# Bab 3 Metode Penelitian

## 3.1. Studi Pustaka

Studi pustaka merupakan kegiatan untuk mengkaji dan mempelajari berbagai sumber literatur dan teori-teori yang mendukung tentang penelitian yang dilakukan. Sumber pembelajaran pada studi pustaka dapat bersumber dari jurnal, paper, artikel, buku-buku, website, dan sumber pembelajaran lainnya yang membahas berkaitan tentang *Mobile Banking*, *Mobile Forensic*, dan *Static Forensic*. Pada tahapan ini akan dilakukan pula penyusunan proposal penelitian.

## 3.2. Alat dan Bahan Penelitian

Untuk mendukung impementasi dalam penelitian ini diperlukan adanya perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian.

### 3.2.1 Hardware

A. PC Core i3, RAM 4 GB sebagai komputer untuk melakukan penarikan data dan analisa.
B. *Smartphone* berbasis Android OS KitKat 5.0.
C. Kabel *connector* USB.

### 3.2.2 Software

A. Andriller.
B. Android Commander.
C. APK Tool.
D. FTK Imager.
E. USB Write Blocker.

## 3.3. Mobile Forensic Umum

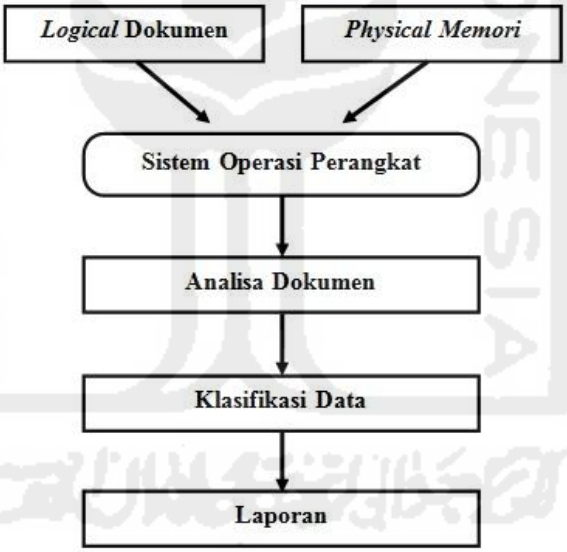
*Mobile forensic* atau forensika ponsel didefinisikan sebagai ilmu untuk memulihkan bukti potensial digital pada perangkat *mobile*, menggunakan teknik yang sama seperti untuk investigasi forensika digital pada umumnya. *Mobile forensic* merupakan cabang ilmu dari *digital forensic*

yang dikhususkan untuk penanganan perangkat *mobile* seperti ponsel pintar, GPS, perangkat seluler, dan lain sebagainya (Mumba 2014).

Sebuah perangkat *mobile* terdiri dari beberapa bagian, yang berfungsi untuk mempertahankan data. Beberapa diantaranya adalah kartu SIM, memori *internal*, modul tambahan berupa GPS, dan kartu memori (*external*).

Peneliti mengkutip salah satu contoh penelitian terdahulu yang dilakukan oleh (Qian et al. 2008) mengenai analisa dan desain *mobile forensic* menggunakan metode *AT Commands* yang pada awal penciptaan ditujukan sebagai metode pada sistem kerja modem untuk PC. Mereka melakukan analisa terhadap perangkat ponsel guna mencari data yang tersimpan di beberapa bagian diantaranya yaitu informasi kalender, SMS, catatan panggilan (*call log*), waktu dan tanggal, rekaman percakapan, dan informasi penting mengenai data pribadi yang berkaitan dengan aplikasi *executable*.

Model analisa yang dilakukan (Qian et al. 2008) mengenai *mobile forensic* terilustrasikan pada Gambar 3.1.



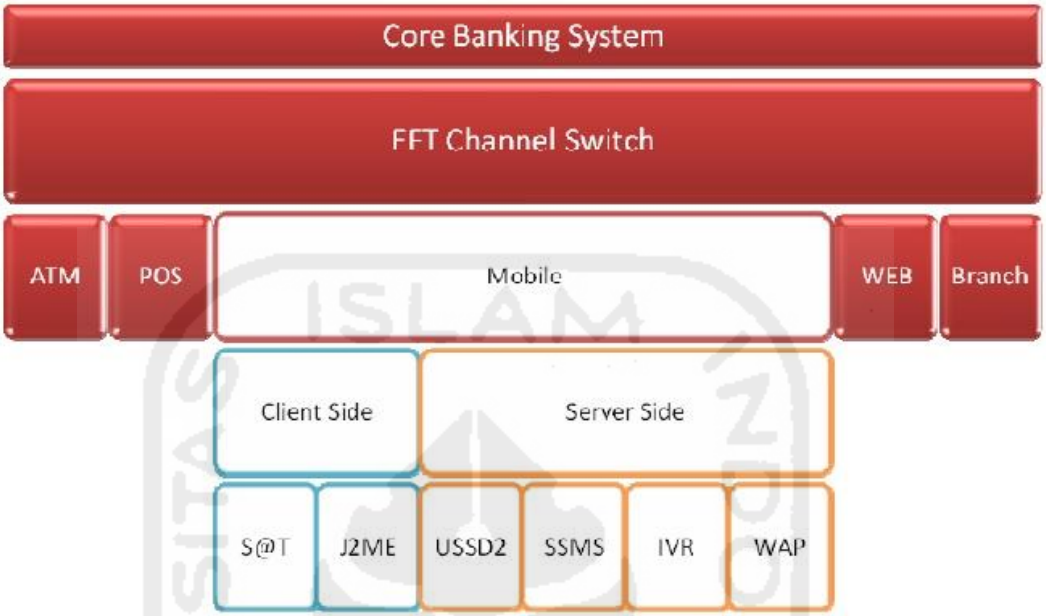

**Gambar 3.1** Model analisa *mobile forensic* pada penelitian Qian Zhicong dan tim (2008)

Penggunaan metode sistem *AT Commands* bertujuan untuk memudahkan analisa perangkat *mobile* dan sebagai alat investigasi *mobile forensic* berupa Encase, WinHex, WINcon, dll.

## 3.4. Arsitektur *Mobile Banking* Secara Umum

Fasilitas layanan *mobile banking* merupakan salah satu bagian dari inti perbankan, seperti penjelasan dari FinMark Trust (*Mobile Banking Technology Options*, 2007). Merupakan aplikasi

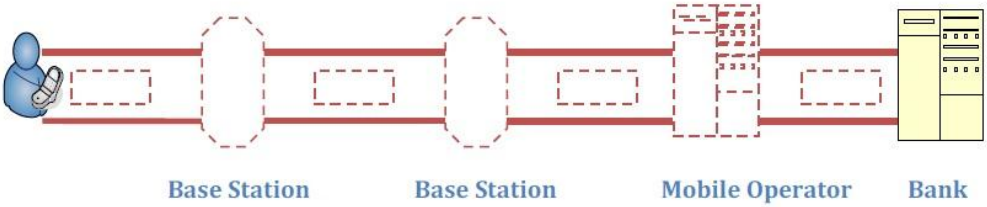
yang dapat di*install* di dalam perangkat *smartphone* milik nasabah agar mempermudah aktifitas transaksi perbankan (Overview 2007). Penjelasan mengenai arsitektur posisi pelayanan *mobile banking* dalam alur sistem perbankan terilustrasi pada Gambar 3.2.




**Gambar 3.2** Arsitektur *mobile banking* secara umum

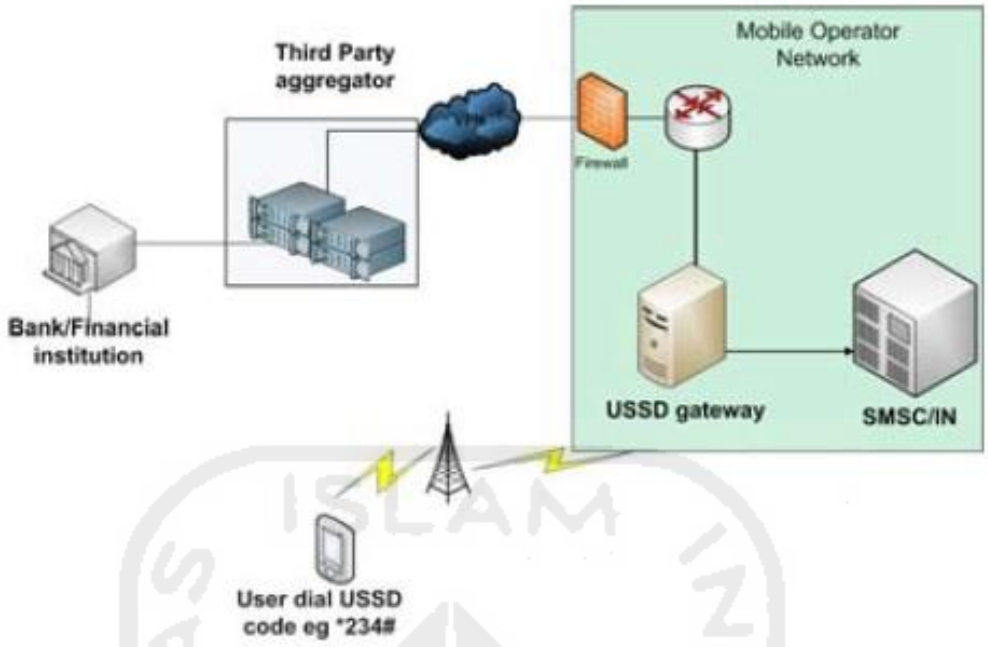
( Sumber : (Overview 2007) )

Pada penerapan sistem keamanan layanan *mobile banking* masing-masing perbankan memiliki cara tersendiri dalam membuat aplikasi yang aman dan nyaman untuk digunakan oleh nasabah. Salah satu sistem keamanan yang mendukung secara tidak langsung dari sisi aplikasi adalah keamanan yang terdapat di dalam sistem operator seluler GSM sebagai perantara atau jalur data antara perangkat *smartphone* dengan server perbankan. Sistem keamanan fasilitas *mobile banking* didukung pula oleh protokol keamanan berlapis jaringan GSM, sebelum mengakses ke sistem server perbankan. Penjelasan tersebut terilustrasikan pada Gambar 3.3.




**Gambar 3.3** Ilustrasi lapisan keamanan jaringan GSM pada layanan *mobile banking*

( Sumber : (Overview 2007) )



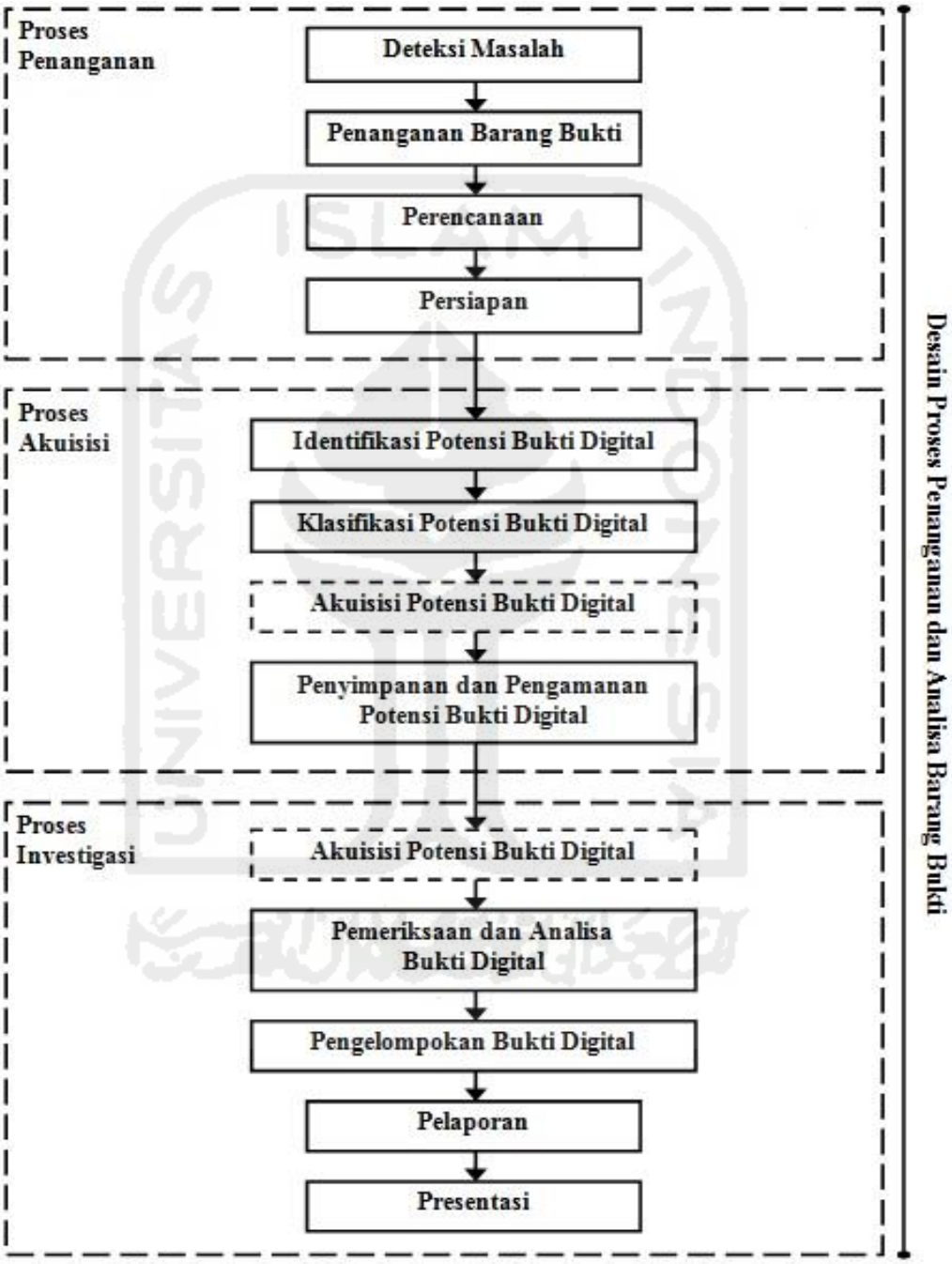

**Gambar 3.4** *Basic* topologi jaringan yang digunakan *mobile banking* secara umum
( Sumber : (Trends 2015) )

Secara teknis user / pengguna fasilitas *mobile banking* mengakses sistem menggunakan perangkat seluler (*smartphone*), kemudian melalui jaringan internet baik menggunakan *wireless* lokal ataupun sinyal *provider* untuk terhubung ke dalam sistem perbankan (melakukan transaksi) (Trends 2015).

Namun sistem jaringan *mobile banking* tidak sesederhana itu. Saat ini banyak sekali sistem keamanan yang diterapkan dalam topologi jaringan *mobile banking* yang beragam antara bank satu dengan bank lainnya guna menjaga keamanan serta kenyamanan para penggunanya atau nasabah. Dengan semakin canggihnya sistem keamanan yang diterapkan, maka semakin mahal pula biaya pembuatan atau pemeliharaan sistem *mobile banking* yang digunakan.

## 3.5. Metode Static Forensic Perangkat Mobile

Adapun desain proses penanganan dan akuisisi potensi bukti digital yang akan dilakukan pada penelitian ini menggunakan metode *static forensic* dapat dilihat pada bagan simulasi Gambar 3.5.




**Gambar 3.5** Desain proses penanganan dan analisa barang bukti

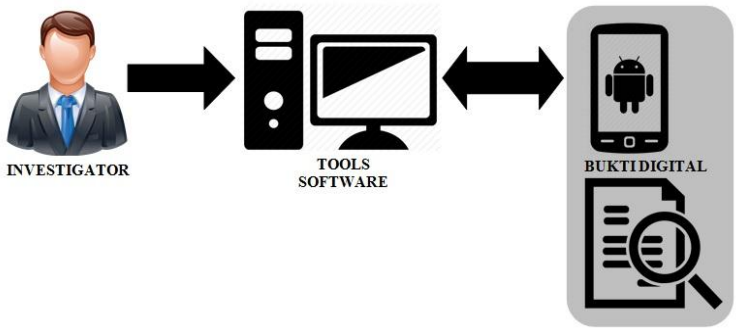
( Mengadopsi dari penelitian (Mumba 2014) )

Desain proses penanganan dan analisa barang bukti Gambar 3.5 mengadopsi pada penelitian terdahulu (Mumba 2014), terdapat 3 fase utama yang disetiap bagiannya memiliki beberapa langkah terurut. Fase pertama adalah Proses Penanganan. Diawali tahap mendeteksi masalah, yaitu menganalisa apa saja permasalahan yang terjadi dan akan ditangani. Kemudian penanganan barang bukti, haruslah mengetahui perangkat apa yang akan ditangani dan bagaimana perlakuan penanganan sesuai dengan tahap – tahap yang baku. Tahap perencanaan merupakan penyusunan rencana langkah – langkah apa saja yang harus dilakukan dalam menangani, menganalisa, hingga membuat laporan terhadap barang bukti digital. Tahap persiapan adalah tahapan akhir di dalam fase pertama ini, terdapat beberapa hal diantaranya yaitu mempersiapkan apa saja *hardware* dan *software* yang diperlukan, kebutuhan penunjang yang berkaitan dengan investigasi haruslah relefan.

Fase kedua adalah Proses Akuisisi. Tahap awal yaitu identifikasi potensi bukti digital terhadap beberapa perangkat yang kemungkinan terdapat bukti digital. Misalkan pelapor atau nasabah menggunakan layanan perbankan tidak hanya di dalam satu perangkat, maka perlu diidentifikasi perangkat mana saja yang kemungkinan terdapat potensi bukti digital. Selanjutnya melakukan klasifikasi potensi bukti digital dengan cara memisahkan masing – masing barang bukti dalam wadah tersendiri dan memberikan label. Tahap terakhir melakukan penyimpanan dan pengamanan terhadap seluruh barang bukti yang telah diklasifikasikan, bahkan harus dilakukan pencatatan secara lengkap dan terperinci.

Proses Investigasi adalah fase terakhir yang diawali tahap pemeriksaan dan analisa bukti digital. Dengan menggunakan alat bantu yang telah dipersiapkan dalam fase sebelumnya, investigator melakukan analisa secara sistematis dan terperinci. Setelah melakukan analisa dan ekstraksi barang bukti digital, tahap selanjutnya mengelompokan bukti digital. Misalkan mengkategorikan data – data bukti digital berupa transaksi legal, transaksi ilegal, dan data lainnya yang mungkin tidak dapat dilakukan analisa karena keterbatasan tertentu. Tahap berikutnya merupakan tahap terakhir yaitu memberikan laporan hasil investigasi sesuai kenyataan temuan yang ada, serta mempresentasikan secara terperinci dan jelas.

Desain proses penanganan dan analisa barang bukti tersebut peneliti mengadopsi dari penelitian yang dilakukan oleh Qian Zhicong dan tim (2008) tentang analisa dan desain *mobile forensic* menggunakan metode *AT Commands*.




**Gambar 3.6** Mekanisme akuisisi secara *static forensic*

Hal utama pada proses *static forensic* adalah melakukan tahapan analisa secara terperinci dan teliti terhadap sistem aplikasi. Serta menganalisa data *offline* di dalam *folder directori* aplikasi *mobile banking* tanpa harus terhubung ke sistem perbankan melalui jaringan (*offline*).

Menganalisa data penting yang memiliki potensi tindak kejahatan *cyber* ataupun dapat digunakan sebagai bukti tindak kejahatan di hadapan hukum. Contohnya berupa data profil nasabah terkait, log transaksi, nomor rekening pemilik akun maupun rekening yang berkaitan dengan data transaksi masa lalu (telah terproses), dan data penting lainnya. Karena masih terdapat beberapa kemungkinan yang terjadi pada aplikasi *mobile banking* yang diteliti. Khususnya perbedaan antara hasil analisa secara *real* yang akan diperoleh dengan harapan hasil analisa yang direncanakan.

## 3.6. Skenario Kasus

Pada penelitian ini diilustrasikan sebuah skenario kasus tindak kejahatan cyber, yaitu peretasan akun akses resmi atau diistilahkan dengan *fraud*. Seorang pelaku memiliki kunci akses sebuah akun *mobile banking* berupa ID Akun dan *Password* Akses aplikasi, serta mengetahui PIN Transaksi yang digunakan untuk melakukan transaksi transfer, pembelian / pembayaran, dan sejenisnya.

Skenario kasus yang terjadi bermula saat pelaku memanfaatkan kelengahan korban pemilik *smartphone* untuk menyematkan aplikasi *keylogger*. Aplikasi tersebut bekerja dengan cara melakukan pencatatan atau *recording* terhadap semua teks yang diketikkan di dalam *smartphone*. Data yang tercatat disimpan dalam bentuk *file log*.

Pemilik *smartphone* tidak mengetahui bahwa di dalam perangkat *mobile* miliknya telah terpasang aplikasi ilegal yang mengincar informasi-informasi terkait semua akun penting. Karena semua hal yang diketik oleh korban akan dicatat dan disimpan. Sehingga besar kemungkinan

akan tersimpan informasi terkait ID dan *Password* akses mengenai aplikasi *mobile banking* yang sudah diincar oleh pelaku.

Setelah semua informasi terkait akun penting milik korban, khususnya akun layanan *mobile banking* telah tercatat dan tersimpan pada sebuah *file log*, selanjutnya pelaku mengambil *file* penting tersebut. Misalkan dengan cara memanfaatkan kelengahan korban, kemudian pelaku menyalin *file log* yang berisikan data penting dari memori internal perangkat *smartphone*.

Pelaku mencari informasi ID dan *Password* akses aplikasi *mobile banking* yang digunakan oleh korban, kemudian akan digunakan pelaku untuk melancarkan aksi *fraud*. Bersumber dari salah satu *file log* yang disalin dari perangkat smartphone milik korban, ID dan *Password* akses akun aplikasi *mobile banking* telah didapatkan oleh pelaku.

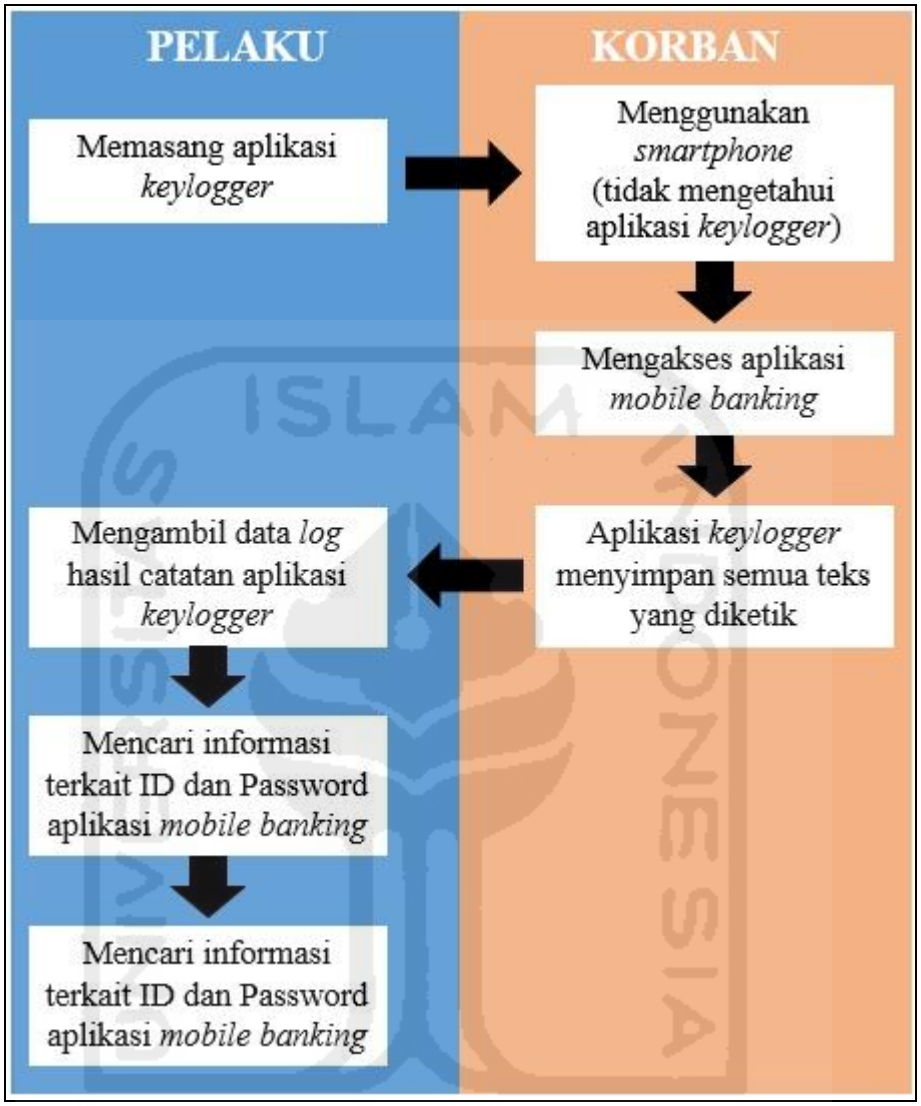
Tindakan akses ilegal atau *fraud* yang akan dilakukan oleh pelaku haruslah menggunakan perangkat *smartphone* milik korban. Karena pada dasarnya sistem kerja aplikasi *mobile banking* jika berganti perangkat harus memerlukan registrasi ulang. Untuk dapat melakukan registrasi ulang tersebut setiap bank menerapkan cara berbeda-beda. Ada cara registrasi yang mengharuskan nasabah atau pemilik akun mendatangi *customer service* bank untuk memberikan informasi terkait registrasi ulang. Ada pula bank yang menerapkan cara registrasi layanan *mobile banking* dari mesin ATM dan menggunakan kartu debit milik nasabah, atau biasa disebut kartu ATM.

Jika proses registrasi ulang berhasil dilakukan, baik melalui layanan pelanggan / *customer service* maupun menggunakan fasilitas pada layanan mesin ATM, selanjutnya konfirmasi aktivasi layanan aplikasi *mobile banking* akan dikirimkan melalui pesan singkat / SMS yang ditujukan kepada nomor telepon seluler terdaftar milik nasabah.

Selang beberapa hari setelah pelaku memperkirakan bahwa korban telah mengakses layanan *mobile banking*, kemudian pelaku melakukan akses ilegal atau *fraud* terhadap layanan aplikasi *mobile banking* menggunakan perangkat *smartphone* milik korban pada saat lengah. Tujuan utama pelaku yaitu mentransferkan uang dalam jumlah besar yang ditujukan pada nomor rekening akun palsu milik pelaku.

Korban menyadari bahwa saldo miliknya telah berkurang dan terkirim pada sebuah rekening yang tidak dia ketahui. Kemudian korban melaporkan hal tersebut kepada bank tempat dia menyimpan dana. Pihak perbankan menjelaskan bahwa transaksi tersebut dilakukan bersumber dari layanan *mobile banking* yang digunakan oleh korban.

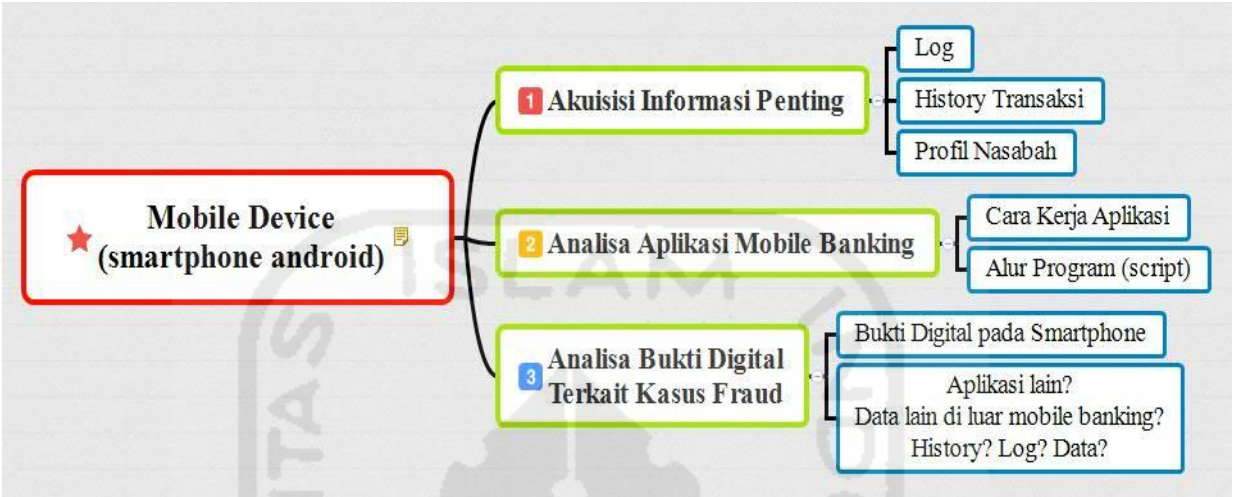
Ilustrasi skenario kasus yang telah dijelaskan pada alur cerita, tergambarkan pada Gambar 3.7.




**Gambar 3.7** Ilustrasi simulasi kasus

## 3.7. Analisa Kasus

Proses analisa terhadap *smartphone* yang diteliti untuk mencari bukti digital terkait tindak kejahatan *fraud* pada Skenario Kasus dapat diilustrasikan pada Gambar 3.8 berikut ini.




**Gambar 3.8** *Mind mapping* analisa dan akuisisi *mobile device* (*smartphone*)

Tahap pertama peneliti akan melakukan akuisisi dan analisa terhadap perangkat *smartphone* berbasis android milik korban. Tahap ini dilakukan guna mencari data-data potensi bukti digital yang difokuskan bersumber dari aplikasi *mobile banking* yang digunakan. Misalkan *log* akses terhadap aplikasi, *history* transaksi yang pernah dilakukan ataupun catatan informasi transaksi yang pernah diakses, maupun data penting terkait informasi akun akses legal atau profil pengguna aplikasi *mobile banking*.

Pada tahap berikutnya peneliti menganalisa aplikasi *mobile banking* yang digunakan oleh korban. Analisis yang dilakukan bertujuan mendapatkan informasi mengenai cara kerja aplikasi yang bersumber pada perintah alur program atau *script*. Serta mengetahui bagaimana alur proses aplikasi tersebut. Dengan informasi perintah alur kerja pada aplikasi *mobile banking*, peneliti dapat mengetahui apa saja yang diperintahkan oleh *script* untuk melakukan pengamanan terkait data-data penting.

Tahap terakhir yaitu proses analisa bukti digital berkaitan dengan tindak kejahatan digital *fraud* yang bersumber di dalam perangkat *mobile* atau *smartphone* milik korban. Penggalian data potensi bukti digital tidak terfokus hanya pada aplikasi layanan *mobile banking*. Tetapi mencari informasi bukti digital pada data-data di luar aplikasi *mobile banking* yang dicurigai sebagai alat

bantu pelaku dalam memperoleh informasi akun penting berupa ID dan *Password* akses, serta PIN proses transaksi.

### 3.8. Desain Tabel Hasil Penelitian

Peneliti mengusulkan tabel hasil penelitian terhadap perangkat yang diakuisisi tertera pada Tabel 3.1. Mengacu dari penelitian yang telah dilakukan oleh Emilio Reymond Mumba dan H.S. Venter (2014) mengenai forensika bergerak dengan metode investigasi proses terstruktur.

**Tabel 3.1** Usulan tabel hasil penelitian

| No | Hasil Temuan | Sumber | Keterangan |
|---|---|---|---|
| 1 | ID Nasabah | (Path Directori) | Terenkripsi |
| 2 | Password / PIN | (Path Directori) | Terenkripsi |
| 3 | Data Log | (Path Directori) | Gambar 3.x |
| 4 | | | |
| 5 | | | |

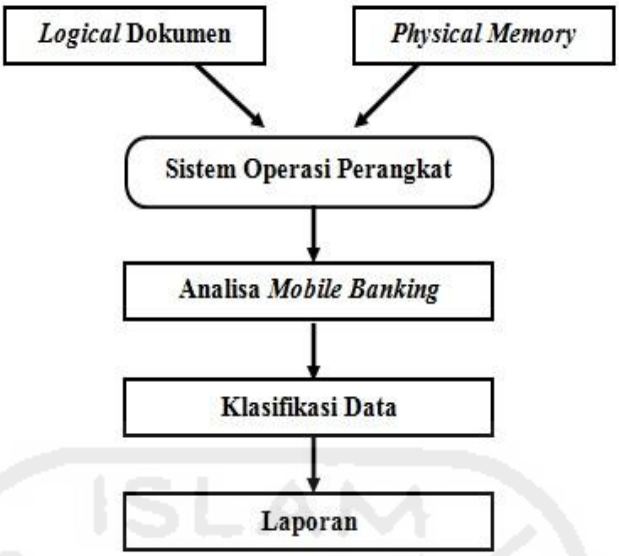
Penjelasan mengenai Tabel 3.1, pada kolom hasil temuan merupakan poin-poin apa saja yang menjadi hasil analisa pencarian data pada aplikasi *mobile banking*. Hal-hal yang diprioritaskan menjadi peran penting di dalam alur kinerja atau alur akses, bermula dari perangkat pendukung *mobile banking* milik nasabah, kemudian dilanjutkan proses permintaan transaksi kepada sistem perbankan, hingga proses pasca transaksi yang telah dilakukan oleh nasabah.

Kolom sumber adalah penjelasan di mana hasil analisa tersebut dapat ditemukan. Baik bersumber dari direktori folder (hasil ekstraksi), maupun dari alur program (*script* / artefak) pada aplikasi *mobile banking*. Singkatnya peneliti dapat menjelaskan secara teknis di mana sumber hasil temuan tersebut berada.

Pada kolom keterangan merupakan penjelasan teknis atau penjelasan analisa terhadap hasil temuan. Misalkan temuan ID nasabah dapat dijelaskan bahwa hasil temuan tersebut dalam bentuk *plain text* atau terenkripsi. Penjelasan hasil temuan dapat pula menjelaskan keadaan yang sebenarnya terhadap hasil analisa dari aplikasi *mobile banking*.

### 3.9. Desain Analisa Penelitian

Mengacu pada penelitian yang telah dilakukan oleh Qian Zhicong dan tim (2008), peneliti mengkonsep model analisa *mobile forensic* pada aplikasi *mobile banking* terilustrasikan pada Gambar 3.9.




**Gambar 3.9** Ilustrasi desain analisa penelitian

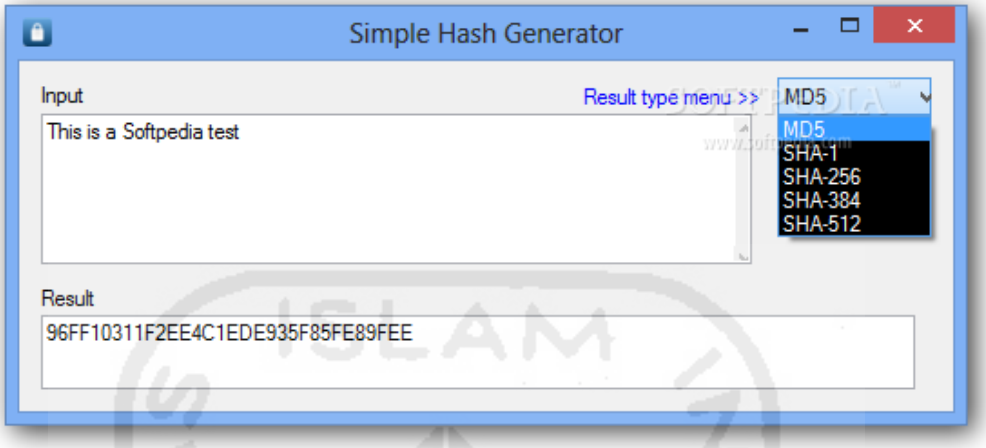
Peneliti terlebih dahulu memisahkan jenis penyimpanan yang digunakan oleh perangkat *smartphone*, antara dokumen *logical* dengan memori fisik. Selanjutnya melakukan analisa terhadap seluruh folder dan data yang terkait dengan aplikasi *mobile banking*. Proses analisa dilakukan secara manual untuk mencari data-data yang dicurigai sebagai catatan transaksi ilegal. Serta langkah analisa manual dilakukan karena diperlukan ketelitian pembedahan data.

Setelah proses analisa, peneliti mengklasifikasikan data terkait catatan transaksi dari *mobile banking*. Memisahkan antara catatan transaksi secara legal yang dilakukan oleh pemilik akun resmi, dengan catatan transaksi ilegal atau yang tidak diketahui (tidak dilakukan) oleh nasabah. Tahap terakhir dilakukan penyajian data atau laporan hasil investigasi.

## 3.10. Verifikasi Data

Setelah peneliti melakukan akuisisi dan ekstraksi terhadap *smartphone* yang digunakan sebagai perangkat transaksi (aplikasi *mobile banking*), kemudian dilakukan verifikasi pengujian kecocokan antara file *image* akuisisi terhadap perangkat barang bukti. Guna mencocokan keaslian data hasil *imaging* dengan data asli yang terdapat pada barang bukti. Hal tersebut dilakukan sebagai pembuktian keberhasilan dari tahap akuisisi sehingga data *image* dapat dianggap sah untuk proses hukum. Proses verifikasi yang akan dilakukan guna mencocokan nilai *hash* antara log data hasil analisis dengan log pada data asli (barang bukti).

Peneliti menggunakan *software tool* atau alat bantu perangkat lunak berupa *Hash Generator* untuk mencocokan nilai *hash* MD5. Dengan contoh tampilan seperti pada Gambar 3.10.




**Gambar 3.10** Contoh penggunaan aplikasi Hash Generator

Selanjutnya peneliti akan menyajikan hasil dari verifikasi kecocokan antara nilai *hash* data *image* dengan data asli dalam bentuk tabel agar mudah dibaca dan dipahami.

**Tabel 3.2** Contoh tabel penyajian verifikasi kecocokan barang bukti

| No | Log Sumber | Log Hasil Analisis | Keterangan |
|---|---|---|---|
| 1 | 9d59fa561cc102eabd2105f534ac4679 | 9d59fa561cc102eabd2105f534ac4679 | Hasil MD5 BB1 cocok |
| 2 | 25ebac623928116bdaa7317154f69bae | 25ebac623928116bdaa7317154f69bae | Hasil MD5 BB2 cocok |
| 3 | .... | ..... | |

Peneliti melakukan verifikasi data menggunakan kecocokan nilai *hash* MD5 antara data yang dianalisa terhadap barang bukti sebagai pembuktian bahwa benar adanya proses analisa terhadap data digital secara otentik bersumber dari barang bukti. Sebatas pembuktian validasi kecocokan nilai *hash* MD5.