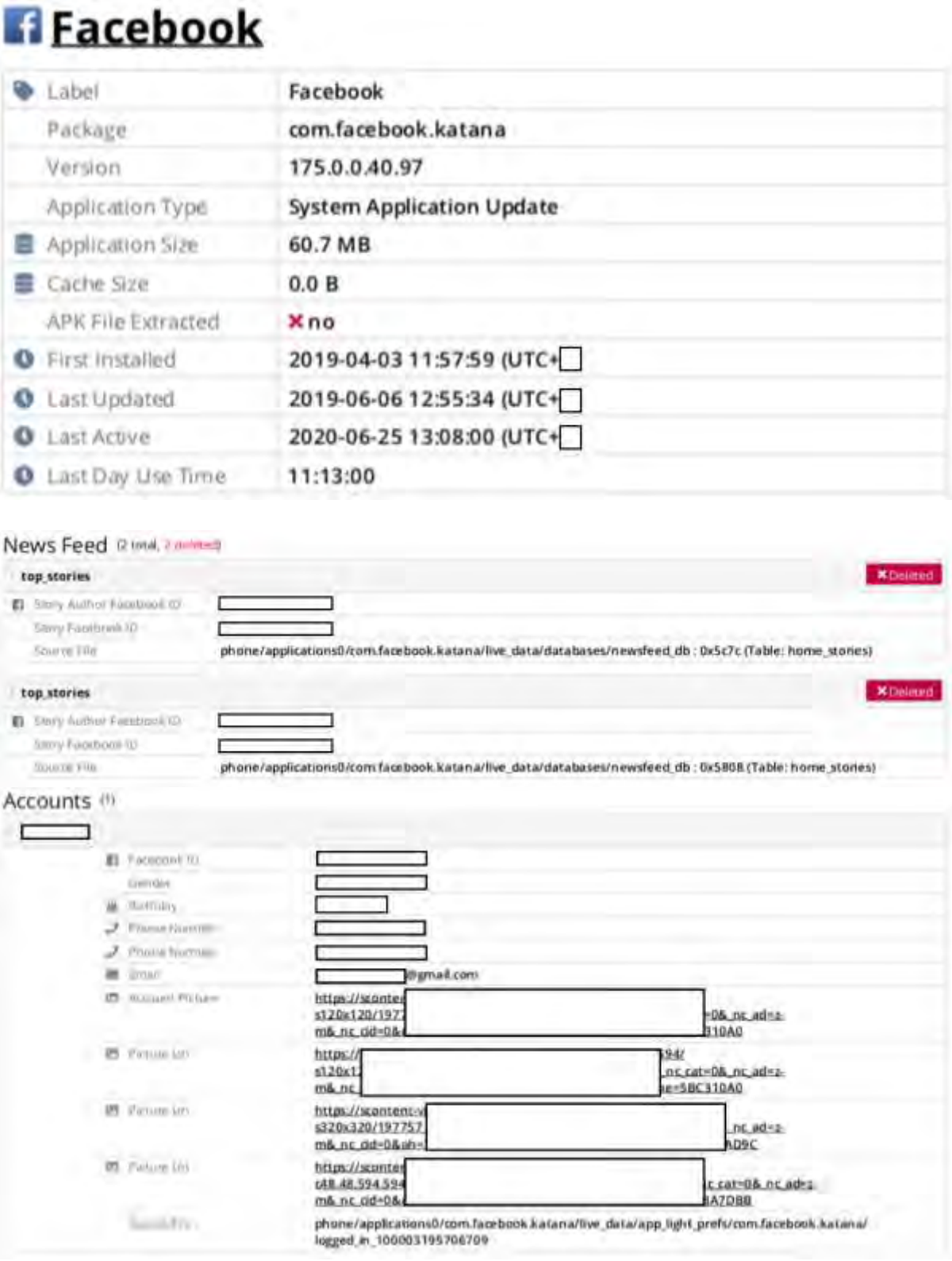
[redacted]

User Name	[redacted]
Password Encrypted	[redacted]*Ph/3G6McEJX1Zl=
Password	[redacted]
Protocol	smtp
Address	smtp.mail.yahoo.com
Port	465
Source file	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x13f2f (Table: HostAuth)

Lampiran 9: *Emails Messages*



Lampiran 10: Facebook



Facebook

Label	Facebook
Package	com.facebook.katana
Version	175.0.0.40.97
Application Type	System Application Update
Application Size	60.7 MB
Cache Size	0.0 B
APK File Extracted	✖ no
First Installed	2019-04-03 11:57:59 (UTC+[redacted])
Last Updated	2019-06-06 12:55:34 (UTC+[redacted])
Last Active	2020-06-25 13:08:00 (UTC+[redacted])
Last Day Use Time	11:13:00

News Feed (2 total, 2 deleted)

top_stories — ✖ Deleted

Story Author Facebook ID	[redacted]
Story Facebook ID	[redacted]
Source File	phone/applications0/com.facebook.katana/live_data/databases/newsfeed_db : 0x5c7c (Table: home_stories)

top_stories — ✖ Deleted

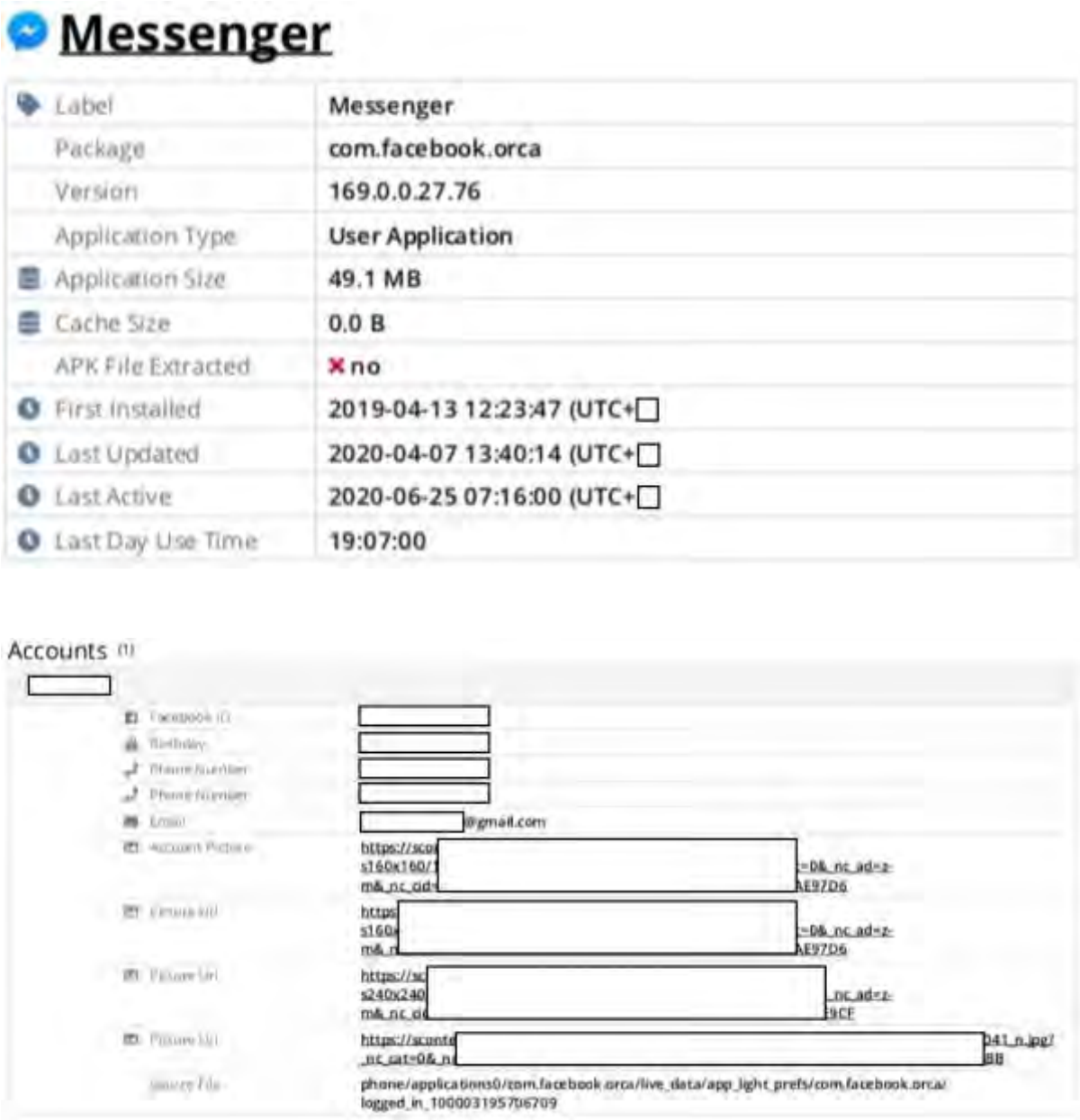
Story Author Facebook ID	[redacted]
Story Facebook ID	[redacted]
Source File	phone/applications0/com.facebook.katana/live_data/databases/newsfeed_db : 0x5808 (Table: home_stories)

Accounts (1)

[redacted]

Facebook ID	[redacted]
Gender	[redacted]
Birthday	[redacted]
Phone Number	[redacted]
Phone Number	[redacted]
Email	[redacted]@gmail.com
Account Picture	https://scontent-[redacted]&_nc_ad=z-m&_nc_oid=0&[redacted]310A0
Picture Url	https://[redacted]/s120x1[redacted]_nc_cat=0&_nc_ad=z-m&_nc_[redacted]e=5BC310A0
Picture Url	https://scontent-[redacted]/s320x320/197757[redacted]_nc_ad=z-m&_nc_oid=0&oh=[redacted]AD9C
Picture Url	https://scontent[redacted]/s48.48.594.594/[redacted]c_cat=0&_nc_ad=z-m&_nc_oid=0&[redacted]8A7DB8
Source File	phone/applications0/com.facebook.katana/live_data/app_light_prefs/com.facebook.katana/logged_in_100003195706709

Lampiran 11: ***Facebook Messenger***



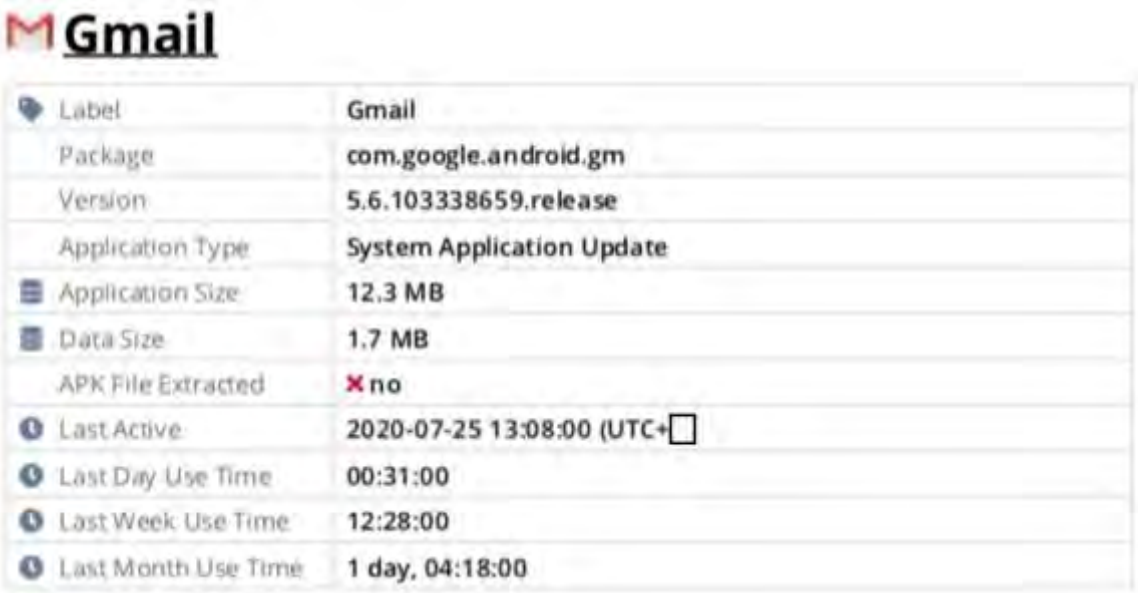
Messenger

Label	Messenger
Package	com.facebook.orca
Version	169.0.0.27.76
Application Type	User Application
Application Size	49.1 MB
Cache Size	0.0 B
APK File Extracted	✖ no
First Installed	2019-04-13 12:23:47 (UTC+☐
Last Updated	2020-04-07 13:40:14 (UTC+☐
Last Active	2020-06-25 07:16:00 (UTC+☐
Last Day Use Time	19:07:00

Accounts (1)

☐	
Facebook ID	☐
Birthday	☐
Phone Number	☐
Phone Number	☐
Email	☐@gmail.com
Account Picture	https://sc☐ s160x160/1☐ =0&_nc_ad=z-m&_nc_oh=☐ AE97D6
Picture Id	https☐ s160x☐ =0&_nc_ad=z-m&_n☐ AE97D6
Picture Url	https://sc☐ s240x240☐ _nc_ad=z-m&_nc_oh=☐ 9CE
Picture Url	https://scontent☐ 041_n.jpg?_nc_cat=0&_nc☐ 88
Source File	phone/applications0/com.facebook.orca/live_data/app_light_prefs/com.facebook.orca/logged_in_1000031957706709

Lampiran 12: ***Gmail***



Lampiran 13: ***Internet***

Lampiran 14: *Password*

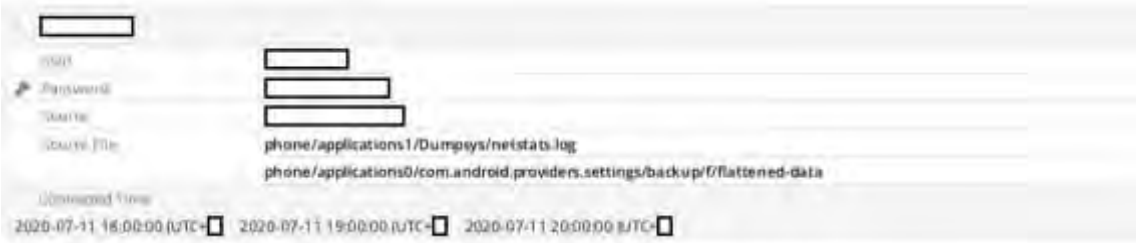
Lampiran 15: *Viber*

Lampiran 16: *Web Browsing History*

Lampiran 17: *Web Search History*

Lampiran 18: *WhatsApp*

Lampiran 19: *Wifi Networks*



Lampiran 20: ***Incoming Evidence Form***

INCOMING EVIDENCE FORM

Your Logo Here	Your Address Here

[Agency name] Case #:		Originating Agency Case #:	
Person Delivering Evidence:		Division / Agency:	
Date Evidence Received:		Time Evidence Received:	

Item #	Qty.	Description	Location Stored

Item #	Released To	Date/Time	Signature

Person Accepting Evidence:		Signature:	

Lampiran 21: ***Evidence Chain of Custody Letter***

YOUR LOGO HERE

[Click **here** and type Date]

[Click **here** and type addressee's name & title]
[Click **here** and type addressee's department name]
[Click **here** and type addressee's company name]
[Click **here** and type P.O. Box or street address]
[Click **here** and type city, state, and zip code]

Subject: **CHAIN OF CUSTODY**

[AGENCY NAME] Case #: "[Click here and type case number]"

Enclosed you will find the [AGENCY NAME] chain of custody form.

UPON RECEIVING THIS PACKAGE, PLEASE:

- Sign and date the Chain of Custody Form (highlighted sections)
- Fax the signed form to (xxx)xxx-xxxx IMMEDIATELY or
- Scan and Email the signed form to email@email.go.id IMMEDIATELY

These steps are required in order to complete the chain of custody and remain in compliance policy and legal requirements.

Thank you,

"[Click here and enter signature information]"

Enclosure: as stated

Lampiran 22: ***Evidence Chain of Custody Form***

CHAIN OF CUSTODY FORM

Your Logo Here	Your Address Here

[Agency Name] Case #:	

Item #	Date/Time Removed	Reason for Removal of Evidence	Signature

Item #	Date/Time Returned	Comments	Signature

Lampiran 23: ***Digital Forensic Report Template***

OFFICIAL USE ONLY

DIGITAL EVIDENCE FORENSIC REPORT

Your Logo Here	Your address here

CASE INFORMATION:

Agency Case #:		Originating Agency Case #:	

[removed] #:		[removed] #:		Remedy#:	
Distribution:	☐ [removed] ☐ [removed] ☐ [removed] ☐ IT ☐ [removed] ☐ Internal Audit ☐ Emp. Relations ☐ CI ☐ Other:				

Date/Time Report Completed:		Date/Time Incident Occurred:	

Type of Report:	Initial

INVOLVED:

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____
Cell Phone: _____ Work Phone: _____ Employee #: _____

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____
Cell Phone: _____ Work Phone: _____ Employee #: _____

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____

Cell Phone:		Work Phone:		Employee #:	

OFFICIAL USE ONLY

SUMMARY:

EVIDENCE SUBMITTED:

Item #	

SOFTWARE UTILIZED

All software utilized in this examination is fully licensed and registered to [Agency Name] or its agents. All software and forensic hardware has been validated pursuant to [Agency Name] policies and procedures.

FORENSIC EXAMINATION OF EVIDENCE ITEM #1

Item #1 – Can be described as

[insert photo here] [insert photo here]
[insert photo here] [insert photo here]

HASH OF ORIGINAL EVIDENCE

The original media was connected to a forensic hardware write blocker (asset tag #) and the write blocker connected to a forensic computer (asset tag #). Prior to doing anything with the original media, the media was hashed to obtain a baseline hash value. This allows the hash value of the original media to later be compared to the hash value of the forensic image created of the original media. By comparing the hash values of the original media and that of the forensic image, the forensic image can be authenticated as an exact duplicate copy of the original evidence.

The hash values obtained from the original evidence were as follows:

☐ MD5:
☐ SHA1:
☐ Other:

FORENSIC IMAGING

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

☐ Government owned, forensically wiped hard drive
☐ Government owned, forensically wiped Storage Area Network (SAN)