STUDI ANALISIS *FORENSIC* PADA PERANGKAT GPS

(*Global Positioning System*)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika



Oleh:

Nama : Bilal Abdussalam

No. Mahasiswa : 10523253

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2014

LEMBAR PENGESAHAN DOSEN PEMBIMBING

STUDI ANALISIS *FORENSIC* PADA PERANGKAT GPS (*Global Positioning System*)

TUGAS AKHIR

OLEH:

Nama : Bilal Abdussalam

NIM : 10523253

Yogyakarta, 29 Agustus 2014

Pembimbing

Yudi Prayudi, S.Si., M.Kom.

LEMBAR PENGESAHAN PENGUJI

STUDI ANALISIS *FORENSIC* PADA PERANGKAT GPS (*Global Positioning System*)

TUGAS AKHIR

OLEH:

Nama	**: Bilal Abdussalam**
No. Mahasiswa	**: 10523253**

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 29 Agustus 2014

Tim Penguji,

Yudi Prayudi, S.Si., M.Kom. _____
Ketua

Syarif Hidayat, S.Kom., M.I.T. _____
Anggota I

Ari Sujarwo, S.Kom., M.I.T. _____
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

Hendrik, S.T., M.Eng.

LEMBAR PERNYATAAN KEASLIAN TUGAS

Yang bertanda tangan dibawah ini

Nama : Bilal Abdussalam

NIM : 10523253

Tugas Akhir dengan Judul:

STUDI ANALISIS *FORENSIC* PADA PERANGKAT GPS (*Global Positioning System*)

Menyatakan dengan sesungguhnya bahwa seluruh isi tulisan atau karya tugas akhir ini adalah hasil saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya tugas akhir ini adalah bukan hasil tugas akhir yang diajukan sebagai karya sendiri, saya siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 29 Agustus 2014

Yang membuat pernyataan

(Bilal Abdussalam)

HALAMAN PERSEMBAHAN

Untuk Allah SWT

Rasa syukur yang selalu hamba ucapkan kepada-Mu untuk segala nikmat, kemudahan serta kesehatan yang telah engkau berikan, sehingga tugas akhir ini dapat terselesaikan.

Untuk Umi dan Abah

Terima kasih abah dan umi yang selalu memberikan dukungan penuh dan do'a restu terhadap anaknya ini. Kasih saying yang tiada batasnya sehingga bilal bisa menyelesaikan tugas akhir ini.

Ketiga adikku, Achmad Naufal, Fathurrahman dan Rizky Dermawan

terima kasih untuk keluarga besar tercinta yang tiada bosan-bosannya memberikan semangat serta dukungan sehingga saya bisa terdorong dan termotivasi dalam mempercepat pengerjaan tugas akhir ini.

Teman-teman

Terima kasih atas bantuan, kritik dan saran, dorongan, serta penyemangat penulis yang sangat membantu dalam penyelesaian tugas akhir ini, dan terima kasih telah menemani saya dari awal pengerjaan ini hingga selesai.

HALAMAN MOTTO

Jadilah orang yang bermanfaat bagi orang-orang yang ada disekitarmu.

Kunci dari kesuksesan adalah berani, jangan sampai keberanianmu terkalahkan oleh ketakutanmu.

Jadilah dirimu sendiri jangan menjadi diri orang lain.

"Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum sebelum mereka mengubah keadaan diri mereka sendiri"
(Q.S Ar-Rad: 12)

"Ya Allah, lapangkanlah dadaku, dan mudahkanlah untukku urusanku, dan lepaskanlah kekakuan lidahku. Agar mereka mengerti perkataanku"
(Q.S At-Taha 25-18)

KATA PENGANTAR



Assalamualaikum Wr. Wb

Alhamdulillah puji syukur ke hadirat Allah SWT yang telah memberikan rahmat, hidayah serta inayahnya, sehingga kita semua masih bisa menghirup udara yang tiada batasnya sampai saat ini. Serta tidak lupa pula shalawat dan salam selalu disanjungkan kepada junjungan Nabi besar, Nabi Muhammad SAW yang telah menyebarkan dan membawa islam dari zaman jahiliah menuju zaman yang terang benderang seperti sekarang ini. Sehingga atas ridho-Nya tugas akhir yang berjudul **"Studi Analisis *Forensic* pada Perangkat GPS(*Global Positioning System*)"** dapat diselesaikan. Tugas akhir ini merupakan syarat terakhir yang harus ditempuh untuk menyelesaikan pendidikan pada jenjang Strata Satu (S1), pada jurusan Teknik Informatika Universitas Islam Indonesia.

Sebagai makhluk yang hidup bermasyarakat yang tidak luput dari bantuan orang lain, penulis mengucapkan banyak terimakasih yang sebesar-besarnya karena telah banyak membantu dalam penyusunan tugas akhir ini, ucapan terima kasih penulis ucapkan kepada:

1. Allah SWT atas semua berkah, rahmat, hidayah, serta inayah-Nya sehingga tugas akhir ini dapat terselesaikan.
2. Keluarga besar tercinta, Ibu, Ayah, dan ketiga adikku. Terima kasih atas doa, semangat, nasihat dan dukungan yang telah diberikan selama pembuatan tugas akhir ini.
3. Yang saya hormati Bapak Ir. Gumbolo H.S.,M.Sc selaku Dekan Fakultas Teknologi Industri.
4. Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia Bapak Hendrik, S.T., M.Eng.
5. Dosen pembimbing tunggal dalam penyusunan ini Bapak Yudi Prayudi, S.Si., M.Kom. yang telah memberikan bimbingan, pengetahuan, pencerahan, nasehat, waktu dan ilmunya sehingga penyusunan tugas akhir ini dapat terselesaikan.

6. Seluruh Bapak/Ibu dosen di Jurusan Teknik Informatika Universitas Islam Indonesia. Semoga ilmu yang telah diajarkan dapat menjadi amal jariyah dan berguna bagi penulis. Amin.
7. Teman-teman angkatan 2010 (SOLITAIRE), teman-teman kelas D dan khususnya untuk seluruh teman-teman kost tumaritis angga, anjar, gega, rio, ardi, alex, ghulam, eko, kholid, ardi, fajar, riri, alpan, rento, banta, dewo, rendra, dan terimakasih juga kepada liza, riza yang sudah banyak membantu dan mendoakan saya sampai tugas akhir ini terselesaikan.
8. Bapak Hamid, S.T., M.T., & Bapak Fietyata Yudha S.Kom. yang telah banyak membantu serta meluangkan waktunya untuk memberikan pencerahan, saran serta pengetahuan dalam pengerjaan skripsi ini.
9. Teman-teman UII Cyber Guard yang selalu membuat saya termotivasi dengan dorongan serta dukungan kalian.
10. Teman-teman KKN Unit 41 Klaten, dan ibu posko yang telah memberikan do'a yang penuh sehingga tugas akhir ini dapat terselesaikan.
11. Semua pihak yang telah membantu dalam pembuatan sehingga terselesaikannya tugas akhir ini, yang tidak dapat disebutkan satu per satu oleh penulis.

Sebagai manusia biasa, penulis tidak pernah luput dari kesalahan, dan kesempurnaan, sehingga dalam penyusunan tugas akhir ini masih banyak terdapat kekeliruan dan kekurangan. Tak lupa bagi para pembaca untuk dapat memberikan kritik dan saran yang bersifat membangun untuk memperbaiki tugas akhir ini semoga bermanfaat bagi penulis khususnya dan pembaca pada umumnya.

Wassalamualaikum Wr. Wb.

Yogyakarta, 29 Agustus 2014

Bilal Abdussalam

SARI

Perannya sebagai alat navigasi tercanggih saat ini, kerapkali sering dilupakan bahwa GPS juga berpontesi menyimpan barang bukti pada suatu kasus. Seperti contohnya kasus pencurian mobil. Dalam penelitian ini dapat diambil permasalahan yaitu bagaimana cara mengungkap suatu kasus yang melibatkan GPS dan menganalisis menggunakan *tools* forensik yang tepat. Dengan tujuan penelitian untuk mempelajari, menganalisis dan mencari *tools* yang tepat dengan menggunakan cara forensik yang efektif dan efisien dan dapat dihasilkan manfaat dari penelitian yaitu memberikan pengetahuan terkait ilmu forensik khususnya GPS forensik serta *tools* yang digunakan untuk analisis forensik.

Dalam penelitian ini, penyelidikan terhadap barang bukti akan dimulai dengan *write blocking*, membuat file *backup* pada GPS serta menganalisis hasil *backup*. Membuat file *backup* dapat dilakukan dengan menggunakan *Oxygen Forensic Suite* untuk melakukan perbandingan dalam hasil *backup tools* yang digunakan yaitu *MOBILedit* File hasil *backup* akan dianalisis menggunakan kedua *tools backup* tersebut.

Hasil dari penelitian tugas akhir ini adalah suatu laporan yang berisi hasil analisis pada GPS *device* dari bukti digital yang tersimpan pada *internal storage* dan informasi mengenai keunikan dari GPS yang dianalisis dibandingkan perangkat GPS lainnya.

Kata kunci: Write Blocking, Backup, Storage, Forensic, GPS

TAKARIR

Write blocking	memblokir penulisan
Backup	membuat cadangan data.
Ekstract	ekstrak
Storage	media penyimpanan
Digital evidence	bukti digital
Internal memory	media penyimpanan dalam
Connector	aplikasi penghubung
Device	perangkat
File	berkas
Route	rute
Waypoint	titik jalan
Track point	titik jalur
Log	catatan
Tool	alat

DAFTAR ISI

LEMBAR PENGESAHAN DOSEN PEMBIMBING ii

LEMBAR PENGESAHAN PENGUJI iii

LEMBAR PERNYATAAN KEASLIAN TUGAS iv

HALAMAN PERSEMBAHAN v

HALAMAN MOTTO vi

KATA PENGANTAR vii

SARI ix

TAKARIR x

DAFTAR ISI xi

DAFTAR GAMBAR xiv

DAFTAR TABEL xvi

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 2

1.3 Batasan Masalah 2

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 4

1.6 Review Penelitian 4

1.7 Metodologi Penelitian 6

1.8 Sistematika Penulisan 7

BAB II LANDASAN TEORI 8

2.1 Latar Belakang dan Sejarah Komputer Forensik 8

2.1.1 Definisi Komputer Forensik 9

2.1.2 Tujuan Komputer Forensik 10

2.1.3 GPS (Global Positioning System)....10
2.1.4 Fungsi GPS....11
2.1.5 Cara Kerja GPS....12
1.2.6 Cara Kerja Assisted GPS....14
2.2 GPS Forensik....17
2.2.1 Pengumpulan dan Penyitaan Barang Bukti....17
2.2.2 Dokumentasi di tempat kejadian perkara....17
2.2.3 Melakukan *backup* terhadap barang bukti....18
2.2.4 Analisis hasil *backup* data terhadap barang bukti *(evidence)*....18
2.3 Tools GPS Forensik....18
2.3.1 Google Earth Free Edition....18
2.3.2 Oxygen Forensic suite....18
2.3.3 MOBILedit....19
2.3.4 SQLite....19
BAB III METODOLOGI....20
3.1 Diagram Alur Penelitian....20
3.2 Studi dan Pengumpulan Data....20
3.2.1 Spesifikasi GPS Garmin....21
3.2.2 Karakteristik GPS....22
3.2.3 Tahapan-tahapan pada komputer forensik....22
3.3 Skenario Kasus....24
3.4 Tahapan GPS Forensik....25
3.4.1 Pengumpulan Barang Bukti....25
3.4.2 Write Blocking dan Backup data....26
3.4.3 Analisis....26
3.4.4 Laporan Hasil dan Presentasi....26
3.5 Analisis Umum GPS Forensik....27
3.6 Kesimpulan....27
BAB IV HASIL DAN PEMBAHASAN....28
4.1 Skenario Pengujian....28
4.2 Asumsi Awal Data Digital....32
4.3 Akuisisi....32

4.3.1 Pengumpulan Barang Bukti 32
4.3.2 Write Blocking dan Backup Data 33
4.3.3 Verifikasi Hasil *Backup* dengan Alat Bukti 37
4.4 Analisis Kasus 38
4.4.1 Analisis Menggunakan *Oxygen Forensic Suite* 38
4.4.2 Analisis Menggunakan *MOBILedit* 43
4.4.3 Analisis Menggunakan *Google Earth* 44
4.4.4 Analisis Menggunakan SQLite 48
4.5 Laporan Hasil Penyelidikan 49
4.6 Presentasi 50
BAB V KESIMPULAN DAN SARAN 53
5.1 Kesimpulan 53
5.2 Saran 54
DAFTAR PUSTAKA 55

DAFTAR GAMBAR

Gambar 1. 1 Bukti digital dari GPS device Navman.....5
Gambar 2. 1 Cara Kerja GPS.....12
Gambar 2. 2 Cara Kerja Assisted GPS.....15
Gambar 3. 1 Diagram Alur Metodologi Penelitian.....20
Gambar 3. 2 Spesifikasi Garmin Nuvi 3592LM.....22
Gambar 3. 3 Tahapan Komputer Forensik (Sulianta, 2008). 23
Gambar 4. 1 Skema Kejahatan.....29
Gambar 4. 2 About Garmin Nuvi 3592LM 30
Gambar 4. 3 Fitur Where To 31
Gambar 4. 4 Bentuk Fisik GPS Garmin Nuvi 3592LM 31
Gambar 4. 5 Evidence Form 33
Gambar 4. 6 Membuat write protect 34
Gambar 4. 7 Peringatan write protection.....35
Gambar 4. 8 Form Backup Oxygen Forensic Suite 35
Gambar 4. 9 Select Physical dump 36
Gambar 4. 10 Export Report hasil Backup 36
Gambar 4. 11 Hasil backup menggunakan MOBILedit 37
Gambar 4. 12 Struktur file hasil backup Oxygen (kiri), struktur file alat bukti (tengah), struktur file hasil backup Mobiledit (kanan).....38
Gambar 4. 13 Langkah pengerjaan tahapan forensic.....38
Gambar 4. 14 Device Information pada GPS Garmin Nuvi 3592LM 40
Gambar 4. 15 Melihat isi file Current.gpx 40
Gambar 4. 16 Melihat isi file Position.gpx.....41
Gambar 4. 17 Melihat isi file database RecentStops.db 41
Gambar 4. 18 Melihat isi file database quick_search_list.db 42
Gambar 4. 19 Melihat isi file database pre.db 42
Gambar 4. 20 Melihat isi file database pre.db 43

Gambar 4. 21 Melihat isi file database pre.db 43
Gambar 4. 22 File Position.gpx pada Google Earth 44
Gambar 4. 23 Analisis file Current.gpx pada Google Earth.....44
Gambar 4. 24 Analisis file Current.gpx pada Google Earth.....45
Gambar 4. 25 Analisis file Current.gpx pada Google Earth.....45
Gambar 4. 26 Analisa file Current.gpx pada Google Earth 46
Gambar 4. 27 Analisa file Current.gpx pada Google Earth 46
Gambar 4. 28 Analisis file Current.gpx pada Google Earth.....47
Gambar 4. 29 Analisis track log menggunakan fasilitas tour.....47
Gambar 4. 30 Analisis file database RecentStops.db menggunakan SQLite .48
Gambar 4. 31 Analisis file database pre.db menggunakan SQLite 48
Gambar 4. 32 Analisis file database quick_search_list.db menggunakan SQLite 49

DAFTAR TABEL

Tabel 4. 1 Data Hasil Analisis 49
Tabel 4. 2 Tabel Perbandingan Tools 50
Tabel 4. 3 Tabel Hasil Analisis Bukti Digital Secara Umum 51

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi saat ini sangat pesat, terutama pada barang elektronik dan digital, penggunaan dan pemanfaatan komputer, *handphone*, GPS, dan lain-lain sebagai alat yang digunakan untuk mempermudah menjalankan aktivitas sehari-hari. Selain itu, barang elektronik juga dimanfaatkan untuk aktivitas kejahatan yang menggunakan barang elektronik. Oleh karena itu, komputer forensik atau digital forensik saat ini banyak dibutuhkan oleh pihak yang berwajib maupun penegak hukum untuk melakukan forensik dan identifikasi kasus dari barang elektronik yang telah menjadi barang bukti dan bisa dijadikan barang bukti yang sah di pengadilan.

Seiring perkembangan teknologi saat ini, banyak orang yang menggunakan alat-alat elektronik untuk mempermudah kegiatannya, salah satunya GPS *(Global Positioning System).* GPS adalah alat navigasi untuk menentukan posisi penggunanya yang langsung terhubung ke satelit sehingga GPS dapat memperhitungkan posisi kita berada di bumi. GPS dimulai dari awal tahun 1960-an saat Departemen Pertahanan (Dephan) Amerika Serikat karena merasa perlu memiliki sistem navigasi yang akurat, dapat berfungsi secara global, dalam segala cuaca, dan berbagai macam kelebihannya, saat ini sudah banyak perusahaan yang memproduksi GPS diantaranya, Garmin, TomTom, dan Magellan.

Beberapa kasus kejahatan di Indonesia yang pernah terjadi, yaitu dengan memanfaatkan GPS sebagai alat bantu untuk melacak suatu kejahatan, sebagai berikut:

- 2009: kasus perampokan Bank BNI di tol Bandara arah Cawang (Wiyatputera, 2010).

- 2013: 4/2 kasus pencurian mobil Toyota Avanza dengan plat B-1017 TOA, polisi menyelidiki kasus ini dengan memanfaatkan alat GPS yang ada pada mobil untuk memantau pergerakan mobil tersebut (Roby, 2014).
- 2013: kasus pencurian oleh oknum TNI, yaitu mobil Toyota Avanza dengan plat B-1713 UZU, Mobil ditemukan di Apartemen Cibubur, Village, Jakarta Timur, polisi dapat dengan mudah melacak pelaku dengan memantau alat GPS yang sudah terpasang pada mobil korban yang telah dicuri (Ariesant, 2013).

Oleh karena itu dari beberapa kasus diatas dapat disimpulkan bahwa GPS merupakan alat yang sangat membantu pihak berwajib dalam menyelesaikan kasus, dimana GPS dapat merekam seluruh lintasan yang pernah dilewati dan memberikan informasi tentang lokasi tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas, maka rumusan masalah pada penelitian ini adalah:

a. Bagaimana cara mengungkap suatu kasus yang melibatkan penggunaan GPS dan menganalisis barang bukti tersebut dengan menggunakan *tools* forensik yang efektif dan efisien.
b. Langkah seperti apa yang harusnya dilakukan untuk forensik barang bukti GPS agar dapat dijadikan barang bukti yang sah di pengadilan.
c. Keunikan apa yang ditemukan dalam menganalisis bukti digital yang terdapat pada GPS Garmin.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini sebagai berikut:

a. Melakukan forensik terhadap informasi yang ada pada *file log*, seperti:

1) *Track* adalah sekumpulan posisi dari perjalanan yang sedang atau sudah ditempuh. Biasanya digambarkan berupa garis pada GPS jika mengaktifkan fitur *display trip log*.
2) *Routes* adalah sekumpulan waypoint yang ingin dituju secara berurutan untuk mencapai suatu tujuan.
3) *Waypoints* adalah lokasi yang telah ditandai. Biasanya digambarkan berupa titik dan simbol (Sawitwatch, 2011).

b. GPS yang dianalisis adalah GPS produksi Garmin.

Ada beberapa *file* yang akan dianalisis dari barang bukti GPS Garmin, seperti:

1) *Current.gpx* adalah *file log* yang hanya berada pada GPS produksi Garmin yang berisi informasi *waypoint*, *trackpoint*, dan *route*.
2) *Postion.gpx* adalah file log yang berisi posisi koordinat terakhir pengguna GPS.
3) *pre.db* adalah file log database yang menyimpan informasi penting menyangkut hasil prediksi dari GPS yang memperhitungkan jarak dari lokasi awal untuk mencapai tujuan.
4) *quick_search_list.db* adalah file log database yang menyimpan informasi hasil pencarian dari beberapa tempat yang ingin dituju.
5) *RecentStops.db* adalah file log database yang menyimpan informasi dari GPS yang merekam di mana saja pengguna melakukan pemberhentian (LeMere, 2012).

1.4 Tujuan Penelitian

Tujuan penelitian tugas akhir ini adalah:

a. Mempelajari bagaimana melakukan identifikasi digital forensik yang efektif dan efisien pada GPS.
b. Mencari *tools* forensik dan *tools* pendukung lainnya untuk menyelesaikan kasus kejahatan yang melibatkan GPS.
c. Menganalisis GPS dengan menggunakan metode forensik yang efektif dan efisien.

1.5 Manfaat Penelitian

Manfaat penelitian tugas akhir ini adalah sebagai berikut:

a. Dapat mengetahui proses identifikasi, investigasi dan proses analisis pada GPS Garmin dengan menggunakan metode yang benar dalam forensik dan mengetahui *tools* yang efektif dan efisien untuk proses analisis dalam penelitian GPS forensik.
b. Dapat mengungkap dan menyelesaikan suatu kasus kejahatan pada GPS Garmin.
c. Memberikan pengetahuan terkait ilmu forensik khususnya GPS forensik serta *tools* yang digunakan untuk analisis forensik.
d. Memberikan pemahaman dalam menggunakan beberapa *tools* forensik untuk forensik GPS dalam penelitian ini.

1.6 Review Penelitian

Perkembangan teknologi saat ini dimanfaatkan oleh sebagian orang untuk melancarkan aksi kejahatan dengan menggunakan sarana pendukung seperti *smartphone*, komputer, GPS, dan sarana pendukung lainnya. Perangkat GPS yang paling banyak digunakan dikalangan masyarakat adalah perangkat GPS pada mobil, karena pada GPS memiliki navigator, maka ketika kendaraan yang memiliki GPS tersebut digunakan untuk kejahatan atau untuk melakukan tindak kriminal, akan terdapat catatan atau *log* pada GPS tersebut yang nantinya akan digunakan sebagai barang bukti dan dilakukan forensik terhadap barang bukti GPS tersebut.

Investigasi GPS forensik ini bergantung pada teknik forensik yang menggunakan keahlian komputer dan pengetahuan tentang navigasi yang nantinya akan menghasilkan data berharga kepada para penyidik. Selain itu GPS juga dapat memberikan informasi yang *real-time* dan *up-to-date* untuk pengendara yang membutuhkan bantuan informasi tempat-tempat seperti Pom Bensin, ATM, Bank, dan lainnya. Oleh karena itu diperlukan proses forensik tersendiri untuk mengungkap bukti yang tersimpan di dalam GPS. Sejumlah penelitian mengenai GPS forensik telah dilakukan oleh beberapa peneliti sebelumnya, diantaranya:

- Cusack, B., & Simms, M (2011), telah melakukan penelitian *recovery* data dari GPS *device*, dalam penelitiannya ada empat unit GPS yang digunakan, yaitu Navman MY-50, Navman S-90i, Navman C 40, dan Navman F20, tujuan dari penelitian ini adalah untuk mengungkap detail teknik yang relevan terhadap penyidik. Brian Cusack dan Mark Simms menggunakan *tools* FTK *Imager* dan EnCase *Forensic* untk membantu proses forensik seperti *imaging*, ekstraksi, analisis, dan pelaporan, berikut adalah hasil analisis bukti digital pada empat perangkat Navman tersebut:

Potential Evidence By GPS Device Model			
Navman S90i	**Navman MY50**	**Navman C40**	**Navman F20**
MyRoute.xml	MyRecentLocations.xml	MyRoute.xml	ROUTE.DAT
MyRecentLocations.xml	MyFavouriteLocations.xml	MyRecentLocations.xml	FAVVER4.DAT
MyFavouriteLocations.xml	MyMileage001 - MyMileage008.xml	MyFavouriteLocations.xml	RECENT.DAT
LOG001 to LOG010.log	LOG001 - LOG002.log	No log files as logging is turned off on this device	
DWRecentPlace.xml			
DWRecentRoad.xml			

Gambar 1. 1 Bukti digital dari GPS device Navman

- Lain halnya dengan penelitian yang dilakukan Mathia, T. N (2009), yaitu melakukan pemeriksaan forensik pada perangkat GPS, dalam penelitiannya Mathia, T. N(2009) juga melakukan proses forensik terhadap GPS TomTom yang terhubung dengan smartphone atau handphone, *file-file* yang dianalisis dari GPS TomTom dalam penelitian Mathia, yaitu: called.txt, callers.txt, contacts.txt, inbox.txt, outbox.txt, TTGO.bif, settings.dat, dan direktori \itn\. Selain itu Mathia juga menganalisis *file* berekstensi ".cfg", file ".cfg" tersebut adalah *file* dimana semua data TomTom tersimpan, contohnya adalah alamat, nomor telepon, informasi perangkat, *recent destinations*, *favorites*, dan lainnya.

1.7 Metodologi Penelitian

Metode-metode yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Studi dan Pengumpulan data

Pada suatu kasus, barang bukti digital adalah barang yang telah digunakan pada kasus kejahatan dengan melibatkan alat yang telah menjadi barang bukti tersebut. Karena barang bukti digital yang telah disita oleh penyidik tidak diperbolehkan untuk diforensik secara fisik melainkan hasil *image* dari barang bukti yang asli, dari hasil *image* itu penyidik diperkenankan untuk menganalisis, yang nantinya dari analisis tersebut penyidik mendapatkan bukti-bukti akurat dan bisa dijadikan barang bukti yang sah di pengadilan. Sebelum melakukan serangkaian proses forensik, diperlukan adanya pengumpulan data terkait proses penyelidikan GPS forensik yang bersumber baik dari internet, buku maupun sumber lainnya guna untuk mempermudah penelitian ini.

b. Uji coba, *back up* dari GPS Garmin

Setelah dilakukannya pengumpulan data, tahapan selanjutnya adalah uji coba dan implementasi pengujian simulasi penggunaan GPS Garmin sebagai alat yang digunakan untuk tindak kejahatan, serta memproses GPS Garmin tersebut untuk dijadikan barang bukti oleh penyidik dengan membuat *backup data* lalu menganalisanya.

c. Analisis Data

Melakukan analisis data terhadap hasil *image* dari GPS Garmin tersangka dengan menggunakan *tools* forensik. Sehingga dari proses analisis data hasil *image*, akan mendapatkan data-data terkait kasus tersebut serta menyelidiki sejauh mana penggunaan GPS Garmin dalam melaksanakan tindak kejahatan.

1.8 Sistematika Penulisan

Sistematika penulisan pada laporan tugas akhir ini berguna untuk mempermudah dalam memahami laporan tugas akhir ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, review penelitian, serta manfaat dari penelitian, metodologi dan sistematika penulisan yang diangkat sebagai materi dalam tugas akhir ini.

BAB II LANDASAN TEORI

Membahas mengenai dasar-dasar teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan terkait dengan GPS forensik dan konsep yang diterapkan pada GPS Forensik yang akan digunakan dalam penelitian.

BAB III METODOLOGI

Memuat uraian tentang studi literatur mengenai permodelan uji coba serta langkah-langkah uji coba proses investigasi forensik.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang proses pengujian, berupa *print screen* serta penjelasan data yang didapat dari hasil forensik, lalu menganalisa data tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini memuat rangkuman kesimpulan dari seluruh hasil penelitian dan berisi saran-saran yang perlu diperhatikan.

BAB II

LANDASAN TEORI

2.1 Latar Belakang dan Sejarah Komputer Forensik

Kemajuan teknologi merupakan suatu hal yang sangat menarik perhatian sebagian kalangan, perkembangannya yang sangat pesat telah melahirkan dimensi lain dari teknologi, yaitu kejahatan dengan sarana komputer sebagai alat yang membantu melancarkan aksi kejahatan, yang biasanya disebut dengan istilah *cybercrime.*

Pada awal tahun 1970-an Kongres Amerika Serikat mulai merealisasikan kelemahan hukum yang ada pada saat itu serta mencari solusi terbaru agar penyelesaian kejahatan komputer bisa lebih cepat. US *Federals Rules of Evidence* 1976 menyatakan permasalahan tersebut. Hukum lainnya yang berkaitan dengan permasalahan tersebut adalah:

a. *Economic Espionage Act* 1996, hukum yang berhubungan dengan pencurian rahasia dagang.
b. *The Electronic Communications Privacy Act* 1986, hukum yang berkaitan dengan penyadapan peralatan elektronik.
c. *The Computer Security Act* 1987 (*Public Law* 100-235), hukum yang berkaitan dengan keamanan sistem komputer pemerintahan (Syafa'at, 2007).

Semakin bertambahnya pengguna internet atau komputer yang juga merupakan salah satu sarana bagi penjahat *cyber* dalam melakukan kejahatannya, berbagai permasalahan baru muncul, yaitu bertambahnya kasus-kasus yang terkait dengan kejahatan internet atau komputer. Setidaknya pada saat ini terdapat 15 kategori aktivitas *cybercrime*, antara lain adalah *hacking*, *carding*, pencurian identitas, pornografi dan prostitusi, penyebaran virus, pencurian dana, dan *worm*, hampir 85% pengguna komputer dan internet pernah memiliki pengalaman buruk sebagai korban dari salah satu aktivitas *cybercrime* (Prayudi, 2013).

2.1.1 Definisi Komputer Forensik

Menurut Judd Robin, penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin. Terkait dengan teori yang dikemukakan oleh Robin tersebut, *New Technologies* mengungkapkan bahwa, komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik (Utdirartatmo, 2005).

Definisi komputer forensik adalah proses ilmiah dalam melakukan penemuan, pencarian, analisis dan pengumpulan barang bukti dari suatu sistem komputer dengan sebuah standard dan dokumentasi tertentu untuk dapat diajukan sebagai bukti hukum yang sah (Sinambela, 2011).

Komputer forensik juga dapat diartikan setiap aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan, penyaringan dan dokumentasi serta interpretasi bukti pada media sistem komputer, investigator forensik melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal, metode-metode yang digunakan untuk:

a. Penemuan informasi atau data pada sistem komputer
b. Pengembalian (*recovery file*) yang sudah dihapus, enkripsi, atau mengalami kerusakan.
c. Monitoring aktifitas seseorang.
d. Mendeteksi pelanggaran terhadap kebijakan (*policy*) perusahaan (Sinambela, 2011).

Dapat diambil kesimpulan bahwa komputer forensik adalah suatu rangkaian prosedur dalam pengumpulan bukti-bukti berbasis digital maupun fisik agar dapat dipergunakan sebagai barang bukti yang sah di pengadilan.

2.1.2 Tujuan Komputer Forensik

Tujuan utama dari komputer forensik, yaitu:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi atau entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan.
2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud (Indrajit, 2011).

2.1.3 GPS (Global Positioning System)

GPS (*Global Positioning System*) adalah sebuah sistem navigasi *global* berbasis satelit GNNS(*Global Navigation Satellite System*) yang dikembangkan oleh Departemen Pertahanan Amerika Serikat. Sistem ini adalah system yang pertama kali dan satu-satunya sistem pemetaan didunia yang berfungsi secara penuh saat ini dan dapat digunakan setiap saat oleh semua orang didunia secara gratis, oleh karena itu nama GPS menjadi terkenal dengan sebutan alat navigasi berbasis satelit. Sistem ini menggunakan beberapa kelompok satelit yang diberi nama NAVSTAR (*Navigational Satellite Timing and Ranging*).

Ada beberapa sistem navigasi global lainnya yang berbasis satelit yang dikembangkan oleh beberapa negara, yaitu: Galileo yang dikembangkan oleh Uni Eropa dan GLONASS (*Global Orbiting Navigation Satellite System*) yang dikembangkan oleh Rusia. Kedua system ini masih belum berfungsi secara penuh karena belum semua satelitnya tersedia di orbit bumi. Bila semua satelit yang diperlukan sudah mengudara, maka kedua system ini akan mulai berfungsi secara penuh. Walaupun begitu, beberapa alat genggam penerima sinyal dari sistem-sistem ini sudah mulai dipasarkan.

Tidak mudah untuk menemukan alat-alat navigasi berbasis satelit yang dapat menerima sinyal satelit Galileo ataupun GLONASS, hampir semua yang dijual di pasar adalah alat navigasi yang hanya dapat menerima sinyal satelit NAVSTAR GPS (*Navigational Satellite Timing and Ranging Global Positioning System*). Hal ini juga mendorong masyarakat dan produsen untuk memakai nama "GPS" bagi semua alat navigasi berbasis satelit (MHP, 2011).

Sistem GPS yang nama aslinya NAVSTAR GPS mempunyai tiga segmen yaitu: satelit, pengontrol dan penerima atau pengguna. Satelit GPS yang mengorbit bumi, dengan orbit dan kedudukan yang tetap (koordinatnya pasti), seluruhnya berjumlah 24 buah dimana 21 buah aktif bekerja dan tiga buah sisanya adalah cadangan (Nugroho, 2012).

2.1.4 Fungsi GPS

Fungsi GPS dalam kehidupan sehari-hari sangat diperlukan dalam menentukan arah dalam perjalanan, selain itu GPS dapat digunakan dalam hal yang lainnya, seperti:

a. Militer

GPS digunakan untuk keperluan perang, seperti menuntun arah bom, atau mengetahui posisi pasukan berada. Dengan cara ini maka kita bisa mengetahui mana teman mana lawan untuk menghindari salah target, ataupun menetukan pergerakan pasukan.

b. Navigasi

GPS banyak juga digunakan sebagai alat navigasi seperti kompas. Beberapa jenis kendaraan telah dilengkapi dengan GPS untuk alat bantu nivigasi, dengan menambahkan peta, maka bisa digunakan untuk memandu pengendara, sehingga pengendara bisa mengetahui jalur mana yang sebaiknya dipilih untuk mencapai tujuan yang diinginkan.

c. SIG (Sistem Informasi Geografis)

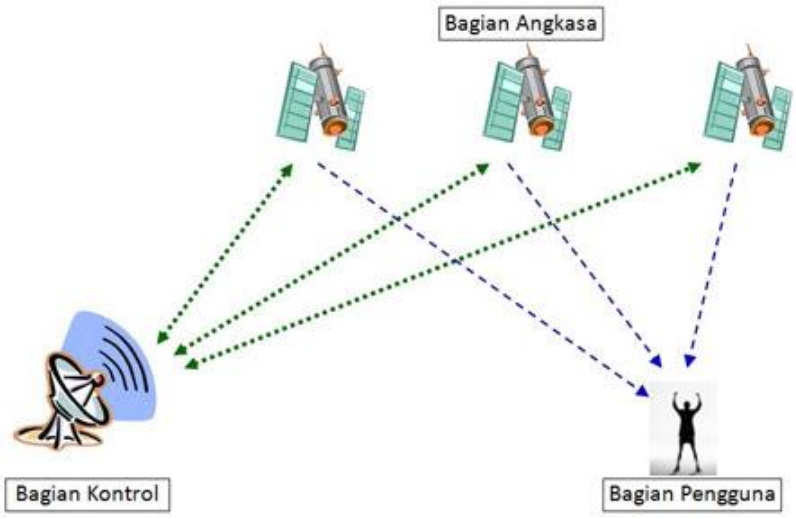
Untuk keperluan Sistem Informasi Geografis, GPS sering juga diikutsertakan dalam pembuatan peta, seperti mengukur jarak perbatasan, ataupun sebagai referensi pengukuran.

d. Pemantau Gempa

Bahkan saat ini, GPS dengan ketelitian tinggi bisa digunakan untuk memantau pergerakan tanah, yang ordenya hanya mm dalam setahun. Pemantauan pergerakan tanah berguna untuk memperkirakan terjadinya gempa, baik pergerakan vulkanik ataupun tektonik (Nugroho, 2012).

2.1.5 Cara Kerja GPS

Sistem ini menggunakan sejumlah satelit yang berada di orbit bumi, yang memancarkan sinyalnya ke bumi dan ditangkap oleh sebuah alat penerima. Ada tiga bagian penting dari sistem ini, yaitu bagian kontrol, bagian angkasa, dan bagian pengguna.



Gambar 2. 1 Cara Kerja GPS

a. Bagian Kontrol

Seperti namanya, bagian ini untuk mengontrol. Setiap satelit dapat berada sedikit diluar orbit, sehingga bagian ini melacak orbit satelit, lokasi, ketinggian,

dan kecepatan. Sinyal-sinyal sari satelit diterima oleh bagian kontrol, dikoreksi, dan dikirimkan kembali ke satelit. Koreksi data lokasi yang tepat dari satelit ini disebut dengan data *ephemeris*, yang nantinya akan dikirimkan kepada alat navigasi kita.

b. Bagian Angkasa

Bagian ini terdiri dari kumpulan satelit-satelit yang berada di orbit bumi, sekitar 12.000 mil diatas permukaan bumi. Kumpulan satelit-satelit ini diatur sedemikian rupa sehingga alat navigasi setiap saat dapat menerima paling sedikit sinyal dari empat buah satelit. Sinyal satelit ini dapat melewati awan, kaca, atau plastik, tetapi tidak dapat melewati gedung atau gunung.

Satelit mempunyai jam atom, dan juga akan memancarkan informasi waktu atau jam ini. Data ini dipancarkan dengan kode *pseudo-random*. Masing-masing satelit memiliki kodenya sendiri-sendiri. Nomor kode ini biasanya akan ditampilkan di alat navigasi, maka kita bisa melakukan identifikasi sinyal satelit yang sedang diterima alat tersebut. Data ini berguna bagi alat navigasi untuk mengukur jarak antara alat navigasi dengan satelit, yang akan digunakan untuk mengukur koordinat lokasi.

Walaupun tidak berhubungan langsung, kekuatan sinyal satelit juga akan membantu alat dalam penghitungan. Kekuatan sinyal ini lebih dipengaruhi oleh lokasi satelit, sebuah alat akan menerima sinyal lebih kuat dari satelit yang berada tepat diatasnya (bayangkan lokasi satelit seperti posisi matahari ketika jam 12 siang) dibandingkan dengan satelit yang berada di garis cakrawala (bayangkan lokasi satelit seperti posisi matahari terbenam/terbit).

Ada dua jenis gelombang yang saat ini dipakai untuk alat navigasi berbasis satelit pada umumnya, yang pertama lebih dikenal dengan sebutan L1 pada 1575.42 MHz. Sinyal L1 ini yang akan diterima oleh alat navigasi. Satelit juga mengeluarkan gelombang L2 pada frekuensi 1227.6 Mhz. Gelombang L2 ini digunakan untuk tujuan militer dan bukan untuk umum.

c. Bagian Pengguna

Bagian ini terdiri dari alat navigasi yang digunakan. Satelit akan memancarkan data almanak dan ephemeris yang akan diterima oleh alat navigasi secara teratur. Data almanak berisikan perkiraan lokasi (*approximate location*) satelit yang dipancarkan terus menerus oleh satelit. Data *ephemeris* dipancarkan oleh satelit, dan valid untuk sekitar 4-6 jam.

Untuk menunjukkan koordinat sebuah titik (dua dimensi), alat navigasi memerlukan paling sedikit sinyal dari tiga buah satelit. Untuk menunjukkan data ketinggian sebuah titik (tiga dimensi), diperlukan tambahan sinyal dari sebuah satelit lagi. Dari sinyal-sinyal yang dipancarkan oleh kumpulan satelit tersebut, alat navigasi akan melakukan perhitungan-perhitungan, dan hasil akhirnya adalah koordinat posisi alat tersebut. Makin banyak jumlah sinyal satelit yang diterima oleh sebuah alat, akan membuat alat tersebut menghitung koordinat posisinya dengan lebih tepat (MHP, 2011).

1.2.6 Cara Kerja Assisted GPS

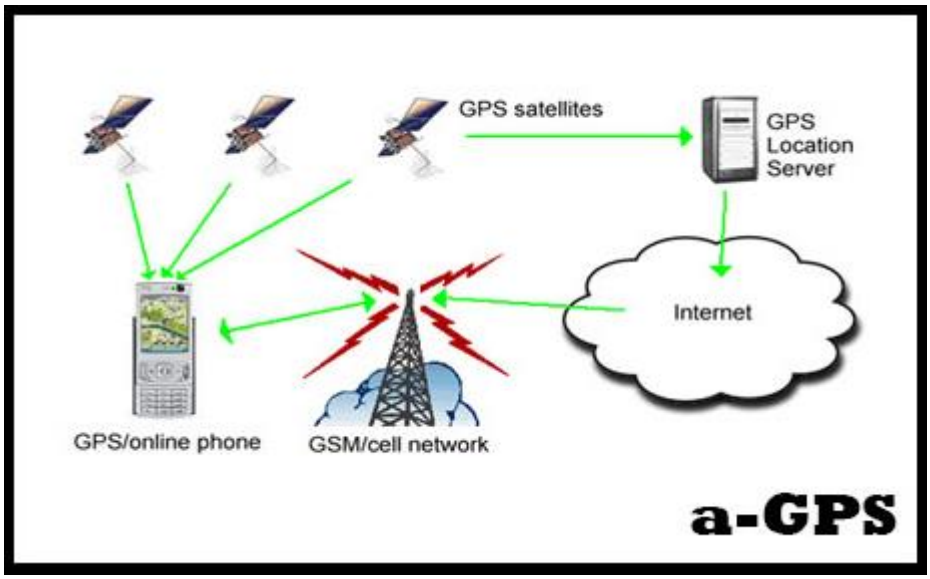
Perangkat GPS menangkap 3 sinyal dari 24 satelit GPS yang ada di luar angkasa. Perangkat GPS kemudian melakukan perhitungan jarak ke setiap satelit. Dari perhitungan itu, perangkat GPS kemudian mengetahui posisi pemegangnya. Supaya perangkat GPS bisa menangkap sinyal dengan baik, perangkat harus berada di luar ruangan, bahkan harus dibawah langit terbuka. Kekuatan sinyal bisa berkurang kalau perangkat GPS berada di bawah pohon, dibawah gedung-gedung pencakar langit atau di dalam kendaraan. Sinyal hampir bisa dipastikan menghilang kalau pembawa perangkat GPS masuk ke dalam gedung. Itulah kelemahan GPS. Makanya, muncullah perbaikan untuk masalah itu. Ialah A-GPS, perbaikannya. A-GPS adalah kependekan dari Assisted-GPS. A-GPS adalah merupakan pengembangan dari GPS.

Karena sinyal handphone bisa menembus ke dalam ruangan, masalah yang dihadapi oleh GPS bisa pun teratasi.Assisted Global Positioning System (A-GPS) akan membantu perangkat Anda menemukan satelit. Saat menggunakan A-GPS, perangkat Anda akan menerima informasi satelit dari server data melalui jaringan

seluler. Apabila perangkat Anda tidak menerima data tersebut, perangkat akan mencoba mendeteksi satelit lain. Dengan bantuan data tersebut, perangkat Anda akan mendeteksi satelit yang tepat, di saat satelit berada di sisi yang sama pada planet dengan perangkat Anda.A-GPS mempercepat penandaan kalkulasi lokasi.

A-GPS didesain untuk memungkinkan perangkat dalam mendapatkan sinyal satelit lebih cepat dan dapat dipercaya daripada dengan GPS standalone. Sebagai contoh, positioning dilakukan lebih cepat dalam keadaan cold-start, yaitu, saat koneksi GPS telah dimatikan dalam waktu yang lama, atau apabila pengguna melakukan perjalanan ke negara yang berbeda. Dengan A-GPS, waktu perkiraan untuk membangun koneksi GPS menurun secara signifikan. A-GPS menurunkan waktu yang diperlukan umumnya puluhan detik.

A-GPS Merupakan teknologi yang menggunakan server bantuan untuk memotong waktu yang dibutuhkan untuk menentukan lokasi (pinpointed) penggunaan GPS. A-GPS membutuhkan 3 komponen dalam proses penentuan posisi, yaitu Satelit, Assistance Server (GSM), Receiver A-GPS, cara kerja Assisted GPS dapat dilihat pada Gambar berikut:



Gambar 2. 2 Cara Kerja Assisted GPS

Server bantuan penyedia data informasi satelit yang dibutuhkan oleh sistem GPS biasanya di supply oleh jaringan operator dengan menggunakan jalur GPRS. Server ini memiliki satelit dengan sinyal yang sangat baik dan mampu melakukan perhitungan yang rumit untuk menentukan posisi handphone. Server itu juga bisa menyajikan data dari satelit GPS sehingga handphone terhubung dengan satelit kemudian menentukan lokasi handphone. Karena sinyal handphone bisa menembus ke dalam ruangan, masalah yang dihadapi oleh GPS bisa pun teratasi. Ketika berada di daerah-daerah yang tidak terjangkau oleh satelit seperti di bawah atap., A-GPS mengambil alih tugas mencari posisi chip GPS dalam handphone.

Karena A-GPS dan server bantuan berbagi tugas, maka proses akan lebih cepat dan lebih efisien dibanding GPS biasa walaupun semua proses itu tergantung pada cakupan jaringan. Keuntungan A-GPS adalah Pengidentifikasian lokasi yang lebih cepat, hanya membutuhkan power yang kecil untuk proses komputasi data, dan lebih hemat baterai. Sedangkan kekurangannya masih bergantung pada cakupan jaringan operator.

GPS mempunyai beberapa batasan yang juga berlaku pada A-GPS. Sebagai contoh, keberadaan dan kualitas sinyal dipengaruhi oleh bangunan, gangguan alam, kondisi cuaca, dan lokasi pengguna. A-GPS menggunakan koneksi jaringan seluler 3G dan 2G dan koneksi data paket GPRS dan EGPRS. Anda juga harus mempunyai titik akses internet yang ditentukankan dalam perangkat kompatibel Anda. A-GPS dapat digunakan di seluruh dunia, selama Anda memiliki akses ke jaringan seluler dan koneksi data. Anda juga dapat menggunakan layanan ini di luar jaringan lokal Anda (roaming). A-GPS tidak tergantung pada layanan operator yang spesifik (Steven, 2010).

2.2 GPS Forensik

Tahapan-tahapan yang akan dilakukan untuk melakukan forensik terhadap *device* GPS Garmin, yaitu:

2.2.1 Pengumpulan dan Penyitaan Barang Bukti

a. Pada tahapan ini penyidik harus melakukan penyitaan barang bukti di tempat kejadian perkara dengan surat-surat penyitaan yang telah dikeluarkan oleh pihak terkait.
b. Perangkat GPS dan perangkat elektronik pendukung lainnya yang digunakan oleh pelaku.
c. Dalam melakukan penyitaan dan pengumpulan barang bukti, penyidik harus memperhatikan tindakan pencegahan yang harus dilakukan agar barang bukti yang akan disita masih bersifat *original*:
    1) Pakailah sarung tangan dan alat pengaman lainnya, agar tidak mengganggu bukti dari sidik jari pelaku yang dimungkinkan ada pada fisik barang bukti.
    2) Berhati-hatilah dalam proses penyitaan barang bukti agar tidak merusak barang bukti asli.
    3) Penyimpanan barang bukti di tempatkan di dalam tas atau pembungkus khusus.
    4) Meletakkan barang bukti di tempat yang aman dari jangkauan pihak yang tidak berkepentingan dalam penanganan kasus ini.

2.2.2 Dokumentasi di tempat kejadian perkara

a. Mendokumentasikan semua informasi yang telah didapatkan dari hasil olah tempat kejadian perkara dengan sebanyak mungkin, serta mengambil foto dari seluruh barang bukti yang telah didapatkan dan seluruh keadaan di tempat kejadian.
b. Meletakkan hasil dokumentasi dan bukti-bukti di tempat yang aman dari jangkauan pihak yang tidak berkepentingan dalam penanganan kasus ini, untuk menjaga originalitas barang bukti.

c. Pastikan seluruh barang bukti dan tempat kejadian telah di dokumentasi.

d. Pemberian label pada setiap barang bukti sangatlah penting untuk mempermudah dalam mengidentifikasi setiap barang bukti.

2.2.3 Melakukan *backup* terhadap barang bukti

Proses *backup* data yaitu proses penyalinan data *original* dari barang bukti secara keseluruhan, agar dapat dilakukan proses analisis untuk mendapatkan bukti yang akurat.

2.2.4 Analisis hasil *backup* data terhadap barang bukti *(evidence)*

Melakukan proses analisis terhadap barang bukti dengan menggunakan *tools* forensik yang efektif dan efisien agar mendapatkan hasil yang akurat.

2.3 Tools GPS Forensik

Seorang analis forensik diharuskan untuk memiliki kemampuan dalam menjalankan berbagai *tools* yang memungkinkan untuk membantu dalam pengujian data, analisis data, dan pengumpulan bukti-bukti digital. Dalam penelitian ini ada beberapa *tools* yang digunakan untuk menganalisis barang bukti, yaitu:

2.3.1 Google Earth Free Edition

Google Earth merupakan suatu *software* terbitan dari perusahaan *google* berbasis *desktop*, berfungsi untuk pemetaan bumi yang bersumber dari Gambar dan dikumpulkan oleh pemetaan satelit, fotografi udara dan globe GIS 3D, yang berguna dalam melakukan proses pencarian lokasi *track point*, *waypoint*, koordinat, r*oute*, dan lainnya.

2.3.2 Oxygen Forensic suite

Oxygen forensic suite adalah salah satu *software* komputer forensik yang berguna untuk melakukan proses ekstraksi atau *backup* data serta menganalisis dan dapat mencari seluruh informasi yang terdapat pada barang bukti asli.

2.3.3 MOBILedit

MOBILedit adalah salah satu *software* komputer forensik yang berguna untuk melakukan proses *backup* data terhadap barang bukti smartphone maupun telepon genggam lainnya serta dapat menganalisis dan dapat mencari seluruh informasi terhadap bukti digital yang ada pada barang bukti. Untuk dapat melakukan *backup* dibutuhkan MOBILedit yang berbayar.

2.3.4 SQLite

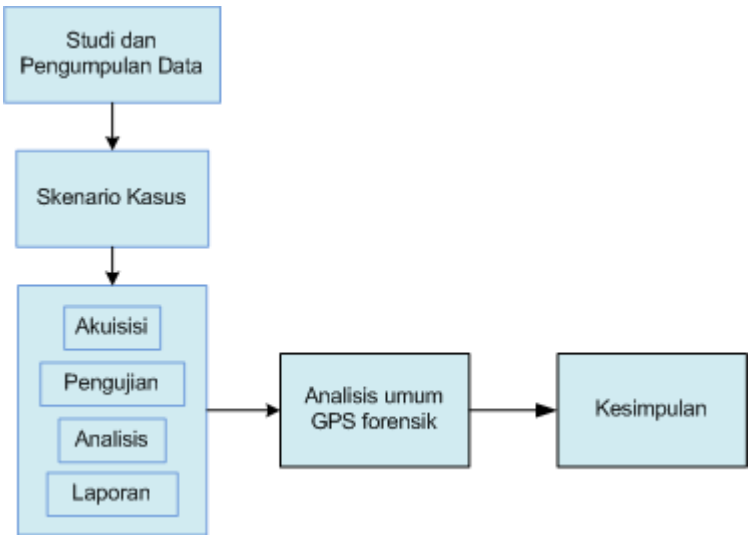
SQLite adalah salah satu *software* yang digunakan untuk membuat *database* dengan ukuran yang sangat kecil dan sangat cocok diimplementasikan pada perangkat android, *mobile*, dan sejenisnya. *Tools* ini akan digunakan untuk membaca file *database* log yang terdapat pada barang bukti.

BAB III

METODOLOGI

3.1 Diagram Alur Penelitian

Beberapa tahapan penelitian yang akan dilakukan, dapat dilihat pada Gambar 3.1 dibawah ini:



Gambar 3. 1 Diagram Alur Metodologi Penelitian

3.2 Studi dan Pengumpulan Data

Kemampuan yang dimiliki GPS dapat digunakan oleh pihak berwajib sebagai salah satu alat dalam membantu menindak suatu kasus kejahatan, dengan adanya GPS forensik akan ditemukan bukti-bukti digital seperti *track points*, *routes* dan *waypoints*. Namun untuk memperoleh bukti digital dari barang bukti yang telah disita maka diperlukan langkah-langkah tertentu untuk mendapatkan hasil yang akurat.

Dalam proses forensik digital, tidak diperbolehkan untuk melakukan forensik terhadap barang bukti secara langsung. Setelah barang bukti GPS disita oleh penyidik, penyidik diharuskan melakukan proses *backup* terlebih dahulu

untuk menjaga keaslian barang bukti dengan menggunakan *tools* forensik, yaitu *Oxygen forensic suite.*

Selanjutnya untuk melakukan pembuktian apakah hasil *backup* dari alat bukti masih original atau telah dimodifikasi, penyidik dapat membuat dua *backup* data dari GPS untuk dapat membuktikan jika alat bukti tersebut masih terjaga keasliannya.

Dari hasil *backup* barang bukti GPS tersebut, penyidik kemudian melakukan penyelidikan pada menggunakan *tools* forensik. *Tool* yang akan digunakan dalam penelitian ini adalah *Oxygen forensic suite* dan *MOBILedit*. *Oxygen forensic suite* digunakan untuk proses *backup* serta menyelidiki barang bukti secara keseluruhan dari hasil *backup*, barang bukti GPS yang telah disita dimata pengadilan sifatnya harus masih original dan menjadi barang bukti yang sah, penyidik hanya boleh menganalisis hasil *backup* dari barang bukti tersebut bukan barang bukti GPS aslinya. *Oxygen forensic suite* digunakan untuk menganalisa *internal memory* dari GPS tersebut.

3.2.1 Spesifikasi GPS Garmin

GPS Garmin adalah salah satu GPS yang diproduksi oleh salah satu perusahaan GPS, yaitu perusahaan Garmin, perusahaan ini memproduksi banyak jenis dan tipe GPS, salah satu jenisnya adalah GPS Otomotif, dan yang akan digunakan dalam penelitian ini adalah Garmin Nuvi 3592LM dengan spesifikasi seperti pada Gambar 3.2:

Physical & Performance:	
Unit dimensions, WxHxD:	5.4"W x 3.4"H x 0.5"D (13.8 x 8.7 x 1.3 cm)
Display size, WxH:	4.4"W x 2.5"H (11.1 x 6.3 cm); 5" diag (12.7 cm)
Display resolution, WxH:	800 x 480 pixels
Display type:	multi-touch, glass, dual-orientation, WVGA color TFT with white backlight
Weight:	262 g
Battery:	rechargeable lithium-ion
Battery life:	up to 2 hours
Video in:	yes (Up to 800x400 pixels)
Audio out:	yes
High-sensitivity receiver:	yes
Waterproof:	no

Maps & Memory:	
Preloaded street maps:	yes
Includes lifetime map updates:	yes
nüMaps Guarantee:	yes
3-D terrain view:	yes
3-D buildings and landmarks view:	yes
Built-in memory:	8G NAND flash
Accepts data cards:	microSD™ card (not included)
Waypoints/favorites/locations:	1000
Routes:	100

Gambar 3. 2 Spesifikasi Garmin Nuvi 3592LM

(Sumber: http://malaysiagps.com.my/site/index.php?cat=8&page=27)

3.2.2 Karakteristik GPS

Karakteristik dari GPS yaitu terletak pada penggunaan akurasi satelit yang selalu *up to date* dan setiap pergerakan pengguna akan terekam pada *track log*, oleh karena itu dalam penanganannya barang bukti GPS harus diamankan dengan peralatan khusus atau pelastik anti signal agar data yang ada pada *storage* GPS dapat terjaga dari perubahan data yang disebabkan oleh signal satelit.

3.2.3 Tahapan-tahapan pada komputer forensik

Pada Gambar 3.3, digambarkan bahwa terdapat empat fase dalam penanganan kasus komputer forensik, yaitu pengumpulan, pengujian, analisa, dan laporan, beserta objek yang dikelola dari setiap fase, yaitu media, data, informasi, dan barang bukti (Sulianta, 2008).



Gambar 3. 3 Tahapan Komputer Forensik (Sulianta, 2008).

a. Pengumpulan Data

Tahap ini adalah tahapan pertama dalam proses forensik komputer untuk pengumpulan media serta mengidentifikasi sumber-sumber potensial dan bagaimana data dari GPS Garmin dikumpulkan. Ada beberapa tahapan Pada Penanganan kasus GPS forensik sebagai berikut:

1) Identifikasi
2) Penamaan (*labeling*)
3) Perekaman (*recording*)
4) Mendapatkan data

b. Pengujian

Setelah melalui proses pengumpulan data, tahap selanjutnya adalah melakukan pengujian. Pada tahap ini proses pengujian dilakukan untuk mengekstraksi dan mengumpulkan banyak informasi-informasi dari data GPS terkait kasus yang ditangani.

Ada banyak *tools* yang akan digunakan pada proses ini. *Tools* yang akan digunakan yaitu *tools* yang bersangkutan dengan proses *backup* data dan proses membuat *image,* serta *tools* yang membantu dalam menyelidiki *image* dan *backup* data yang telah dibuat.

c. Analisa

Setelah proses pengujian, tahapan selanjutnya adalah penyidik melakukan analisis data dari hasil *image* dan *backup* data, analisa dilakukan dengan melakukan ekstrak data lalu dianalisis untuk merumuskan kesimpulan dan menggambarkan data.

d. Laporan

Pelaporan atau *reporting* adalah tahap akhir pada proses komputer forensik, pada tahap ini dilakukan representasi informasi dari hasil proses analisis.

3.3 Skenario Kasus

Maraknya tindak kriminal yang melibatkan barang bukti GPS merupakan salah satu alasan dibutuhkannya ahli forensik. Pada saat penyidik mendapatkan suatu kasus, dengan menggunakan analisis forensik akan didapatkan data-data seperti apa, siapa, bagaimana, dan kapan terjadinya tindak kriminal pada barang bukti yang didapatkan, untuk memperoleh bukti-bukti yang akurat harus melalui tahapan-tahapan forensik agar dapat mempermudah dalam melakukan proses penyelidikan, dibutuhkan beberapa *tools* untuk penyelesaiannya. Dalam uji coba kali ini, *tool* yang digunakan untuk proses *backup* data dari *memory internal* GPS yang telah diamankan yaitu menggunakan *Oxygen forensic suite* dan *MOBILedit*, setelah didapatkan hasil *backup* data langkah selanjutnya adalah menganalisis hasil backup tersebut dengan menggunakan *tools* seperti *Oxygen forensic suite*, *MOBILedit*, *Google Earth* dan *SQLite*. Dari *tools* tersebut didapatkan banyak informasi dan data yang ada pada barang bukti yang nantinya akan diungkap di pengadilan.

Pada penelitian ini dibuat sebuah skenario kasus, Telah ditemukan satu unit mobil dari tersangka berinisial AL yang terlibat kasus pebunuhan, tindakan kriminal yang dilakukannya yaitu pembunuhan dengan dasar balas dendam. Pada saat polisi melakukan olah TKP (Tempat Kejadian Perkara), polisi melakukan interogasi terhadap rekan-rekan satu kost korban, selanjutnya dari keterangan yang diperoleh didapatkan beberapa informasi bahwa pada saat sebelum kejadian

ada salah satu rekan korban yang datang ke kost korban, usut punya usut ternyata mobil yang digunakan AL adalah mobil sewaan, selanjutnya polisi melakukan pencarian terhadap tersangka dengan memanfaatkan GPS yang telah terpasang pada mobil sewaan tersebut. Setelah diselidiki melalui alat monitoring yang ada pada alat kontrol di tempat AL menyewa mobil, akhirnya ditemukan mobil sewaan yang terparkir di parkiran gedung kuliah, dan pada saat mobil tersebut ditemukan, tersangka AL sudah tidak ada di tempat. Selanjutnya polisi menyelidiki GPS yang terpasang di mobil tersangka untuk mendapatkan beberapa bukti digital yang akan dianalisis untuk mendapatkan beberapa lokasi yang telah dikunjungi oleh AL. Pada saat dilakukan analisis ada satu titik yang menunjukkan lokasi rumah AL. Polisi lalu melakukan penahanan terhadap AL. Diduga tersimpan data *log*, seperti *track points*, *routes* dan *waypoints* yang oleh tersangka digunakan untuk menunjukkan arah jalan mana saja yang dilalui, rute-rute mana saja yang pernah dilewati dan lokasi-lokasi mana saja yang pernah disinggahi, sehingga dari *log* tersebut dapat ditemukan jejak-jejak dari tersangka yang akan diselidiki lebih lanjut oleh pihak kepolisian dan akan dijadikan alat bukti di pengadilan.

3.4 Tahapan GPS Forensik

3.4.1 Pengumpulan Barang Bukti

Tahap awal yang harus dilalui adalah pengumpulan barang bukti sesuai dengan tahapan forensik pada Gambar 3.2. tahapan ini berfungsi untuk mengumpulkan sumber-sumber potensial pada barang bukti GPS dan bagaimana kemudian data-data tersebut dikumpulkan. Pada kasus ini, barang bukti GPS diambil sebagai barang bukti karena pada saat penyergapan pihak yang berwajib menemukan barang digital yang terdapat di TKP. Selanjutnya pihak yang berwajib menyerahkan ke tim forensik kepolisian melakukan pemeliharaan terhadap barang bukti agar data pada barang bukti masih terjaga keasliannya.

3.4.2 Write Blocking dan Backup data

Write Blocking dan *Backup* data merupakan serangkaian proses dalam tahap pengujian komputer forensik seperti Gambar 3.2. Data yang telah ditemukan nantinya akan diproses mulai dari proses duplikasi sampai dengan proses ekstraksi informasi dari data-data yang dikumpulkan.

a. *Write Blocking*

Pada saat proses *backup* data, teknik *write blocking* sangat diperlukan untuk menjaga keaslian data. *Device* yang terhubung langsung melalui komputer tanpa *write blocking* sangat dimungkinkan terjadinya perubahan data, seperti perubahan waktu akses pada *device* tersebut dan *hash* dari *device* tersebut akan berubah, oleh karena itu teknik *write blocking* dibutuhkan untuk menjaga integritas data supaya tidak terjadi perubahan.

b. *Backup* data GPS

GPS mempunyai media penyimpanan internal maupun external yang dapat menyimpan informasi mengenai koordinat *track*, *route* dan *waypoint*. Untuk mendapatkan data-data tersebut harus dilakukan *backup* data dengan memanfaatkan *tools Oxygen forensic suite*.

3.4.3 Analisis

Setelah proses pengujian skenario, tahapan selanjutnya adalah melakukan analisis data. Analisis data dilakukan dengan merumuskan kesimpulan dari data-data yang telah didapat melalui proses *backup* data yang sebelumnya telah dilakukan. Ada banyak data yang ditemukan pada saat proses analisis, untuk itu perlu dilakukan proses eliminasi dan pengalaman dalam menangani suatu kasus.

3.4.4 Laporan Hasil dan Presentasi

Pada tahap ini dilakukan pelaporan dari semua proses forensik terhadap barang bukti yang didokumentasikan dalam sebuah laporan. Laporan ini berisi tentang kesimpulan dari hasil analisis yang telah dilakukan sebelumnya. Setelah itu dilakukan presentasi oleh pihak penyidik yang berperan sebagai saksi ahli,

dimana dalam presentasi ini pihak penyidik menjelaskan secara garis besar semua penyelidikan dari hasil yang telah didapat.

3.5 Analisis Umum GPS Forensik

Setelah hasil dari pengujian telah dilakukan selesai dilakukan maka didapatkan *digital evidence* pada *internal storage* GPS *device*, selanjutnya barang bukti digital tersebut akan dianalisis untuk mendapatkan informasi yang akurat terhadap kasus yang sedang ditangani. Dari *digital evidence* tersebut didapatkan beberapa informasi jejak-jejak tersangka seperti catatan perjalanan tersangka yang akan dijadikan alat bukti di pengadilan.

3.6 Kesimpulan

Peneliti menjelaskan kesimpulan yang didapat selama masa penelitian baik dari keunikan maupun keuntungan dalam melakukan forensik pada perangkat GPS sampai hasil analisis berdasarkan penelitian-penelitian sebelumnya.

BAB IV

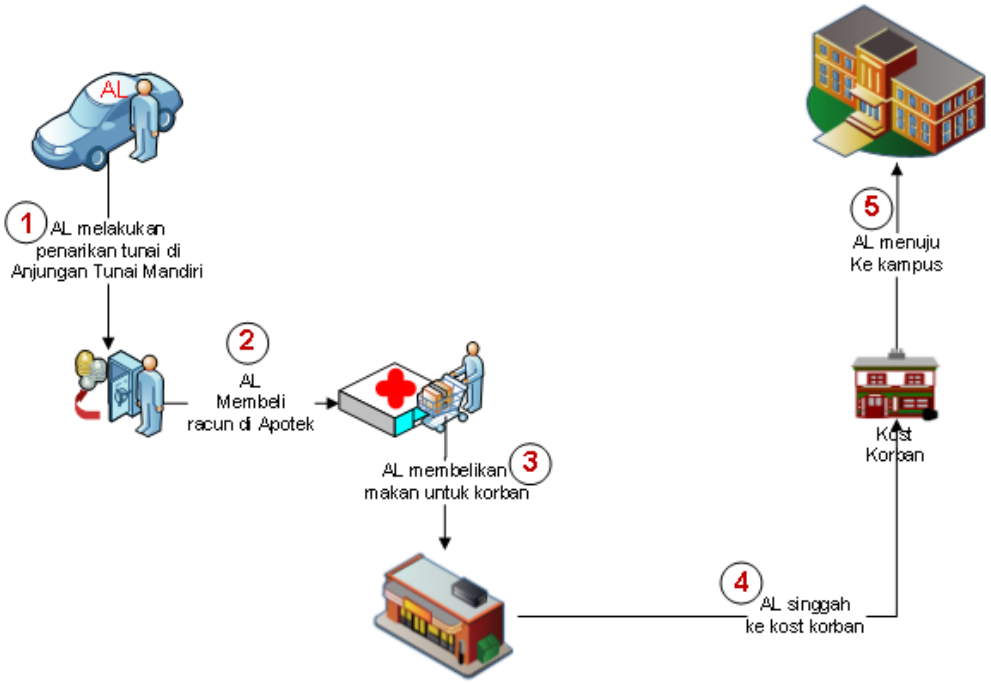
HASIL DAN PEMBAHASAN

4.1 Skenario Pengujian

Maraknya tindak kriminal yang melibatkan barang bukti GPS merupakan salah satu alasan dibutuhkannya ahli forensik. Pada saat penyidik mendapatkan suatu kasus, dengan menggunakan analisis forensik akan didapatkan data-data seperti apa, siapa, bagaimana, dan kapan terjadinya tindak kriminal pada barang bukti yang didapatkan, untuk memperoleh bukti-bukti yang akurat harus melalui tahapan-tahapan forensik agar dapat mempermudah dalam melakukan proses penyelidikan, dibutuhkan beberapa *tools* untuk penyelesaiannya. Dalam uji coba kali ini, *tool* yang digunakan untuk proses *backup* data dari *memory internal* GPS yang telah diamankan yaitu menggunakan *Oxygen forensic suite* dan *MOBILedit*, setelah didapatkan hasil *backup* data langkah selanjutnya adalah menganalisis hasil backup tersebut dengan menggunakan *tools* seperti *Oxygen forensic suite*, *MOBILedit*, *Google Earth* dan *SQLite*. Dari *tools* tersebut didapatkan banyak informasi dan data yang ada pada barang bukti yang nantinya akan diungkap di pengadilan.

Pada penelitian ini dibuat sebuah skenario kasus, Telah ditemukan satu unit mobil dari tersangka berinisial AL yang terlibat kasus pebunuhan, tindakan kriminal yang dilakukannya yaitu pembunuhan dengan dasar balas dendam. Pada saat polisi melakukan olah TKP (Tempat Kejadian Perkara), polisi melakukan interogasi terhadap rekan-rekan satu kost korban, selanjutnya dari keterangan yang diperoleh didapatkan beberapa informasi bahwa pada saat sebelum kejadian ada salah satu rekan korban yang datang ke kost korban, usut punya usut ternyata mobil yang digunakan AL adalah mobil sewaan, selanjutnya polisi melakukan pencarian terhadap tersangka dengan memanfaatkan GPS yang telah terpasang pada mobil sewaan tersebut. Setelah diselidiki melalui alat monitoring yang ada

pada alat kontrol di tempat AL menyewa mobil, akhirnya ditemukan mobil sewaan yang terparkir di parkiran gedung kuliah, dan pada saat mobil tersebut ditemukan, tersangka AL sudah tidak ada di tempat. Selanjutnya polisi menyelidiki GPS yang terpasang di mobil tersangka untuk mendapatkan beberapa bukti digital yang akan dianalisis untuk mendapatkan beberapa lokasi yang telah dikunjungi oleh AL. Pada saat dilakukan analisis ada satu titik yang menunjukkan lokasi rumah AL. Polisi lalu melakukan penahanan terhadap AL. Diduga tersimpan data *log*, seperti *track points*, *routes* dan *waypoints* yang oleh tersangka digunakan untuk menunjukkan arah jalan mana saja yang dilalui, rute-rute mana saja yang pernah dilewati dan lokasi-lokasi mana saja yang pernah disinggahi, sehingga dari *log* tersebut dapat ditemukan jejak-jejak dari tersangka yang akan diselidiki lebih lanjut oleh pihak kepolisian dan akan dijadikan alat bukti di pengadilan.



Gambar 4. 1 Skema Kejahatan

Keterangan:

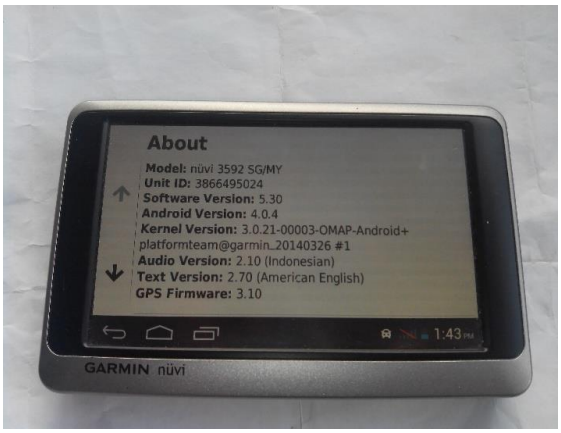
1. Karena AL masih menyimpan dendam terhadap korban dan berencana melakukan balas dendam yaitu dengan meracuni korban, karena AL tidak

memiliki uang untuk membeli obat racun, maka AL pergi ke ATM untuk melakukan penarikan tunai.

2. Selanjutnya AL menuju ke apotek yang menjual obat racun.
3. AL membeli makanan untuk korban, yang sebelumnya telah diberi racun.
4. Setelah itu AL menghampiri kost korban untuk melakukan pembunuhan yaitu dengan memberikan makanan tersebut kepada korban.
5. Setelah mengantarkan makanan yang sudah diberi racun tersebut, lalu AL menuju kampus untuk melaksanakan perkuliahan.
6. Selesai melaksanakan perkuliahan, AL lalu pulang ke rumah. Dan mobil sewaan yang telah dibawa AL ditinggal diparkiran untuk menghilangkan jejak dengan melarikan diri menggunakan kendaraan lainnya.

Setelah dilakukan penyelidikan oleh pihak kepolisian, diperoleh beberapa alat bukti, salah satu alat bukti tersebut adalah GPS *device* yang terdapat pada mobil milik sewaan yang telah disewa oleh tersangka AL. Pihak kepolisian lalu menyerahkan alat bukti tersebut kepada tim digital forensik untuk ditindaklanjuti guna memperoleh bukti-bukti pada GPS *device* tersebut. Setelah di laporkan dan diproses oleh tim penyidik polri, dilakukan beberapa dokumentasi sebagai penjelas dari GPS sebelum dilakukan forensik.

Pada Gambar 4.2 Merupakan hasil dokumentasi foto yang menunjukkan tentang GPS device.



Gambar 4. 2 About Garmin Nuvi 3592LM

Pada Gambar 4.3 Merupakan hasil dokumentasi foto yang menunjukkan fitur pencarian pada GPS untuk mencari lokasi yang diinginkan dan hendak dituju.



Gambar 4. 3 Fitur *Where To*

Pada Gambar 4.4 Merupakan hasil dokumentasi foto yang GPS Garmin Nuvi 3592LM secara fisik.



Gambar 4. 4 Bentuk Fisik GPS Garmin Nuvi 3592LM

4.2 Asumsi Awal Data Digital

Dugaan sementara data digital diperlukan untuk dapat memperkirakan data apa saja yang terdapat pada alat bukti yang dari asumsi tersebut akan dilakukan proses analisis lebih lanjut.

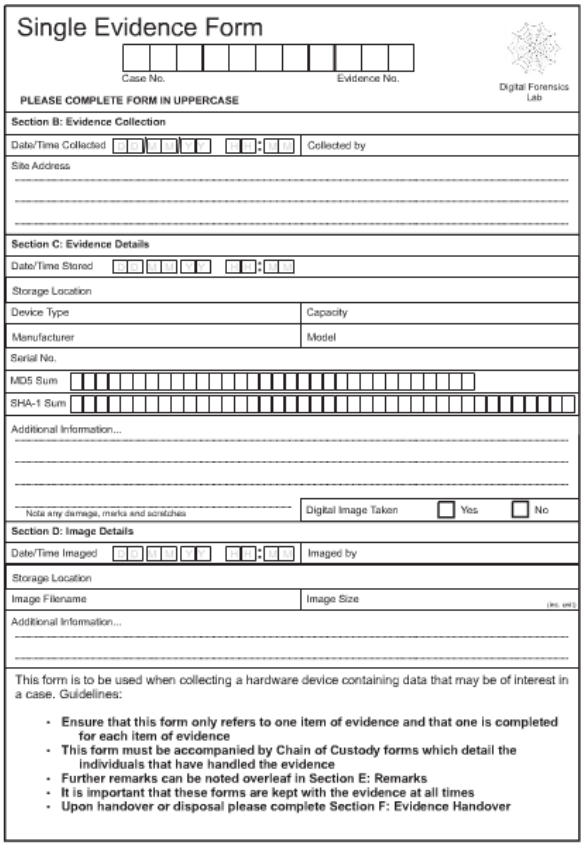
Asumsi awal data digital yang ada pada barang bukti GPS Garmin Nuvi 3592LM, yaitu sebagai berikut:

a. Informasi dari GPS *device*.
b. Catatan dari *Waypoint* dan *track log* yang terdapat pada *file log Current.gpx* dan *Position.gpx.*
c. Informasi hasil pencarian lokasi, hasil prediksi dari lokasi awal ke lokasi tujuan dan tempat pemberhentian, pengguna, dll yang tersimpan pada *database log RecentStops.db, quick_search_list.db, pre.db*.

4.3 Akuisisi

4.3.1 Pengumpulan Barang Bukti

Pengumpulan barang bukti dilakukan untuk mendapatkan suatu petunjuk dari tindak kejahatan yang dilakukan oleh pelaku. Pada skenario kasus ini barang bukti yang digunakan adalah GPS Garmin Nuvi 3592LM. Setelah mendapatkan surat izin penggeledahan sebagai ahli forensik, penyidik harus mengamati dan memahami kejadian terhadap kasus yang terjadi di TKP. Dibutuhkan catatan berupa dokumentasi dari TKP dan pengambilan foto atau gambar di TKP. Setelah mengamati TKP, penyidik mengumpulkan barang bukti, salah satunya adalah GPS *device*. Selanjutnya GPS *device* dimasukkan dalam kantong isolasi dan diberi label khusus agar tidak terjadi pertukaran data atau sinkronasi data antara GPS *device* dengan satelit, selanjutnya penyidik mengisi *Evidence Form*. Gambar 4.5 merupakan contoh *Evidence Form*.



Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected Collected by

Site Address

Section C: Evidence Details

Date/Time Stored

Storage Location

Device Type Capacity

Manufacturer Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken Yes No

Section D: Image Details

Date/Time Imaged Imaged by

Storage Location

Image Filename Image Size

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Gambar 4. 5 Evidence Form

(Sumber: http://www.docstoc.com/docs/88213375/Sample-Chain-of-Custody-Form-for-Digital-Forensics)

Setelah dilakukannya pengumpulan data oleh tim penyidik, selanjutnya adalah melakukan pengujian, pada tahap ini perlu beberapa tahapan yang harus dilalui, seperti berikut:

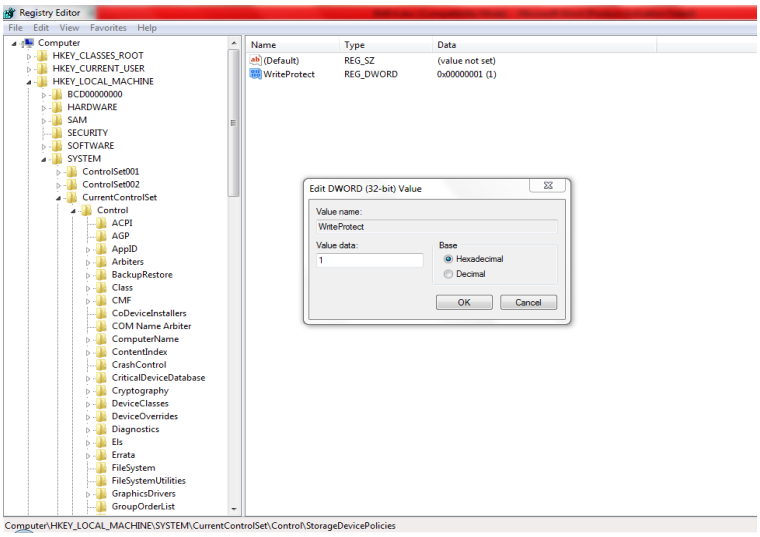
4.3.2 Write Blocking dan Backup Data

1. *Write Blocking*

Sebelum melakukan proses *backup* data pada alat bukti, perlu dilakukan *write blocking* agar tidak terjadi pertukaran data yang tidak disengaja. Berikut adalah langkah-langkah dalam *write blocking* pada sistem operasi *Windows*:

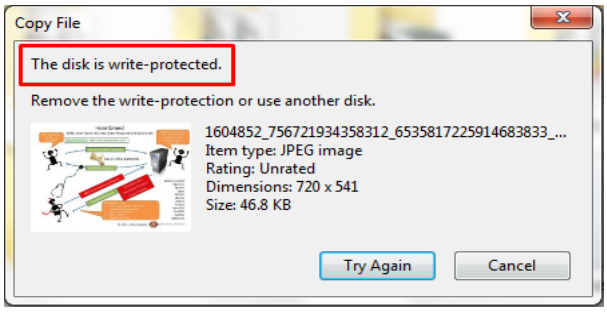
1) Buka *Registry Editor*.
2) Pilih HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control.

3) Buat *key* baru dengan nama *StorageDevicePolicies*.
4) Pada *key* tersebut, buatlah sebuah DWORD (32-bit) *Value* dengan nama *WriteProtect*, seperti terlihat pada Gambar 4.6.
5) Klik dua kali pada *WriteProtect* dan atur *Value Data* menjadi 1.



Gambar 4. 6 Membuat *write protect*

Tanpa di-*restart*, semua *user* pada komputer dengan sistem operasi *windows* tidak akan bisa transfer atau menulis data pada media penyimpanan yang terhubung melalui *port* USB. Jika hal tersebut dilakukan, maka akan muncul peringatan "*The disk is write protected. Remove the write protection or use another disk*", seperti pada Gambar 4.7 yang memperlihatkan bahwa peringatan tersebut muncul, maka proses *Write Blocking* berhasil dengan catatan bahwa pada saat membuat *write protect*, tidak ada media penyimpanan yang terhubung melalui *port* USB. Jika sudah ada media penyimpanan yang terhubung pada saat *write protect* dibuat, maka media penyimpanan tersebut masih bisa melakukan pertukaran data, dan jika ingin mengembalikan seperti semula atau *write unblocking*, cukup dengan mengganti *Value Data* dari 1 menjadi 0.



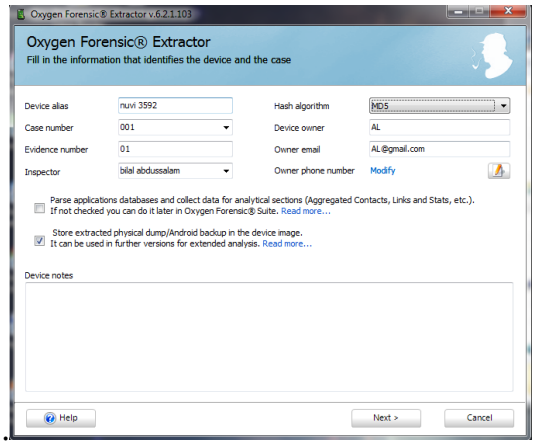
Gambar 4. 7 Peringatan write protection

2. *Backup* Data

Proses *backup* data dilakukan dengan menggunakan *tools Oxygen forensic suite* dan *MOBILedit forensic*.

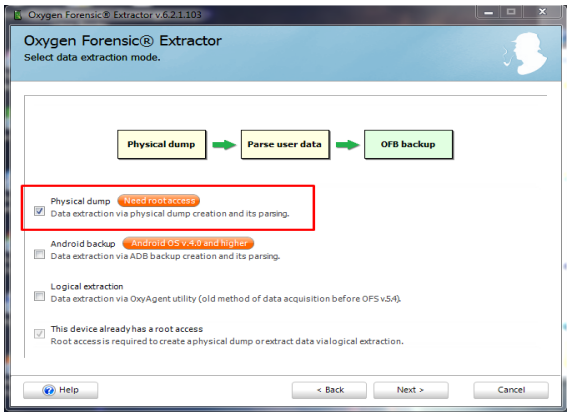
1) *Backup* Data dengan *Oxygen Forensic Suite*

Untuk melakukan analisis menggunakan *Oxygen forensic suite* diperlukan *backup* data dari alat bukti. *Oxygen forensic suite* telah melengkapinya dengan fasilitas *extract*. Untuk melakukan *backup* menggunakan *Oxygen forensic suite* pilih *connect device*, lalu pilih *auto device connection*, selanjutnya *Oxygen forensic suite* akan melakukan deteksi terhadap *device* yang terpasang. Setelah *device* terdeteksi *Oxygen* dan menampilkan informasi *device*, pilih *next*, lalu akan diminta untuk melakukan pengisian *form backup* guna mempermudah dalam identifikasi kasus, serta melakukan *hashing* md5 untuk membuktikan jika hasil dari *backup* tersebut masih *original* dan belum dimodifikasi, seperti pada Gambar 4.8.



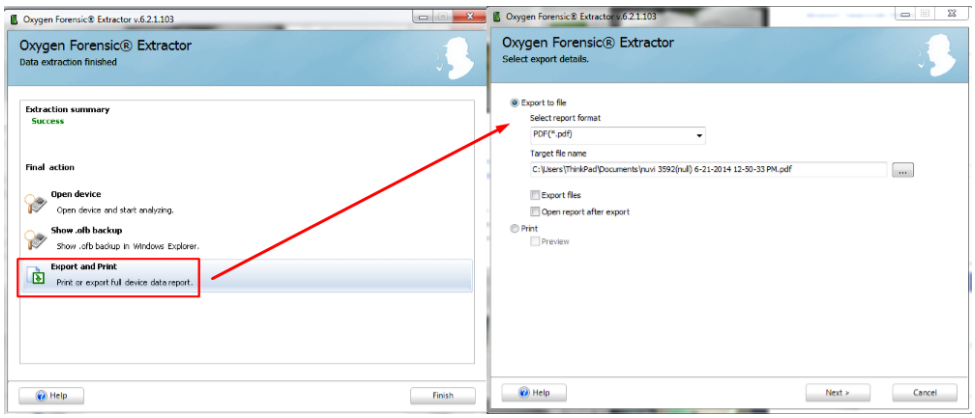
Gambar 4. 8 Form *Backup* Oxygen Forensic Suite

Selanjutnya pilih *next* lalu akan ada pilihan mode *extract*, di sini ada dua pilihan yaitu *recommended mode* dan *advance mode*. Agar dapat mengekstrak data secara fisik pilih *advance mode*. Setelah itu akan ada pilihan *extract mode* seperti pada Gambar 4.9 lalu pilih *physical dump* untuk melakukan *extract* data secara fisik pada GPS *device* yang telah di-*root* atau yang sudah mendapatkan hak akses penuh.



Gambar 4. 9 *Select Physical dump*

Dibutuhkan waktu yang cukup lama dalam melakukan *extract* data, setelah selesai proses *extract* data, lalu simpan hasil *extract* tersebut ke dalam *drive* komputer. Kemudian, buat hasil *report* dengan format PDF ke dalam *drive* komputer melalui fasilitas yang telah disediakan *Oxygen* seperti Gambar 4.10.

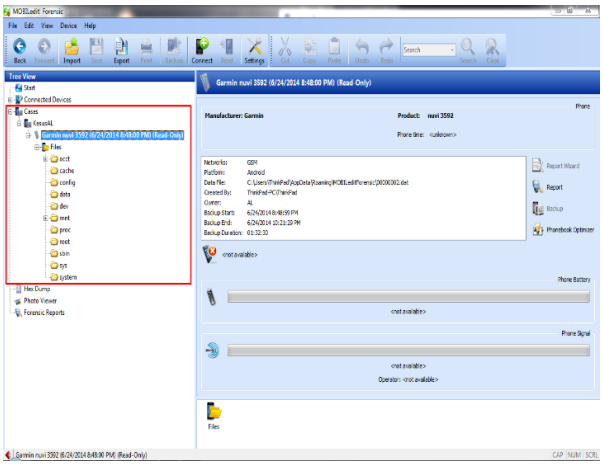


Gambar 4. 10 *Export Report* hasil *Backup*

Setelah melalui proses *extract*, maka akan tampil *device* yang telah di-*extract* tadi, lalu pilih *show .ofb backup* untuk menganalisis hasil *backup* tersebut.

2) *Backup* Data dengan *MOBILedit Forensic*

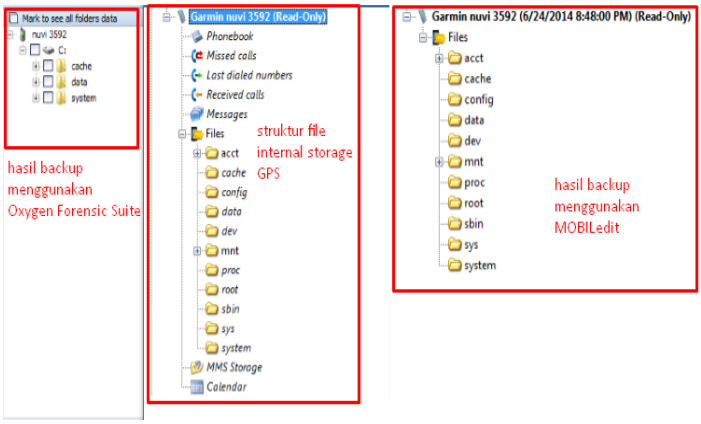
Untuk melakukan analisis dengan menggunakan *MOBILedit Forensic*, diperlukan *backup* data dari alat bukti. *MOBILedit* telah melengkapinya dengan fasilitas *backup*. Penggunaan *MOBILedit* dengan cara menekan *Connect*, *MOBILedit* akan melakukan deteksi otomatis terhadap *device* yang terpasang dan melakukan *backup* dari *storage* GPS. Diperlukan waktu yang cukup lama untuk melakukan *backup* pada *device*. Setelah dilakukan proses *backup*, akan tampil *device* yang sudah di-*backup* tadi. Dapat dilihat pada Gambar 4.11:



Gambar 4. 11 Hasil *backup* menggunakan *MOBILedit*

4.3.3 Verifikasi Hasil *Backup* dengan Alat Bukti

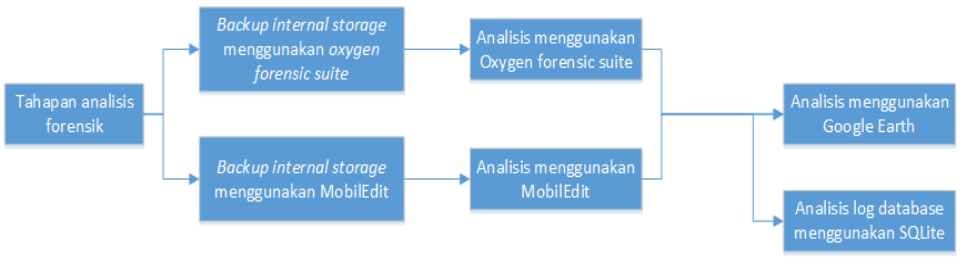
Setelah tahap *write blocking* dan *backup* dilakukan, langkah selanjutnya adalah melakukan verifikasi *file system* hasil *backup* dengan alat bukti guna validasi data. Pengecekan dilakukan dengan membandingkan struktur *file* alat bukti dengan struktur *file* hasil *backup*. Ada beberapa perbedaan struktur *file* dari hasil *backup* menggunakan *oxygen forensic suite* dengan hasil *backup* menggunakan *MOBILedit*, seperti yang ditunjukkan pada Gambar 4.12.



Gambar 4. 12 Struktur *file* hasil *backup Oxygen* (kiri), struktur *file* alat bukti (tengah), struktur *file* hasil *backup Mobiledit* (kanan)

4.4 Analisis Kasus

Setelah melakukan beberapa tahapan akuisisi pada GPS Garmin Nuvi 3592LM, didapatkan bukti *digital* dari hasil *backup internal storage*, selanjutnya dilakukan analisis untuk mendapatkan data-data atau informasi yang dapat dijadikan bukti *digital*. Analisis kasus pada penelitian ini menggunakan *tools Oxygen Forensic Suite, MOBILedit, Google Earth,* dan *SQLite*. Karena setiap *tools* forensik mempunyai langkah-langkah yang berbeda dalam proses penyelidikan barang bukti, maka dibuatlah langkah-langkah pengerjaan tahapan forensik seperti Gambar 4.13 di bawah ini.



Gambar 4. 13 Langkah pengerjaan tahapan *forensic*

4.4.1 Analisis Menggunakan *Oxygen Forensic Suite*

Analisis dilakukan menggunakan *backup* yang telah dibuat sebelumnya. *Oxygen forensic suite* telah memberikan fasilitas kelengkapan *backup* yang berbeda pada setiap *device*. Pada GPS yang dimiliki tersangka AL, dapat diperoleh informasi dan data dari *physical storage* GPS. Informasi yang didapat

dari *physical storage* GPS adalah informasi rekam jejak tersangka AL dalam perjalanan yang tersimpan dalam file berekstensi *.gpx* dan *log search location* yang tersimpan pada file berekstensi *.db*.

a. Hasil dan Pembahasan Struktur File GPS Garmin Nuvi 3592LM

GPS Garmin tersebut memiliki karakteristik yang sangat unik dibandingkan *device* GPS lainnya, yaitu menggunakan *Operating System* Android. Dalam penelitian kali ini penulis membahas sedikit struktur file pada Garmin Nuvi 3592LM.

1) **/cache**

Partisi ini menyimpan data yang dapat diakses dan komponen aplikasi. Menghapus isi partisi ini tidak berdampak pada data personal anda, tapi hanya membersihkan data yang ada dalam partisi tersebut.

2) **/data**

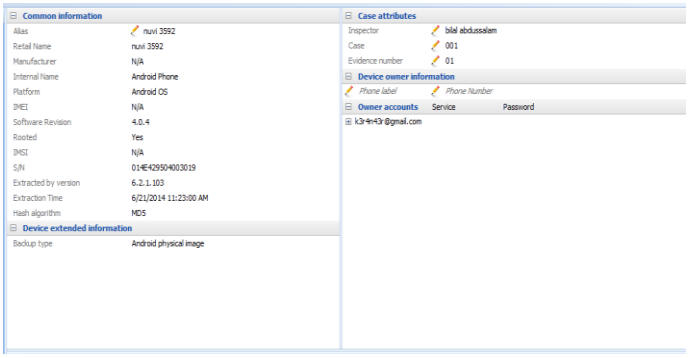
Partisi ini biasa disebut *userdata*, data-data partisi di dalamnya berisi data GPS, seperti: data *log*, *track point*, *waypoint*, *route*, dan aplikasi yang telah terpasang. Menghapus partisi ini bisa berdampak kehilangan data-data penting pada GPS.

3) **/system**

Partisi ini pada dasarnya berisi sistem operasi secara keseluruhan.

b. Hasil dan Pembahasan *Device Information*

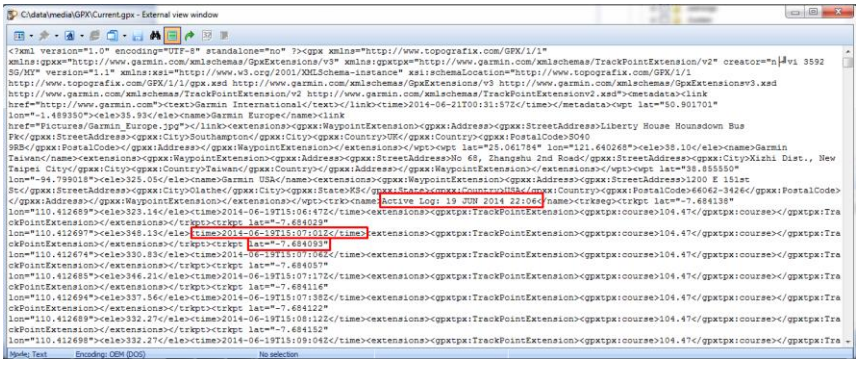
Device Information akan memuat informasi keseluruhan dari hasil *backup* alat bukti. Terlihat pada Gambar 4.14, menu ini akan menampilkan informasi umum dari *device* pada kasus yang akan diselidiki, dari hasil yang didapatkan yaitu informasi *retail name, platform, internal name, software version, rooted*, dan serial number.



Gambar 4. 14 *Device Information* pada GPS Garmin Nuvi 3592LM

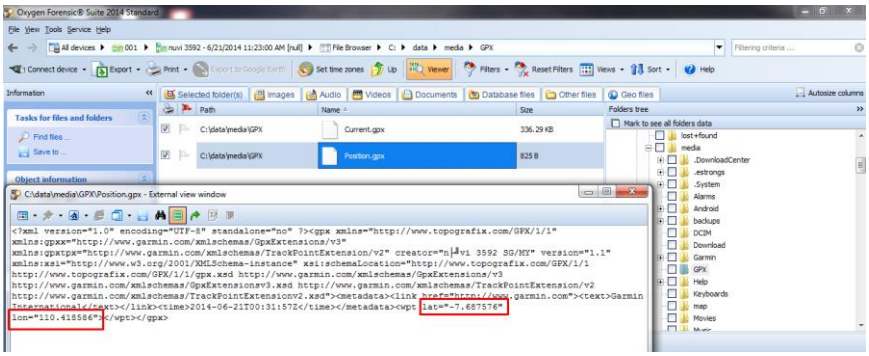
c. Hasil dan Pembahasan pada *Log File Current.gpx* dan *Position.gpx*

Log file Current.gpx adalah salah satu *file* yang menyimpan banyak informasi tentang rekam jejak perjalanan yang telah dilakukan dari tersangka sehingga dari *log file* tersebut penyidik dapat lebih mudah menganalisis jejak tersangka. Informasi yang didapatkan yaitu *active log* dan koordinat perjalanan yang telah dilalui tersangka, Seperti yang terlihat pada Gambar 4.15.



Gambar 4. 15 Melihat isi *file Current.gpx*

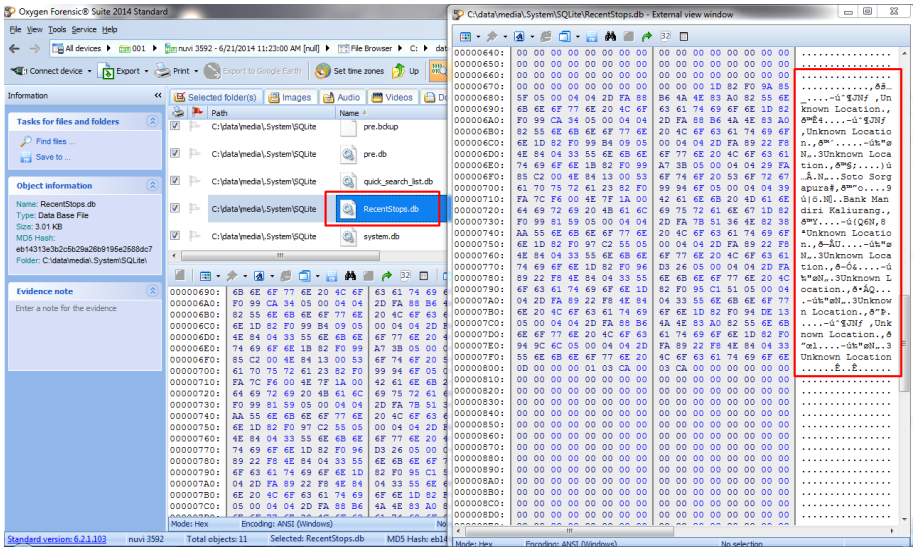
Log file Position.gpx adalah salah satu file yang menyimpan informasi tentang posisi GPS terakhir dalam bentuk koordinat, seperti pada Gambar 4.16.



Gambar 4. 16 Melihat isi *file Position.gpx*

d. Hasil dan Pembahasan pada *Log Database RecentStops.db*

Log file database RecentStops.db adalah salah satu *file database* yang menyimpan banyak informasi penting menyangkut lokasi di mana tersangka AL melakukan pemberhentian atau singgah ke tempat yang dituju, informasi yang didapat dapat dilihat pada Gambar 4.17.

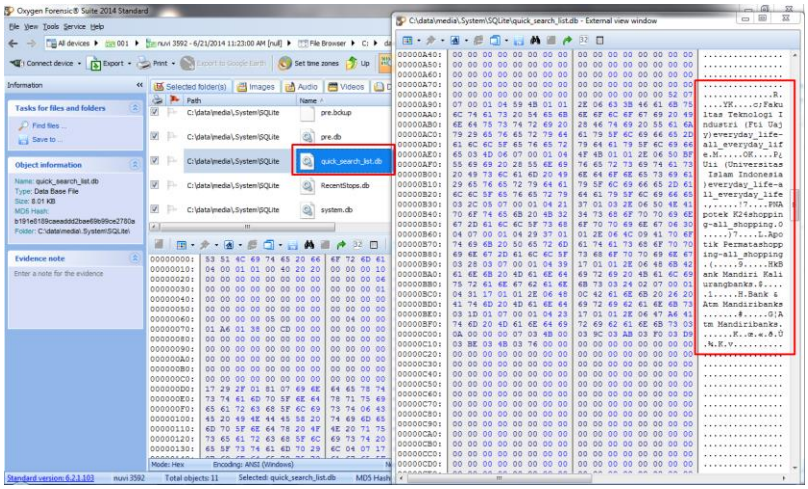


Gambar 4. 17 Melihat isi *file database RecentStops.db*

e. Hasil dan Pembahasan pada *Log Database Quick_Search_List.db*

Log file database quick_search_list.db adalah salah satu *file database* yang menyimpan banyak informasi penting menyangkut hasil pencarian lokasi

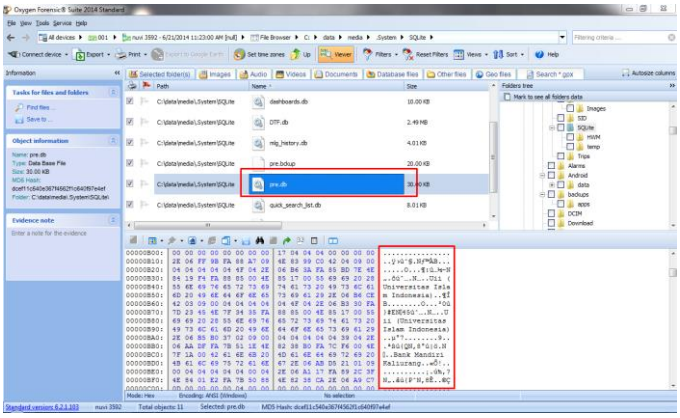
atau tempat yang ingin dituju oleh tersangka, informasi yang didapatkan seperti yang terlihat pada Gambar 4.18.



Gambar 4. 18 Melihat isi *file database quick_search_list.db*

f. Hasil dan Pembahasan pada *Log Database pre.db*

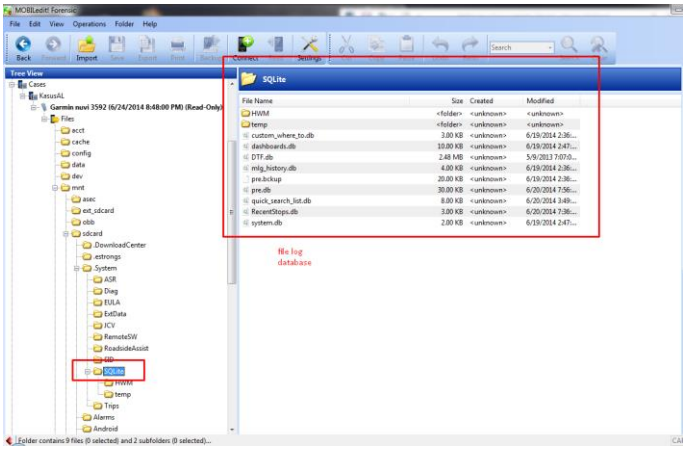
Log file database pre.db adalah salah satu *file database* yang menyimpan banyak informasi penting menyangkut hasil prediksi dari GPS yang memperhitungkan jarak dari suatu lokasi awal untuk mencapai tujuan, seperti pada Gambar 4.19.



Gambar 4. 19 Melihat isi *file database pre.db*

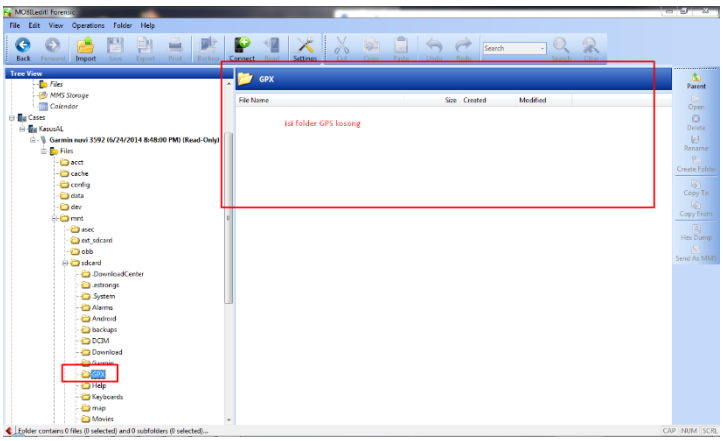
4.4.2 Analisis Menggunakan *MOBILedit*

Analisis dilakukan menggunakan hasil *backup* sebelumnya. *MOBILedit* telah memberikan fasilitas kelengkapan *backup* yang berbeda pada setiap *device*. Pada GPS yang dimiliki tersangka AL, dapat diperoleh informasi struktur *file*, *file log database*, seperti pada Gambar 4.20.



Gambar 4. 20 Melihat isi *file database pre.db*

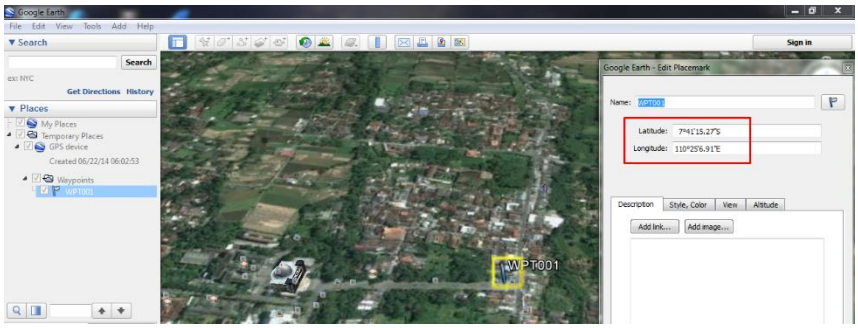
Untuk kelengkapan data *MOBILedit* tidak dapat mem-*backup* seluruh *file* penting yang berhubungan pada kasus ini, yang ada pada *internal storage* GPS, terlihat pada Gambar 4.21.



Gambar 4. 21 Melihat isi *file database pre.db*

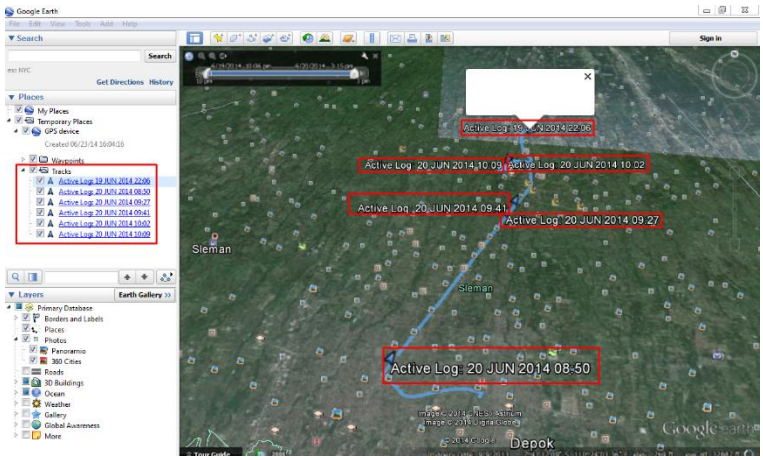
4.4.3 Analisis Menggunakan *Google Earth*

Analisis dilakukan menggunakan hasil *backup* yang telah dibuat sebelumnya. Dari hasil *backup* tersebut didapatkan beberapa *file log* seperti *Current.gpx* dan *Position.gpx*, selanjutnya *file log* tersebut akan dianalisis menggunakan *Google Earth* untuk mempermudah dalam menganalisis koordinat-koordinat pada *file log* tersebut yang akan dipetakan pada *Google Earth*, seperti pada Gambar 4.22.



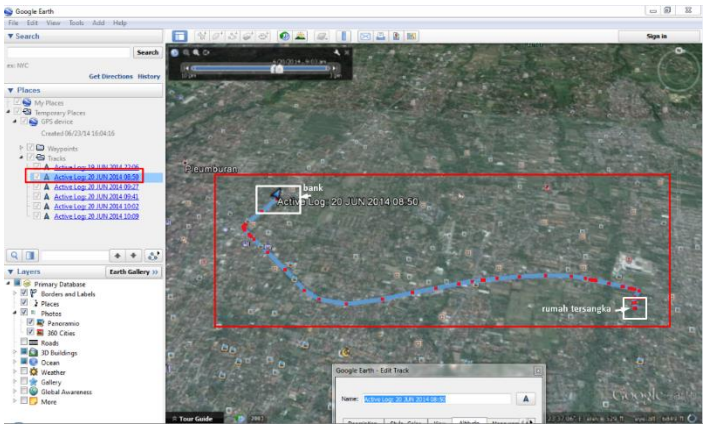
Gambar 4. 22 *File Position.gpx* pada *Google Earth*

Pada gambar 4.23, terlihat keseluruhan jalur yang telah dilalui oleh tersangka AL, dari hasil analisis menggunakan *Google Earth* pada *file Current.gpx* informasi yang didapat seperti tanggal, jam, dan jalur yang telah dilewati tersangka.



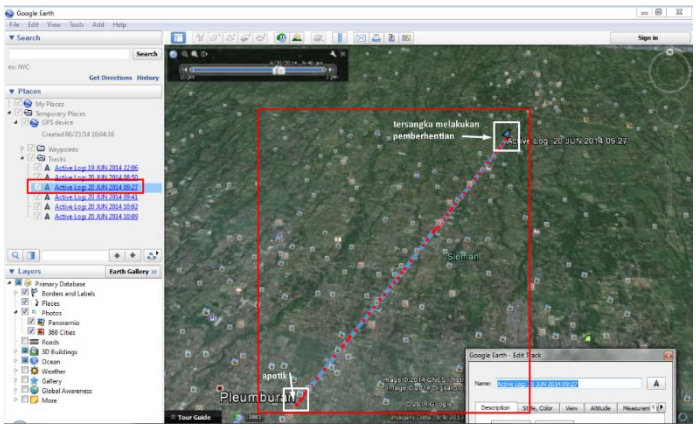
Gambar 4. 23 Analisis *file Current.gpx* pada *Google Earth*

Selanjutnya akan dianalisis satu per satu *active log* yang telah terekam pada *trip log*. Diketahui tersangka hendak melakukan perjalanan menuju kampus, kemudian di tengah perjalanan, tersangka berhenti di salah satu bank untuk melakukan penarikan tunai, seperti yang terlihat pada Gambar 4.24.



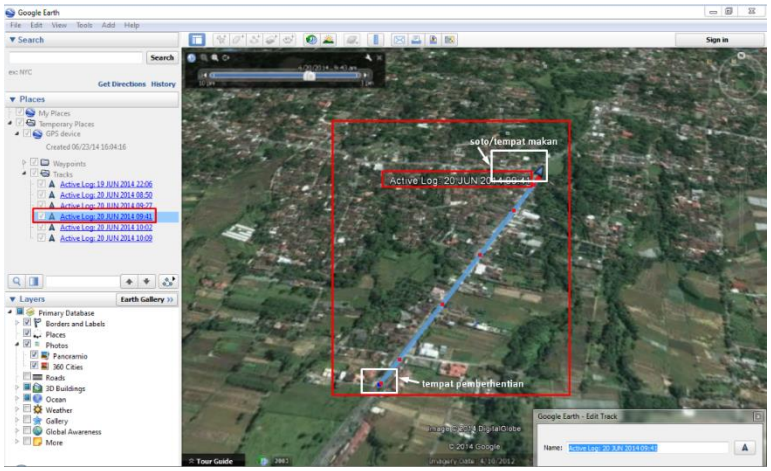
Gambar 4. 24 Analisis *file Current.gpx* pada *Google Earth*

Pada Gambar 4.25, menunjukkan bahwa setelah mengambil uang di bank, tersangka berjalan menuju apotek, lalu tersangka melanjutkan perjalanannya menuju kampus, namun di tengah perjalanan tersangka melakukan pemberhentian, seperti yang terlihat pada *active log* pada pukul 09:27.



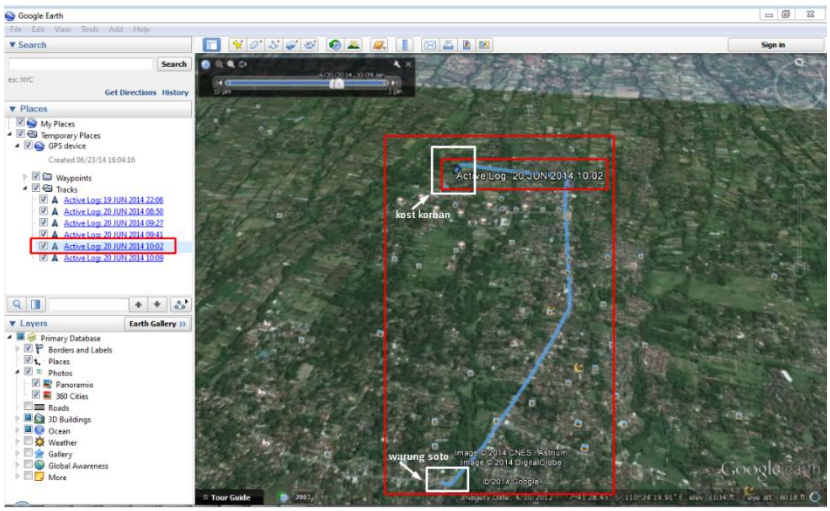
Gambar 4. 25 Analisis *file Current.gpx* pada *Google Earth*

Setelah melakukan pemberhentian, tersangka lalu melanjutkan perjalanannya menuju ke warung soto seperti yang dapat terlihat pada Gambar 4.26.



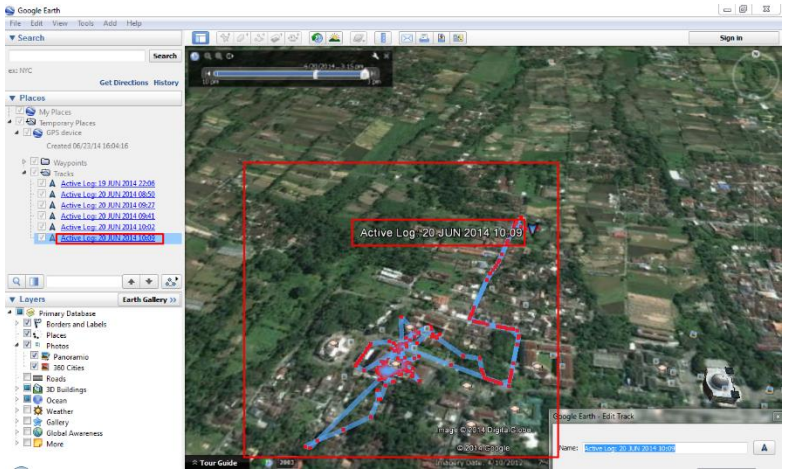
Gambar 4. 26 Analisa *file Current.gpx* pada *Google Earth*

Setelah mengunjungi warung soto, tersangka lalu melanjutkan perjalanannya menuju kost korban seperti yang terlihat pada Gambar 4.27.



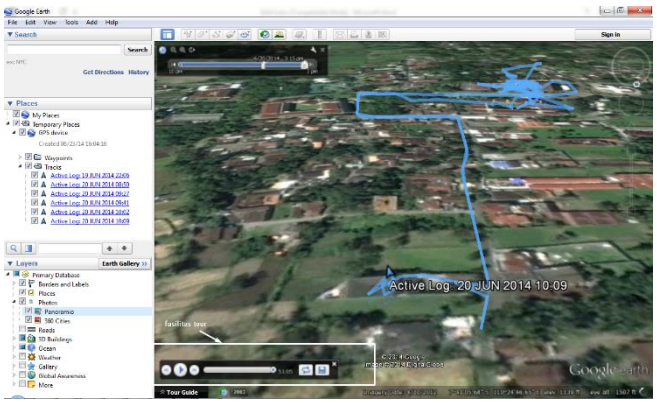
Gambar 4. 27 Analisa *file Current.gpx* pada *Google Earth*

Setelah mengunjungi kost korban, lalu tersangka melanjutkan perjalanan menuju kampus, seperti yang terlihat pada Gambar 4.28.



Gambar 4. 28 Analisis *file Current.gpx* pada *Google Earth*

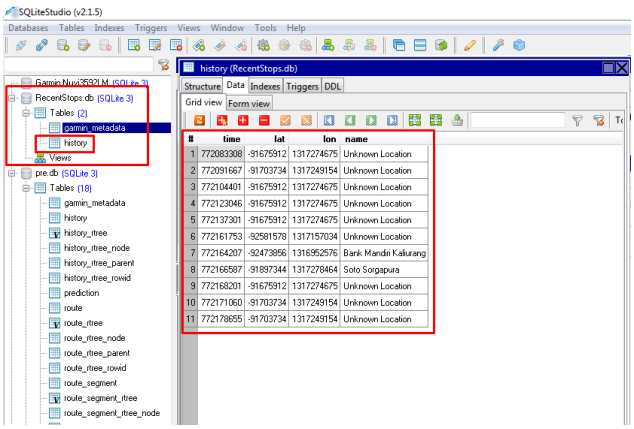
Data *log* tersebut juga dapat ditunjukkan dengan menggunakan fasilitas *tour google earth* yang akan menunjukkan jalur dari jejak awal sampai akhir. seperti yang dapat dilihat pada Gambar 4.29.



Gambar 4. 29 Analisis *track log* menggunakan fasilitas *tour*

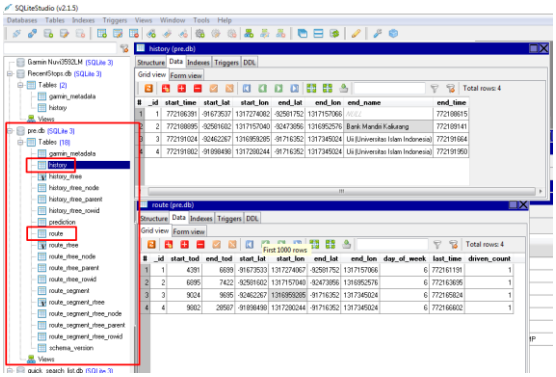
4.4.4 Analisis Menggunakan SQLite

Pada Gambar 4.30, menunjukkan seluruh data atau informasi dari alat bukti di mana saja tersangka melakukan pemberhentian, seperti yang terekam pada *log file database RecentStops.db*, informasi yang didapatkan, yaitu *time*, koordinat dan nama lokasi.



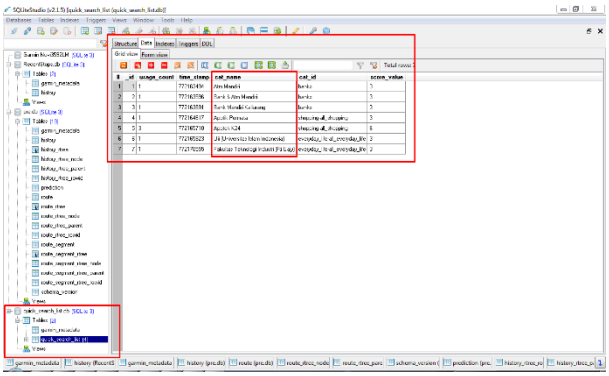
Gambar 4. 30 Analisis *file database RecentStops.db* menggunakan SQLite

Gambar 4.31 Menunjukkan seluruh informasi dari alat bukti yaitu hasil prediksi jarak dari GPS yang akan ditempuh tersangka AL, seperti yang terekam pada *log file database pre.db*, informasi yang didapatkan, yaitu *start time*, *end time*, koordinat awal, koordinat akhir, dan nama lokasi tujuan.



Gambar 4. 31 Analisis *file database pre.db* menggunakan SQLite

Gambar 4.32 Menunjukkan seluruh informasi dari alat bukti yaitu hasil pencarian dari beberapa tempat yang ingin dikunjungi tersangka, informasi yang bisa didapatkan yaitu *time stamp* dan nama lokasi yang ada pada file *database quick_search_list.db*.



Gambar 4. 32 Analisis *file database quick_search_list.db* menggunakan SQLite

4.5 Laporan Hasil Penyelidikan

Setelah selesai melakukan analisis terhadap alat bukti, kemudian dibuat laporan yang memberikan ringkasan serta fakta yang terungkap dari alat bukti, untuk selanjutnya diserahkan kepada polisi untuk ditindaklanjuti. ringkasan hasil laporan dapat dilihat pada Tabel 4.1:

Tabel 4. 1 Data Hasil Analisis

Oxygen Forensic Suite	*MOBILedit*	*Google Earth*	*SQLite*
• *File log Current.gpx* menunjukkan bahwa tersangka AL pernah mengunjungi kost korban • *File log Position.gpx* • *Database pre.db* • *Database quick_search_list.db* • *Database RecentStops.db*	Hanya dapat menampilkan beberapa file yang tidak berhubungan dalam kasus ini.	Terdapat *track point* dan *waypoint* yang dikonversi dari file *log* berekstensi .gpx	Terdapat beberapa rekaman data hasil pencarian, prediksi lokasi tujuan, serta lokasi pemberhentiandari *file log database* berekstensi *.db*

Berdasarkan dari keempat *tools* pada Tabel 4.1 yang digunakan dalam analisis, didapatkan informasi yang cukup akurat dari hasil analisis menggunakan *Oxygen forensic suite*, *Google Earth*, dan *SQLite*, sedangkan *MOBILedit* masih belum bisa menemukan informasi-informasi dari alat bukti pada kasus ini.

4.6 Presentasi

Tahapan terakhir dari beberapa prosedur forensik yang telah dilalui yaitu presentasi. Sebagai penyidik, harus bisa mempertanggungjawabkan hasil penyelidikannya di pengadilan dalam bentuk presentasi. Namun, pada saat presentasi di pengadilan, diperlukan penjelasan yang sederhana dan tidak menyinggung masalah teknis, sehingga orang yang masih awam terhadap forensik dapat mengerti maksud dari yang disampaikan dalam presentasi tersebut. Hal ini berbeda pada saat presentasi dengan pihak yang berwajib yang mengharuskan penjelasan lebih detail tentang forensik baik dari segi teknis maupun non-teknis.

Berdasarkan alat bukti yang ditemukan, yaitu dari hasil analisis *track log* dan *waypoint*, terbukti bahwa tersangka AL melakukan pembunuhan terhadap korban. Analisis kasus pada penelitian ini menggunakan *Oxygen Forensic Suite* dan *MOBILedit Forensic*, karena pada setiap *tools* forensik mempunyai perbedaan dalam menganalisis alat bukti, sehingga terdapat beberapa perbandingan hasil analisis yang didapat dari *tools* yang digunakan sebagai berikut:

Tabel 4. 2 Tabel Perbandingan *Tools*

Oxygen Forensic Suite	***MOBILedit***
• Dapat mem-*backup file-file log.*	• Tidak dapat mem-*backup file-file log.*
• Dapat membaca *file log Position.gpx* dan *Current.gpx* dengan *text editor* yang dimiliki *Oxygen.*	• Tidak dapat membaca *file log Position.gpx* dan *Current.db* dengan *text editor* milik *MOBILedit Forensic*
• Dapat membaca *database log pre.db*, *quick_search_list.db*, dan *RecentStops.db* menggunakan *hex editor* yang ada di *Oxygen*.	• Tidak dapat membaca *database log pre.db* menggunakan *hex editor MOBILedit Forensic*.
• Setelah dilakukan *backup* dengan	• *Generate report* hanya dapat

menggunakan O*xygen forensic suite standart version*, O*xygen* dapat membuat atau *generate report* dari hasil *backup* menggunakan format yang telah ditentukan secara otomatis.	dilakukan jika menggunakan *MOBILedit* berbayar.
• Tidak membutuhkan *connector* tambahan untuk menghubungkan *device* ke komputer, hanya membutuhkan usb *debugging* untuk menghubungkan *device*.	• Membutuhkan *Android Forensic Connector* yang nantinya harus ter-*install* di *device* yang akan dilakukan forensik.

Berdasarkan perbandingan pada Tabel 4.2 dapat diketahui bahwa penggunaan *tool Oxygen forensic suite standard version* lebih akurat dalam menganalisis bukti digital GPS, serta dapat mem-*backup* file-file penting yang berhubungan dengan kasus ini seperti *file-file log* dari alat bukti yang dianalisis pada kasus ini. Sedangkan *MOBILedit Forensic* belum bisa mem-*backup* data-data penting yang berhubungan pada kasus ini.

Tabel 4. 3 Tabel Hasil Analisis Bukti Digital Secara Umum

Informasi yang didapat	*Cara Mendapatkan*	*Path Direktori*
• Catatan *Waypoint* • Catatan *Trackpoint*	• Setelah melakukan *backup* dilakukan analisis file *Current.gpx* menggunakan *tools Oxygen*, dan *Google Earth.*	• /data/media/GPX/Current.gpx
• *Database log* seperti *pre.db*, *quick_search_list.db*, dan *RecentStops.db*	• Setelah didapatkan menggunakan *Oxygen* dilakukan analisis menggunakan *SQLite* untuk dapat membuka isi dalam file *database* tersebut.	• /data/media/.System/SQLite/ pre.db • /data/media/.System/SQLite/ quick_search_list.db • /data/media/.System/SQLite/ RecentStops.db

Berdasarkan perbandingan pada Tabel 4.3 dapat diketahui bahwa informasi yang didapat dari alat bukti pada kasus ini adalah catatan *waypoint* dan *trackpoint* dari *file log* berekstensi .gpx, serta catatan hasil pencarian lokasi, hasil

prediksi lokasi awal ke lokasi tujuan, dan lokasi terakhir pemberhentian pada *file database log* berekstensi .db.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, didapatkan beberapa kesimpulan, sebagai berikut:

a. Untuk mengungkap GPS *device* sebagai barang bukti dalam kasus ini, serta *tools* forensik yang efektif dan efisien dalam menganalisis barang bukti. Adapun Barang bukti yang ditemukan dari *internal storage* GPS adalah:

   1) *Log waypoint* dan *trackpoint* yang terdapat pada *file log* dengan extensi *file .gpx* yang menyimpan seluruh catatan jejak dari pelaku, dengan menggunakan *tools Oxygen forensic suite* untuk mem-*backup* serta menganalisis file tersebut, serta menggunakan *tools* tambahan seperti *Google Earth* untuk memetakan *waypoint* dan *trackpoint* pada *map* yang telah disediakan *Google Earth*.
   2) *Log database* hasil pencarian lokasi, hasil prediksi lokasi awal ke lokasi tujuan, dan lokasi tempat pemberhentian tersangka didapatkan dari hasil analisis menggunakan *tool SQLite* untuk membuka *log database*, karena *file log* ini berbentuk file database dan hanya dapat dilihat menggunakan *SQLite. Berbeda dengan Oxygen forensic suite* yang hanya dapat melihat *strings* dari *file log database* tersebut.

b. Beberapa batasan hasil analisis adalah sebagai berikut:

   1) Dari hasil analisis *file log .gpx*, penyidik hanya mendapatkan *log* dari *waypoint* dan *trackpoint.*
   2) Analisis bukti digital yang dilakukan adalah terhadap beberapa *file log* seperti *file log* dengan ekstensi *.gpx* dan *file log* database dengan ekstensi *.db.*

c. Langkah yang dilakukan dalam forensik barang bukti GPS, yaitu
   1) Proses backup *internal storage* GPS menggunakan *Oxygen Forensic Suite* dan *MOBILedit*.
   2) Analisis hasil *backup* barang bukti menggunakan *Oxygen Forensic Suite*, *MOBILedit*, *Google Earth* dan *SQLite*.

d. Beberapa keunikan yang didapatkan dari GPS Garmin Nuvi 3592LM pada saat dilakukan analisis forensik, yaitu:
   1) Sistem operasi yang digunakan adalah android.
   2) Penggunaan sistem operasi android memberikan keunikan pada *device* dalam penyimpanan basis data.
   3) Struktur *file* berbeda dengan GPS Garmin pada umumnya.

5.2 Saran

Dari hasil pengujian dan implementasi yang telah dilakukan, ada beberapa saran yang perlu disampaikan oleh penulis, yaitu:

a. Untuk penelitian yang selanjutnya sebaiknya melakukan penelitian terhadap GPS device lainnya, dikarenakan karakteristik dan tipe GPS device yang berbeda-beda serta untuk menambah pengetahuan yang lebih tentang GPS forensik.
b. Untuk penelitian selanjutnya disarankan menggunakan *tools* yang lebih lengkap dan dapat menampilkan koordinat dari log yang dapat dipresentasikan dalam bentuk peta serta menemukan keunikan lain dari GPS forensik.

DAFTAR PUSTAKA

Cusack, B., Simms, M. (2011). Evidential Recovery From GPS Device. Journal of Applied Computing and Information Technology. ISSN 2230-4398, Volume 15 (01), 2011

LeMere, B. (2012). *GPS Forensic Overview*. Diakses 19 Maret 2014 [*online*]. http://www.slideshare.net/blemere/gps-forensics-17474724

Mathia, T. N. (2009). The Forensic examination of Embedded device such Global Position System (GPS). *Thesis.* University of Wales Newport

Sawitwatch. (2011). Pengenalan GPS Navigasi dan Aplikasinya. Diakses 17 Maret 2014 [*online*]. http://sawitwatch.or.id/download/manual%20dan%20modul/163_Prinsip%20GPS%20dan%20Navigasi.pdf

Ariesant. (2013). Oknum TNI Terlibat Pencurian Mobil. Diakses 17 Maret 2014, [online] www.gobekasi.com/index.php/detail/5739/oknum-tni-terlibat-pencurian-mobil

Roby. (2014). Kasus pencurian mobil di Jakarta terungkap berkat GPS. Diakses 17 Maret 2014 [online] http://www.super-spring.com/kasus-pencurian-mobil-di-jakarta-terungkap-berkat-gps/

Wiyatputera, D. (2010). *Kegunaan GPS bagi Polisi*. Diakses 17 Maret 2014, [online] http://teknologi.kompasiana.com/internet/2010/04/24/kegunaan-gps-bagi-polisi-125924.html

Indrajit, R. E. (2011). Forensik Komputer. Diakses 20 Maret 2014 [*online*]. http://folder.idsirtii.or.id/pdf/IDSIRTII-Artikel-ForensikKomputer.pdf

MHP, A. T. (2011). GPS Bagi Pemula. Diakses 20 Maret 2014 [*online*]. http://mantugaul.wordpress.com/2011/06/10/review-buku-berkenalan-dengan-gps-andre-tanoe-its-all-about-gps/

Steven, W. (2010). Perbedaan GPS dan A-GPS system. Diakses 6 September 2014 [*online*]. http://stevenwahid.blogspot.com/2010/10/perbedaan-gps-dan-gps-system.html

Nugroho, A. E. (2012). Pengenalan Alat Ukur GPS. Diakses 20 Maret 2014 [*online*]. http://bpkh3.dephut.go.id/pdf/pengenalan_alat_ukur_gps.pdf

Prayudi, Y. (2013). *Komputer Forensik: Pengantar*. Diakses 20 Maret 2014 [*online*]. http://catatanforensikadigital.wordpress.com/2013/11/13/komputer-forensik/

Sinambela, J. M. (2011). Computer Forensic. Diakses 20 Maret 2014 [*online*]. http://josh.rootbrain.com/seminar/Computer%20Forensic-Josua-M-Sinambela.pdf

Syafa'at, A. (2007). *Tutorial Interaktif Instalasi Komputer Forensik Menggunakan Aplikasi Open Source.* Jakarta: Departemen Komunikasi dan Informatika.

Utdirartatmo, F. (2005). *Cara Mudah Menguasai Komputer Forensik dan Aplikasinya.* Yogyakarta: GRAHA ILMU.

Sulianta, F. (2008). *Komputer Forensik.* Jakarta: PT. Elex Media Komputindo.