PENGEMBANGAN *MOBILE FORENSICS* PADA APLIKASI *MOBILE BANKING* MENGGUNAKAN METODE *STATIC FORENSIC*

Adam Prayogo Kuncoro, S.Kom

13917134

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2017

Lembar Pengesahan Pembimbing

PENGEMBANGAN *MOBILE FORENSICS* PADA APLIKASI *MOBILE BANKING* MENGGUNAKAN METODE *STATIC FORENSICS*

Nama: Adam Prayogo Kuncoro

NIM: 13917134

Yogyakarta, Januari 2017

Pembimbing I	Pembimbing II
Dr. Imam Riadi, M.Kom	Ahmad Luthfi, S.Kom, M.Kom

Lembar Pengesahan Penguji

PENGEMBANGAN *MOBILE FORENSICS* PADA APLIKASI *MOBILE BANKING* MENGGUNAKAN METODE *STATIC FORENSICS*

Nama: Adam Prayogo Kuncoro

NIM: 13917134

Yogyakarta, Januari 2017

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Ahmad Luthfi, S.Kom, M.Kom
Anggota I

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

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

Abstrak

Masyarakat modern saat ini sering melakukan transaksi melalui perbankan untuk berbagai macam keperluan. Misalkan transfer antar rekening ataupun antar bank, pembayaran abonemen bulanan, dan lain sebagainya. Untuk memudahkan transaksi tersebut, banyak perbankan memberikan salah satu pelayanan kepada para nasabah berupa aplikasi *mobile banking*. Namun semakin canggih teknologi yang digunakan dalam memberikan layanan tersebut, maka semakin besar pula ancaman tindak kejahatan di dunia *cyber* di sekitar nasabah.

Melalui cara analisa forensik data dengan metode static forensik diharapkan dapat mendapatkan informasi atau data penting yang dapat digunakan sebagai bukti digital. Misalkan *log* akses, catatan transaksi, profil nasabah, dan sebagainya. Karena informasi penting tersebut dapat disalahgunakan sebagai celah keamanan untuk melakukan akses ilegal.

Penelitian ini difokuskan pada analisis dari aplikasi *mobile banking log* data, hasil yang diharapkan mencapai 80%. Setelah pengujian dan analisis dari aplikasi *mobile banking*, tidak ada informasi penting yang dapat digunakan untuk akses yang tidak sah. Dan tingkat keamanan yang diterapkan cukup modern untuk mengamankan dari tindakan akses yang tidak sah.

Kata kunci : *mobile banking*, keamanan, *mobile forensic*, *log*

Abstract

Modern society often conducts transactions through the banking system in many purposes. Suppose transfers between accounts or between banks, monthly subscription payments, and so forth. To facilitate such transactions, many banks provide a service to customers in the form of mobile banking applications. But the increasingly sophisticated technology used in providing the service, the greater the threat of cybercrime in the world around customers.

By way of forensic analysis forensic data with the static method expected to obtain important information or data that can be used as digital evidence. Suppose the access log, transaction records, customer profiles, and so on. Because the important information that can be misused as a security loophole to carry out illegal access.

This study focused on the analysis of the log data mobile banking application, expected results reached 80%. After testing and analysis of the mobile banking application, there is no important information that can be used for unauthorized access. And the security level applied modern enough to secure from unauthorized access action.

Keywords : Mobile Banking, Mobile Forensics, Log, Security

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, Desember 2016

Adam Prayogo Kuncoro, S.Kom

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis.

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

BISMILLAHIRRAHMANIRRAHIM...

Kupersembahkan karyaku ini kepada orang-orang yang telah mengajariku belajar memaknai kehidupan :

1. Ayahku pahlawanku, Ibuku yang menjadi rumah bagiku, dan kedua adik tersayang.
2. Orang tua bagiku yang selalu memberikan dukungan dan doa.
3. Istri dan anak-anak ku tercinta yang selalu mendukung dan mendoakan tiap langkahku.
4. Terima kasih atas segala bantuan dan doa dari teman-teman seperjuangan studi yang tidak dapat saya sebutkan satu persatu.
5. Dr. R. Teduh Dirgahayu, ST, M.Sc selaku Direktur Program Pascasarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia.
6. Bapak Dr. Imam Riadi, M.Kom dan Bapak Ahmad Luthfi, M.Kom selaku Dosen Pembimbing yang telah memberikan ilmu, waktu dan pemikiran Beliau dalam penyusunan tesis ini.
7. Bapak Yudi Prayudi, S.Si, M.Kom selaku Dosen Penguji dalam penelitian tesis ini dan memberikan bimbingan kepada penulis selama masa studi.
8. Seluruh staf pengajaran Program Studi Pascasarjana Teknik Informatika, Universitas Islam Indonesia yang dengan ikhlas mensuport penulis selama masa studi.
9. Terima kasih kepada pihak-pihak lain yang tidak dapat disebutkan satu persatu telah mendukung sepenuhnya atas proses studi penulis hingga akhir masa studi pascasarjana.

Akhir kata, semoga tesis ini memberikan manfaat bagi penulis dan seluruh pembaca untuk dapat memberikan ilmu yang telah diperoleh.

Yogyakarta, Desember 2016

Adam Prayogo Kuncoro, S.Kom

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Alhamdulillah atas segala rahmat yang diberikan oleh Allah SWT. Sholawat dan salam selalu disanjungkan kepada Nabi Muhammad SAW. Atas ridho Allah *ta'ala* tesis yang berjudul "PENGEMBANGAN *MOBILE FORENSICS* PADA APLIKASI *MOBILE BANKING* MENGGUNAKAN METODE *STATIC FORENSIC*" dapat diselesaikan dengan baik. Tesis ini merupakan syarat terakhir yang harus ditempuh untuk menyelesaikan pendidikan pada jenjang pascasarjana (S2), Program Pascasarjana Teknik Informatika, Universitas Islam Indonesia. Ucapan terima kasih saya haturkan kepada :

1. Dr. R. Teduh Dirgahayu, ST, M.Sc selaku Direktur Program Pascasarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia.
2. Bapak Dr. Imam Riadi, M.Kom dan Bapak Ahmad Luthfi, M.Kom selaku Dosen Pembimbing yang telah memberikan ilmu, waktu dan pemikiran Beliau dalam penyusunan tesis ini.
3. Bapak Yudi Prayudi, S.Si, M.Kom selaku Dosen Penguji dalam penelitian tesis ini dan memberikan bimbingan kepada penulis selama masa studi.
4. Seluruh staf pengajaran Program Studi Pascasarjana Teknik Informatika, Universitas Islam Indonesia yang dengan ikhlas mensuport penulis selama masa studi.
5. Terima kasih kepada pihak-pihak lain yang tidak dapat disebutkan satu persatu telah mendukung sepenuhnya atas proses studi penulis hingga akhir masa studi pascasarjana.

Penulis menyadari bahwa karya tulis ini masih jauh dari sempurna, kritik dan saran yang membangun sangat penulis harapkan. Semoga tesis ini dapat menjadi manfaat bagi orang lain dan penulis sendiri. Semoga Allah *ta'ala* selalu meridhoi seluruh umat-Nya. Aamiin...

Wassalamu'alaikum Wr. Wb.

Yogyakarta, Desember 2016

Adam Prayogo Kuncoro, S.Kom

Daftar Isi

Daftar Tabel

Daftar Gambar

Bab 1 Pendahuluan

1.1. Latar Belakang

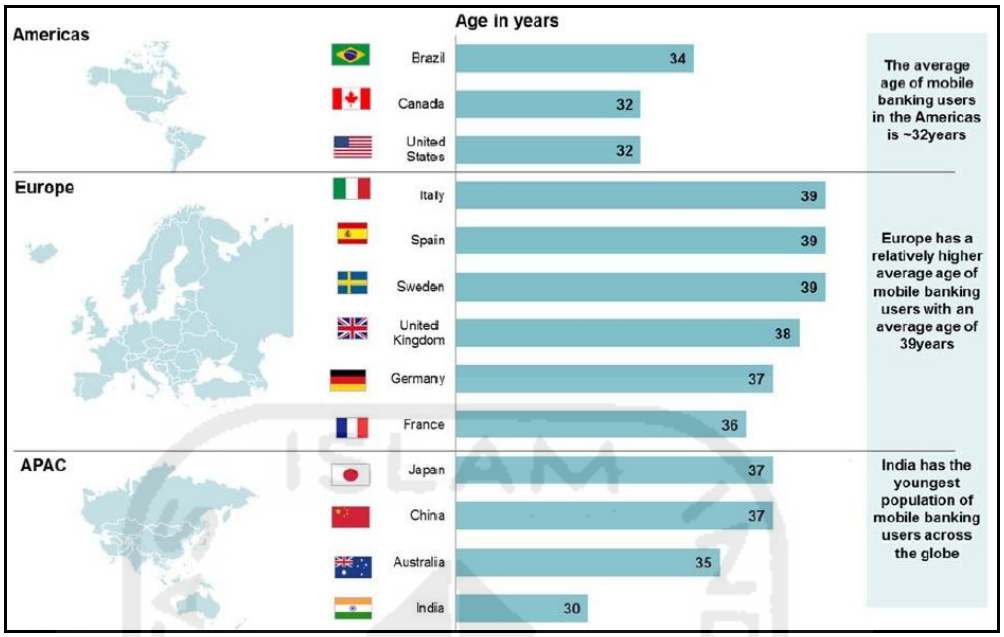
Masyarakat modern saat ini sering melakukan transaksi melalui perbankan untuk berbagai macam keperluan. Misalkan transfer antar rekening ataupun antar bank, pembayaran abonemen bulanan, dan lain sebagainya. Untuk memudahkan transaksi tersebut, setiap perbankan memberikan pelayanan kepada para nasabah dengan menggunakan berbagai macam cara. Salah satunya yaitu memberikan pelayanan berupa aplikasi *Mobile Banking*.

Aplikasi *mobile banking* merupakan sebuah piranti lunak yang dapat disematkan ke dalam ponsel pintar. *Mobile banking* dapat didefinisikan sebagai kemampuan untuk menjalankan transaksi perbankan melalui suatu peralatan yang bergerak (*mobile device*), atau lebih luas lagi untuk menjalankan transaksi keuangan melalui terminal bergerak (*mobile terminal*) (Drexelius dan Herzig, 2002).

Dengan memanfaatkan fasilitas *mobile banking* dapat membantu dan mempermudah keperluan masyarakat dalam melakukan kebutuhan transaksi yang berkaitan dengan perbankan. *Mobil*e *banking* memiliki kemampuan melakukan kegiatan perbankan secara virtual kapan pun (tanpa batasan waktu) dan di mana pun (tanpa batasan lokasi) (Kiesnoski, 2002).

Setiap aplikasi *mobile banking* memiliki fasilitas yang berbeda antar perbankan. Tetapi pada umumnya fasilitas yang tersedia antara lain yaitu untuk proses transfer antar rekening ataupun transfer antar bank, pembayaran abonemen bulanan ataupun pembelian *voucher* pulsa, pengecekan saldo dan mutasi transaksi yang pernah dilakukan oleh nasabah, dan lain sebagainya.

Pada hasil survei yang dilakukan oleh Badan KPMG (sebuah perseroan terbatas yang beroperasi di Inggris) bekerja sama dengan lembaga UBS *Evidence Lab* dalam melakukan penelitian dan survei terhadap daya minat masyarakat global / dunia dalam menggunakan fasilitas *mobile banking* yang saat ini semakin berkembang. Diperoleh data sebagaimana tertera pada Gambar 1.1.



Gambar 1.1 *Grafik pengguna fasilitas* mobile banking *di dunia ditinjau dari usia pengguna*
(Sumber : KPMG Inggris bekerja sama dengan UBS *Evidence Lab* - 2015)

Pada Gambar 1.1 menjelaskan bahwa para pengguna *mobile banking* efektif di dunia memiliki rentang usia antara 30 sampai dengan 39 tahun. Dan pada penelitian tersebut menghasilkan penemuan bahwa tingkat pengguna layanan fasilitas *mobile banking* tertinggi berada di wilayah Asia, antara lain yaitu negara India dan Cina dengan rentang penggunanya antara 60% hingga 70% dari jumlah akun aktif perbankan di kedua negara tersebut. Dibandingkan dengan negara-negara di Amerika Serikat, Kanada dan Inggris yang mayoritas masyarakatnya masih tidak terlalu memerlukan fasilitas dari *mobile banking* yang ditawarkan oleh perbankan (KPMG, 2015).

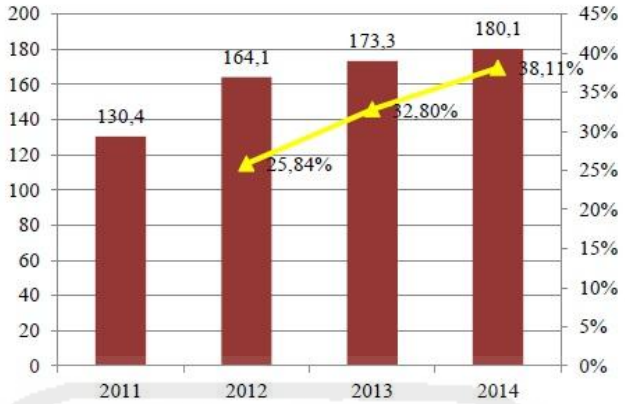
Masyarakat pengguna layanan *mobile banking* di Indonesia semakin meningkat penggunanya. Meski sebagian besar masyarakat tidak memiliki kartu kredit, kian banyak warga yang terhubung dengan Internet melalui *smartphone* untuk melakukan transaksi. Meningkatnya minat masyarakat terhadap layanan *mobile banking* didukung pula dengan semakin banyaknya *e-commerce* atau sistem berbelanja secara *online* tanpa harus melakukan transaksi secara fisik. Sehingga proses transaksi pembayaran dapat dilakukan dengan cara yang mudah dan efisien, khususnya bagi pengguna layanan *mobile banking* dapat melakukan pembayaran belanja *online* kapan saja dan di mana saja.

Data terkait peningkatan jumlah masyarakat pengguna layanan *mobile banking* yang difasilitasi oleh 4 (empat) bank di Indonesia tercatat sekitar 23,65 juta pada awal tahun 2015. Jumlah tersebut meningkat 25% (persen) dari jumlah pengguna *mobile banking* pada tahun 2014, tercatat sekitar 18,8 juta pengguna. Data tersebut tersaji dalam grafik pada Gambar 1.2 yang bersumber dari Sharing Vision.

Gambar 1.2 Data pengguna mobile banking di Indonesia pada tahun 2015

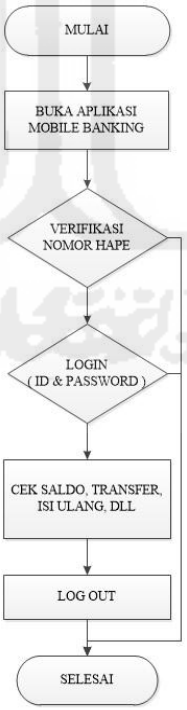
(Sumber : https://sharingvision.com/2015/05/pertumbuhan-smsmobile-banking-di-indonesia/)

Peningkatan pengguna layanan *mobile banking* didukung dari topologi wilayah perkotaan yang semakin meluas. Selain itu ada pula efek berantai tentang kepuasan para nasabah perbankan secara umum yang saling mengaplikasikan pemanfaatan *mobile banking* dalam kehidupan sehari-hari. Dan efek terbesar yang dapat kita perhatikan di kalangan masyarakat modern Indonesia adalah karena meningkatnya jumlah pengguna *smartphone* di Indonesia. Hal tersebut sangat mendukung penggunaan fasilitas *mobile banking*. Seperti hasil survey yang dilakukan pada tahun 2015 tentang peningkatan jumlah pengguna *smartphone* di Indonesia sejak tahun 2011 hingga 2014 tersaji pada Gambar 1.2.



Gambar 1.3 Jumlah pengguna smartphone di Indonesia (dalam jumlah juta orang)

Tingginya minat masyarakat dalam menggunakan layanan aplikasi *mobile banking* ini memiliki risiko dan ancaman bahaya dari pelaku tindak kejahatan *cyber crime* yang dapat mengakibatkan kerugian material. Salah satu tindak kejahatan tersebut yaitu dengan cara menduplikasi (kloning) otorisasi akses *mobile banking* tersebut. Sistem perbankan tidak mengetahui apakah transaksi yang dilakukan dari fasilitas *mobile banking* benar-benar berasal dari nasabah pemilik akun tabungan yang asli atau bukan.



Gambar 1.4 Diagram alur proses penggunaan aplikasi *mobile banking*

(Sumber : analisa penggunaan aplikasi *mobile banking* milik sebuah bank di Indonesia)

Pada Gambar 1.3 merupakan penerapan analisa pada sebuah aplikasi *mobile banking* milik sebuah bank di Indonesia menggunakan perangkat *smartphone* guna mengetahui bagaimana alur proses penggunaan aplikasi tersebut oleh nasabah. Dimana aplikasi *mobile banking* memerlukan verifikasi terhadap nomor telepon selular yang digunakan dalam *smartphone* sebagai identitas pengenal yang menyatakan pengguna / nasabah yang berhak mengakses ke tahap *log in* berikutnya. Setelah aplikasi melakukan verifikasi nomor telepon selular kemudian diperlukan ID dan *password* atau PIN akses untuk dapat melanjutkan penggunaan fasilitas transaksi pada aplikasi *mobile banking* tersebut (transfer, cek saldo, pembelian, isi ulang, dll).

Seiring dengan meningkatnya penggunaan layanan *mobile banking* di kalangan masyarakat Indonesia, semakin besar pula potensi kejahatan yang dilakukan dengan memanfaatkan perangkat *smartphone* para pengguna. Kasus tindak kejahatan digital yang menjadikan para pengguna *mobile banking* sebagai target terangkum pada Tabel 1.1.

Tabel 1.1 Kasus tindak kejahatan digital terkait layanan mobile banking

Tindak Kejahatan & Sumber Berita	Kronologi	Tanggal Terbit
Aplikasi *mobile banking* palsu (http://tekno.liputan6.com/ read/2446888/kemkominfo-dan-ojk-bakal-usut-kasus-aplikasi-mobile-banking-palsu)	Masyarakat tidak mengetahui bahwa aplikasi *mobile banking* yang diunduh dan diinstal pada perangkat *smartphone* adalah palsu atau tidak dirilis resmi oleh sebuah bank di Indonesia, sehingga pelaku kejahatan penyebar aplikasi palsu tersebut memiliki akun akses terhadap layanan *mobile banking* yang asli	28/02/2016
SMS *phising* terkait undian palsu dan aktivasi layanan *mobile banking* (http://www.antaranews.com/ berita/371225/bca-deteksi-lima-kasus-tren-kriminal-perbankan)	Pelaku mengirimkan SMS *phising* yang berisikan info undian berhadiah dan target harus mengaktifkan layanan *mobile banking* kepada target untuk mengirimkan akun akses	25/04/2013

Tabel 1.1 Kasus tindak kejahatan digital terkait layanan mobile banking (Lanjutan)

Tindak Kejahatan & Sumber Berita	Kronologi	Tanggal Terbit
Fraud aplikasi layanan mobile banking (http://www.laporpolisi.com/ 3320/penipuan-membobol-tabungan-dengan-mobile-banking)	Seorang korban mengalami kerugian uang sejumlah 19 juta rupiah, bersumber dari aplikasi layanan *mobile banking* yang dia gunakan. Korban tidak mengetahui bagaimana cara pelaku melakukan tindak kejahatan pembobolan rekening miliknya yang menggunakan ID dan *password* aplikasi *mobile banking*	11/01/2016
Penipuan undian berhadiah dan transaksi menggunakan *mobile banking* (http://www.ihsanulafwan.com/ index.php/2015/08/15/awas-penipuan-berbasis-m-banking/)	Pelaku menghubungi korban memberikan informasi palsu bahwa korban menjadi pemenang undian berhadiah dan uang akan ditransfer ke rekening korban. Kemudian pelaku meyakinkan korban untuk membuat akun *mobile banking* terlebih dahulu dan menuntun korban untuk memproses registrasi via ATM. Tetapi nomor telepon yang didaftarkan adalah milik pelaku.	15/08/2015

Berdasarkan gambaran latar belakang yang telah dipaparkan maka ranah tujuan yang akan dilakukan oleh peneliti adalah menggali informasi berpotensi sebagai bukti digital pada perangkat *smartphone* berbasis android yang berkaitan dengan aplikasi *mobile banking* sebagai upaya membantu melengkapi informasi pada aktivitas *mobile forensic* dan menganalisa faktor-faktor terkait cara kerja tindak kejahatan digital terhadap para pengguna layanan *mobile banking*.

1.2. Perumusan Masalah

Berdasarkan latar belakang penelitian yang telah dipaparkan, berikut ini adalah beberapa rumusan masalah yang akan dikaji oleh peneliti :

A. Bagaimana proses forensik pada kejahatan digital dalam penggunaan layanan *mobile banking*

B. Apa saja bukti digital yang terkait tindak kejahatan terhadap layanan *mobile banking*?

1.3. Batasan Penelitian

Untuk lebih memfokuskan arah penelitian yang dilakukan dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya maka peneliti memberikan batasan dalam penelitian ini yaitu :

A. Penelitian hanya berlingkup pada aplikasi *mobile banking* yang sedang diteliti.

B. Penelitiaan menggunakan ponsel pintar berbasis android dengan sistem operasi versi 5.1.1 Lollipop.

C. Peneliti melakukan penggalian informasi pada aplikasi *mobile banking* dengan menggunakan *tools digital forensics* platform windows

1.4. Tujuan Penelitian

Adapun beberapa tujuan yang ingin dicapai dari penelitian ini yaitu :

A. Melakukan investigasi forensik guna mencari bukti digital terhadap kejahatan terkait layanan *mobile banking*.

B. Mengetahui data apa saja yang dapat digunakan sebagai penunjang bukti digital terhadap layanan *mobile banking*.

1.5. Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat yang ingin dicapai dalam penelitian ini yaitu :

A. Untuk pengembangan ilmu pengetahuan

a. Memberikan panduan dalam proses investigasi *forensics* pada perangkat *mobile* yang menggunakan aplikasi *mobile banking*

b. Sebagai pendalaman materi dalam bidang *mobile forensics*

B. Untuk Penelitian Selanjutnya

Sebagai bahan referensi untuk penelitian berikutnya yang meneliti tentang seputar aplikasi *mobile banking*, atau dapat digunakan untuk memperkaya wawasan untuk pengembangan penelitian pada bidang *mobile forensics*

C. Untuk Peneliti

Penelitian ini diharapkan dapat menambah wawasan dan kualitas keilmuan baik dalam hal teori maupun praktik

1.6. Metode Pengumpulan Data

Adapun langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut :

A. Studi Literatur

Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan keamanan *mobile banking*, penggunaan fasilitas aplikasi *mobile banking* dan materi-materi yang berkaitan dengan *mobile forensics* serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

B. Analisis

Tahapan analisis ini dilakukan terhadap informasi yang terdapat dalam aplikasi *mobile banking* yang dapat memiliki nilai bukti digital serta analisa penggunaan *tools mobile forensics* yang dapat difungsikan untuk menarik data dari aplikasi *mobile banking* tersebut.

C. Perancangan

Pada tahapan perancangan ini peneliti memberikan perancangan terkait dengan tahapan apa saja yang akan dilakukan untuk melakukan penarikan data dari aplikasi *mobile banking*.

D. Implementasi

Tahapan implementasi yang dimaksud yaitu mengimplementasikan perancangan yang telah dibuat sebelumnya untuk dapat diaplikasikan terhadap penelitian.

E. Ujicoba dan Analisis

Tahapan ini bertujuan untuk mengetahui keberhasilan dalam penarikan data dan informasi dari aplikasi *mobile banking* serta menganalisa informasi yang telah berhasil ditarik dengan metode *static forensics*.

F. Laporan

Tahapan laporan adalah tahapan akhir yaitu penyampaian kesimpulan atas hasil dari penelitian ini. Dan dapat pula dilakukan komparasi hasil penelitian terhadap kajian penelitian orang lain.

1.7. Sistematika Penulisan

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika penulisan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam penulisan.

A. Bab I : Pendahuluan

Tahapan ini merupakan tahapan awal yang dilakukan dalam penelitian. Pada tahapan ini berisikan penjelasan terkait dengan latar belakang penelitian antara lain penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan yang dilakukan.

B. Bab II : Landasan Teori

Pada tahapan ini membahas tentang beberapa teori yang mendukung dalam penelitian yang dilakukan, terkait dengan *mobile banking*, *mobile forensics* dan *static forensics*.

C. Bab III : Analisa dan Perancangan

Tahapan ini berisikan gambaran secara umum tentang analisa yang dilakukan terhadap masing-masing tahapan penelitian dan menganalisa hasil penelitian, serta melakukan perancangan metode penelitian dan penggunaan aplikasi dalam melakukan implementasi terhadap pelaksanaan penelitian.

D. Bab IV : Implementasi

Tahapan ini membahas tentang implementasi dari tahapan penelitian sistem keamanan aplikasi *mobile banking* serta penggunaan *tools mobile forensics* dan kemudian melakukan analisa hasil penelitian.

E. Bab V : Kesimpulan dan Saran

Tahapan ini adalah merupakan tahapan terakhir yang dilakukuan peneliti dengan memaparkan kesimpulan dari keseluruhan uraian pada setiap bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan ilmu pengetahuan di kemudian hari.

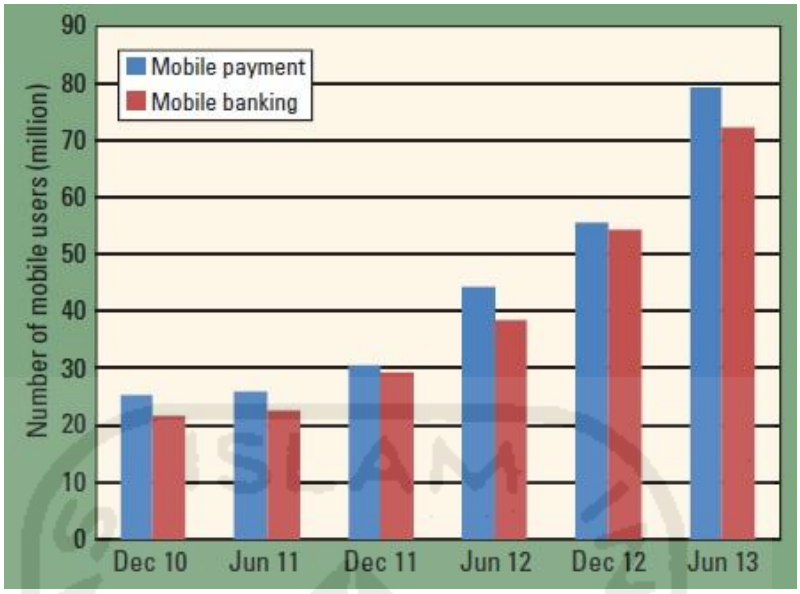
Bab 2 Tinjauan Pustaka

2.1. Penelitian Terdahulu

Penelitian yang terkait dengan *mobile forensics* telah banyak dilakukan, terlebih saat ini banyak sekali fungsi serta kegunaan dari perangkat *smartphone* atau perangkat *mobile* lainnya. Jika kita tinjau dari segi kegunaan *smartphone* sekarang ini tidak dapat dipisahkan dari masyarakat modern global yang cenderung sudah 'kecanduan'. Beberapa fasilitas yang ditawarkan dari produsen *smartphone* yaitu guna memudahkan masyarakat untuk melakukan rutinitas harian baik dari segi pribadi ataupun sosial.

Menurut penelitian yang dilakukan oleh (Purwanegara et al. 2014) mengemukakan bahwa perkembangan saat ini ada peningkatan jumlah pengguna *mobile banking* internet untuk melakukan transaksi di tengah kesibukan masyarakat modern. Teknologi *mobile banking* memungkinkan orang untuk melakukan transaksi kapan saja dan di mana saja. Sehingga perbankan saat ini menawarkan berbagai layanan transaksi secara *mobile* untuk memudahkan para nasabah. Dan penyediaan layanan elektronik *mobile* semacam itu hanya membutuhkan biaya yang relatif lebih murah jika dibandingkan dengan biaya penempatan sebuah mesin ATM (*Automated Teller Machine*) beserta dengan biaya pemeliharaannya.

Pada tahun 2014 Wai-Ming To dan Linda S.L Lai melakukan sebuah penelitian tentang penggunaan layanan *mobile banking* di Cina. Tingginya penggunaan layanan *mobile banking* dan pembayaran secara *online* di Cina didukung oleh pesatnya perkembangan internet dan kemudahan teknologi untuk digunakan dalam membantu kegiatan masyarakat sehari-hari. Bahkan sejak awal tahun 2008 penggunaan internet di Cina telah melampaui Amerika Serikat, yang diproyeksikan sekitar 690 juta total pengguna akses internet di dunia. Pada tahun itu juga merupakan salah satu tahun pemasaran ponsel pintar dengan tingkat besar di dunia, dengan total pengguna *smartphone* diperkirakan sebanyak 451 juta jiwa. Seperti yang tertera pada Gambar 2.1 di bawah ini yang menjelaskan tentang peningkatan penggunaan layanan *mobile banking* dan pembayaran secara *online* di Cina sejak tahun 2010 hingga 2013 (To & Lai 2014).



Gambar 2.1 Tingkat pengguna layanan *mobile banking* dan *mobile payment* di Cina (Sumber : (To & Lai 2014))

Penelitian yang dilakukan oleh Azham Hussain, Hamisu Ibrahim Abubakar dan Norlaily Binti Hashim (2014) tentang mengevaluasi aplikasi *mobile banking* dari segi pengukuran dan sudut pandang penggunaan. Salah satu tolak ukur penentu keberhasilan sebuah aplikasi *mobile banking* adalah kemudahan aplikasi tersebut untuk dapat digunakan (*user friendly*). Serta terdapat empat poin penting dalam menentukan penilaian untuk menilai sebuah aplikasi *mobile banking* yang ditawarkan kepada para penggunanya. Antara lain yaitu efisiensi, efektifitas, aman dan sederhana (tidak menyulitkan) dalam penggunaannya (Hussain et al. 2015).

Meninjau dari ketiga penelitian di atas, peneliti tertarik untuk melakukan studi analisa terhadap aplikasi *mobile banking* karena di Indonesia telah banyak masyarakat yang memanfaatkan fasilitas tersebut. Namun hanya sedikit nasabah yang menyadari perlunya kewaspadaan tentang keamanan dalam bertransaksi menggunakan *mobile banking*. Peneliti bertujuan menganalisa data penting yang terdapat dalam sistem aplikasi *mobile banking*, data yang berpotensi sebagai *vulnerability* tindak kejahatan digital berupa transaksi tanpa diketahui oleh pemilik akun perbankan atau nasabah.

Tahun 2013 Zilole Simate dari Universitas Copperbelt di Kitwe, Zambia, melakukan penelitian mengevaluasi keamanan *mobile network* dalam Kasus Transaksi *Mobile* di Zambia. Dia mengemukakan bahwa dengan memperkenalkan kemudahan fasilitas transaksi *mobile*

banking telah mengubah pola hidup masyarakat modern menjadi lebih dinamis. Namun dari transaksi yang dilakukan dapat terancam oleh adanya tindak kejahatan digital, karena masih kurangnya tingkat keamanan terhadap jaringan GSM yang digunakan. Khususnya jaringan 2G yang masih banyak digunakan di Zambia. Meskipun penggunaan jaringan GSM 3G akan disebar dan cenderung memiliki tingkat keamanan yang lebih baik. Hal ini merupakan salah satu alasan mengapa operator selular harus turut menjaga keamanan jaringan dan mengikuti regulasi keamanan secara internasional. Peneliti mengutip penelitian Zilole Simate karena memiliki kesimpulan bahwa jaringan GSM sebagai jalur internet pendukung fasilitas *mobile banking* telah memiliki sistem keamanan yang dapat membentengi tindak kejahatan digital sebelum pelaku dapat mengakses ke dalam sistem bank (Simate 2013).

Penelitian yang dilakukan Thomas Zefferer dan Peter Teufl (2013) mengenai Penilaian Kebijakan Keamanan Pengguna Perangkat *Mobile* : Sebuah Alternatif Managemen Solusi Perangkat *Mobile* untuk Ponsel Pintar Android, mengkritisi level keamanan dan integritas keamanan perangkat yang digunakan untuk transaksi *mobile*. Banyak para pengguna *smartphone* menonaktifkan fitur keamanan demi kenyamanan, bahkan ada pula pengguna menginstal aplikasi yang tidak terpercaya sehingga tertanam *malware* di perangkat *smartphone*. *Mobile Device Management* (MDM) merupakan solusi dengan menyediakan sarana untuk pengelola aplikasi dan konfigurasi *smartphone*. MDM akan digunakan secara efektif pada layanan *mobile banking* dan *mobile government*, dengan cara bekerja sama sebagai fendor aplikasi pihak ketiga untuk dapat mengintegrasi penggunaan aplikasi yang disematkan ke dalam *smartphone,* serta menjaga fitur keamanan agar tetap aktif digunakan (Zefferer & Teufl 2013).

Penelitian tentang Analisa Potensi Kerentanan Aplikasi *Mobile Banking* yang dilakukan oleh Taenam Cho, Yunki Kim, SungBong Han, dan Seung-Hyun Seo pada tahun 2013 mengemukakan bahwa masyarakat yang menggunakan fasilitas *mobile banking* memiliki tingkat sensitifitas mengenai informasi pribadi yang digunakan dan transaksi keuangan yang dilakukan. Maka peneliti menganalisa penggunaan aplikasi *mobile banking* mengenai hak akses yang tersedia sebagai salah satu mekanisme keamanan di dalam aplikasi tersebut (Cho et al. 2013). Sistem izin hak akses yang ditanamkan pada aplikasi *mobile banking* dapat menyebabkan dampak serius jika level keamanan tersebut diketahui oleh orang lain dan digunakan tidak sesuai pemilik akses yang sebenarnya. Analisa terhadap level keamanan tersebut dapat di lihat pada Tabel 2.1.

Tabel 2.1 Analisa level keamanan yang digunakan Teanam Cho beserta tim

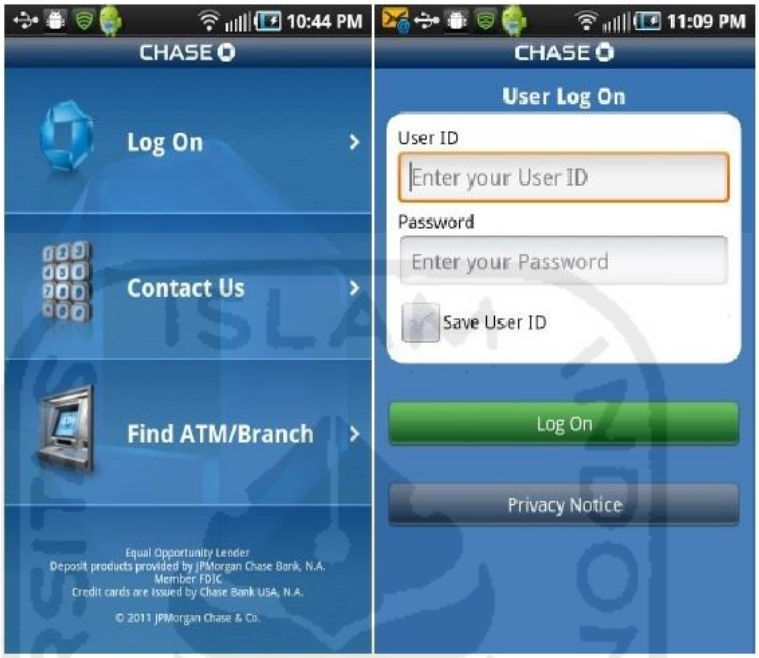
protection Level	Meaning
Normal	A lower-risk permission that gives requesting apps access to isolated app-level features, with minimal risk to other apps, the system, or the user.
Dangerous	A higher-risk permission that would give a requesting app access to private user data or control over the device that can negatively impact the user.
Signature	A permission that the system grants only if the requesting app is signed with the same certificate as the app that declared the permission.
System	A permission that the system grants only to apps that are in the Android system.

Peneliti mengutip jurnal penelitian yang dilakukan oleh Teanam Cho beserta tim karena terdapat rencana penggunaan tabel analisa mengenai level keamanan yang terdapat pada sistem aplikasi *mobile banking* yang akan diteliti. Sehingga memudahkan pembaca maupun peneliti selanjutnya untuk mengetahui apa saja level keamanan yang digunakan pada aplikasi *mobile banking* yang diteliti.

Leili Nosrati dan tim (2015) melakukan penelitian tentang Penilaian Keamanan *Mobile Banking* di Iran. Peneliti memandang tindakan *hacking* terhadap akun perbankan secara global (di dunia) telah menyebabkan kerugian yang tak terhitung nilainya. Hal tersebut dikarenakan terdapat banyak kelemahan di dalam sistem perbankan, khususnya peneliti menganalisa sistem keamanan pada aplikasi *mobile banking*. Analisa yang dilakukan bertujuan mengidentifikasi dan mengklasifikasi penyematan sistem keamanan pada *mobile banking.* Hasil yang ditemukan pada penelitian tersebut adalah penggunaan level keamanan berenkripsi, terdapat sistem otentikasi dan otorisasi yang berlapis, serta terdapat sistem keamanan *network layer* (Nosrati 2015).

Penelitian yang dilakukan oleh Biswajit Panja dan rekan-rekan (2013) meneliti tentang analisa keamanan pada aplikasi perbankan *mobile*. Mereka melakukan analisa tentang bagaimana sistem keamanan *mobile banking* dapat diretas untuk mencari informasi tentang akses pengguna dan kata sandinya. Karena pada sistem keamanan jaringan yang digunakan haruslah sudah memenuhi standar kelayakan keamanan. Baik jaringan nirkabel (*wireless*) ataupun jaringan provider GSM. Pada hasil penelitian mengemukakan bahwa sistem keamanan yang diterapkan pada aplikasi *mobile banking* tersebut hanya terdapat pada aktifitas *login* saja, sehingga kemungkinan besar untuk dilakukan tindakan *hacking* terhadap aplikasi masih sangat

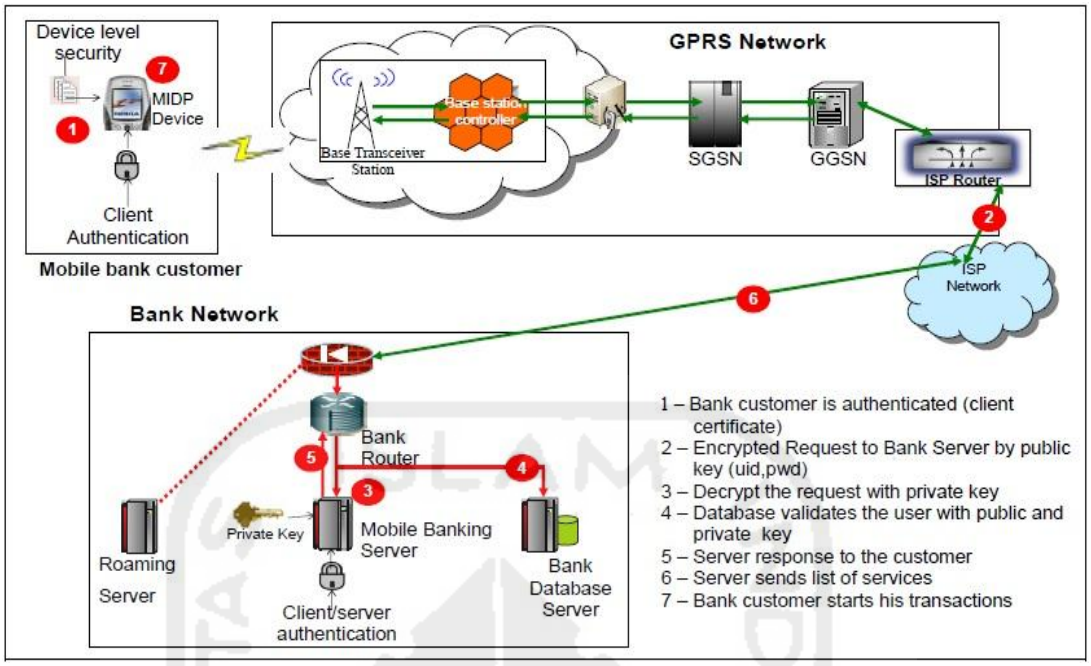
memungkinkan. Pada Gambar 2.2 merupakan tampilan *interface* halaman *login* aplikasi *mobile banking* yang telah dianalisa (Panja et al. 2013).



Gambar 2.2 Halaman *login* aplikasi *mobile banking* yang diteliti
(Sumber : Penelitian C. Narendiran dan tim, 2014)

Penelitian yang dilakukan di India oleh C. Narendiran, S. Albert Rabara dan N. Rajendran (2014) tentang sistem keamanan *mobile banking* yang menggunakan kunci infrastruktur publik, memiliki pendapat bahwa aplikasi *mobile banking* menarik karena nyaman digunakan, meskipun masih terdapat celah keamanan (Narendiran et al. 2009). Kemudian peneliti menganalisa sistem keamanan pada jaringan GSM yang digunakan untuk mengoperasikan aplikasi *mobile banking* yang dimaksud agar dapat terhubung dengan server perbankan. Dan menganalisa apa saja sistem keamanan yang digunakan pada aplikasi *mobile banking*.

Dengan hasil analisa penelitian sistem keamanan yang digunakan dalam proses kinerja aplikasi *mobile banking* tersebut yaitu menggunakan level keamanan pada jaringan GSM yang telah disediakan oleh operator selular berupa kriptografi publik, serta penggunaan tanda tangan digital dan enkripsi pesan yang terdapat di dalam aplikasi. Penjelasan gambaran level keamanan pada jaringan dan *framework* pengoperasian aplikasi *mobile banking* dapat dilihat pada Gambar 2.3.



Gambar 2.3 *Framework* keamanan *mobile banking*

(Sumber : (Narendiran et al. 2009))

Penelitian yang dilakukan oleh Sriramulu Bojjagani dan V. N. Nastry (2015) tentang Protokol Keamanan *Mobile Banking* Berbasis SMS dengan Verifikasi Formal, merupakan sebuah usulan mengenai protokol baru untuk disematkan dalam keamanan aplikasi *mobile banking*. Sistem yang akan ditanamkan pada level otentikasi dan pembayaran ini diharapkan dapat memberikan keamanan dalam komunikasi SMS antara nasabah dengan sistem bank melalui aplikasi *mobile banking*. Metode formal yang dimaksud yaitu berupa *Automated Validation of Internet Security Protocols and Aplications* (AVISPA) dan *Burrows Abadi and Needham logic* (BAN). Hasil yang diperoleh dari penelitian ini adalah meningkatnya level keamanan pada aplikasi dan meminimalisir kemungkinan serangan *hacking* melalui jaringan, karena terdapat skema kriptografi bertingkat di dalamnya (Bojjagani 2015).

Seluruh penelitian terdahulu yang telah dipaparkan telah terangkum dalam *literature review* pada Tabel 2.2.

Tabel 2.2 Tabel *literature review*

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
1	Mustika Purwanegara, Atik Apriningsih, dan Febri Andika (2013)	Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes	Peneliti melakukan survey dan ekplorasi terhadap masyarakat Indonesia yang menggunakan fasilitas *mobile banking* tentang kesadaran mereka dalam menggunakan fasilitas tersebut, memahami regulasi yang berlaku, dan mengetahui seberapa jauh bahaya atau risiko dalam penggunaan *mobile banking*	Para pengguna *mobile banking* di Indonesia secara mayoritas telah mengetahui regulasi mengenai transaksi elektronik. Dan apabila terjadi kerugian material yang menimpa, telah ada payung hukum undang-undang di Indonesia
2	Wai-Ming To dan Linda S.L Lai (2014)	Mobile Banking and Payment in China	Penelitian dilakukan terhadap tingkat penggunaan *mobile banking* di Cina. Peningkatan penggunaan *mobile banking* didukung oleh meningkatnya penggunaan *smartphone* dan akses internet yang mudah didapatkan.	Penyebaran aplikasi *mobile banking* dan pembayaran secara *online* harus diimbangi dengan tingkat keamanan dan kerahasiaan penggunanya. Serta meminimalisir resiko tentang tindak kejahatan yang akan ditimbulkan.
3	Azham Hussain, Hamisu Ibrahim Abubakar dan Norlaily Binti Hashim (2014)	Evaluating Mobile Banking Application: Usability Dimensions and Measurements	Ketertarikan akan penggunaan sebuah produk aplikasi *mobile banking* biasanya bermula dari *interface* yang mudah dipahami. Namun ditinjau pula pada penyesuaian sistem yang selalu dievaluasi terhadap tingkat pelayanan agar selalu nyaman digunakan. Evaluasi tersebut meliputi sejumlah tahapan. Dan yang utama adalah memandang penggunaan *mobile banking* dalam jangka waktu ke depan.	Pengukuran dan sudut pandang penggunaan diyakini sebagai factor kunci keberhasilan bagi penyebaran pemanfaatan piranti lunak *mobile banking*. Bahkan dapat memberikan pelayanan untuk memudahkan nasabah dalam melakukan transaksi kapan pun dan di mana pun tanpa merasakan kesulitan saat menggunakan fasilitas tersebut (*user friendly*).
4	Zilole Simate (2013)	Evaluation of Mobile Network Security A Case of Mobile Transactions in Zambia	Tingginya pengguna fasilitas *mobile banking* di Zambia masih terdapat ancaman tindak kejahatan *cyber*. Karena kurangnya penyematan enkripsi sebagai level keamanan. Serta penggunaan jaringan yang masih pada level 2G.	Pemerintah telah membuat regulasi tentang keamanan terhadap fasilitas transaksi *mobile*. Dan operator selular akan menyebar jaringan 3G yang dapat meminimalisir tindak kejahatan terhadap transaksi *mobile*.

Tabel 2.2 Tabel *literature review* (Lanjutan)

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
5	Thomas Zefferer dan Peter Teufl (2013)	Policy-based Security Assessment of Mobile End-user Devices : An Alternative to Mobile Device Management Solutions for Android Smartphones	Banyak para pengguna *smartphone* menonaktifkan fitur keamanan dengan alasan untuk kenyamanan. Bahkan tidak sedikit pengguna yang menginstal aplikasi tidak terpercaya, karena terdapat kemungkinan tertanam *malware* di dalam *smartphone*. Sehingga keamanannya terancam.	Peneliti melakukan pendekatan kepada fendor aplikasi sebagai pihak ketiga dengan menawarkan MDM (*Mobile Device Management*). Guna mengintegrasi penggunaan aplikasi yang disematkan ke dalam *smartphone*, serta menjaga fitur keamanan agar tetap aktif digunakan.
6	Teanam Cho, Yunki Kim, SungBong Han, dan Seung-Hyun Seo (2013)	Potential Vulnerability Analysis of Mobile Banking Applications	Penggunaan *smartphone* berbasis android membuat tingginya pengguna aplikasi *mobile banking*. Sehingga peneliti melakukan analisa terhadap level keamanan hak akses yang digunakan dalam aplikasi tersebut.	Peneliti mendapatkan informasi tentang level keamanan hak akses yang bertingkat dalam aplikasi *mobile banking* yang dianalisa. Tidak hanya keamanan pada *interface login* saja, melainkan ada keamanan hak akses lagi untuk dapat melakukan transaksi yang diinginkan (misalkan untuk transfer, cek saldo, pembayaran, dll).
7	Leili Nosrati dan Amir Massoud Bidgoli (2015)	Security Assessment of Mobile Banking	Peneliti menganalisa sistem keamanan pada aplikasi *mobile banking* karena terdapat *vulnerability* yang dapat dimanfaatkan oleh *hacker*. Analisa yang dilakukan bertujuan mengidentifikasi dan mengklasifikasi penyematan sistem keamanan pada *mobile banking.*	Hasil yang ditemukan pada penelitian tersebut adalah penggunaan level keamanan berenkripsi, terdapat sistem otentikasi dan otorisasi yang berlapis, serta terdapat sistem keamanan *network layer*.

Tabel 2.2 Tabel *literature review* (Lanjutan)

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
8	Biswajit Panja, Dennis Fattaleh, Mark Mercado, Adam Robinson, dan Priyanka Meharia (2013)	Cybersecurity in Banking and Financial Sector : Security Analysis of a Mobile Banking Application	Peneliti melakukan analisa terhadap aplikasi *mobile banking* mengenai apa saja level keamanan yang digunakan. Karena tidak dapat hanya mengandalkan keamanan pada jaringan saja. Pada aplikasi haruslah terdapat level keamanan yang berlapis.	Pada hasil penelitian mengemukakan bahwa sistem keamanan yang diterapkan pada aplikasi *mobile banking* tersebut hanya terdapat pada aktifitas *login* saja, sehingga kemungkinan besar untuk dilakukan tindakan *hacking* terhadap aplikasi masih sangat memungkinkan.
9	C. Narendiran, S. Albert Rabara dan N. Rajendran (2014)	Public Key Infrastructure For Mobile Banking Security	Peneliti menganalisa sistem keamanan pada jaringan GSM yang digunakan untuk mengoperasikan aplikasi *mobile banking* yang dimaksud agar dapat terhubung dengan server perbankan. Dan menganalisa apa saja sistem keamanan yang digunakan pada aplikasi *mobile banking*.	Aplikasi memanfaatkan sistem keamanan yang berlevel pada jaringan GSM yang telah disediakan oleh provider selular berupa kriptografi publik. Serta penggunaan tanda tangan digital dan enkripsi pesan yang terdapat di dalam aplikasi.
10	Sriramulu Bojjagani dan V. N. Nastry (2015)	SSMBP: A Secure SMS-based Mobile Banking Protocol with Formal Verification	Peneliti mengusulkan protokol keamanan baru berupa Automated Validation of Internet Security Protocols and Aplications (AVISPA) dan Burrows Abadi and Needham logic (BAN).	Hasil yang diperoleh dari penelitian ini adalah meningkatnya level keamanan pada aplikasi dan meminimalisir kemungkinan serangan *hacking* melalui jaringan, karena terdapat skema kriptografi bertingkat di dalamnya.

Berbeda dengan penelitian terdahulu, pada penelitian ini berada pada kategori *Mobile Forensic* dan *Live Forensic* dengan objek penelitian aplikasi *mobile banking* dari perbankan di Indonesia. Paparan singkat mengenai rencana penelitian tertulis pada Tabel 2.3.

Tabel 2.3 Penelitian yang diusulkan

Nama	Judul	Uraian Singkat	Hasil Yang Diharapkan
Adam Prayogo Kuncoro (2017)	Pengembangan Mobile Forensic Pada Aplikasi Mobile Banking Menggunakan Metode Static Forensic	Melakukan analisa dan explorasi terhadap aplikasi *mobile banking* untuk dapat memetakan karakteristik dan fungsi. Mengetahui bagaimana proses pengambilan data dan menggali informasi yang dapat digunakan dalam investigasi tindak kejahatan terhadap layanan *mobile banking*.	1) Melakukan investigasi forensik guna mencari bukti digital terhadap kejahatan terkait layanan *mobile banking*. 2) Mengetahui data apa saja yang dapat digunakan sebagai penunjang bukti digital terhadap layanan *mobile banking*.

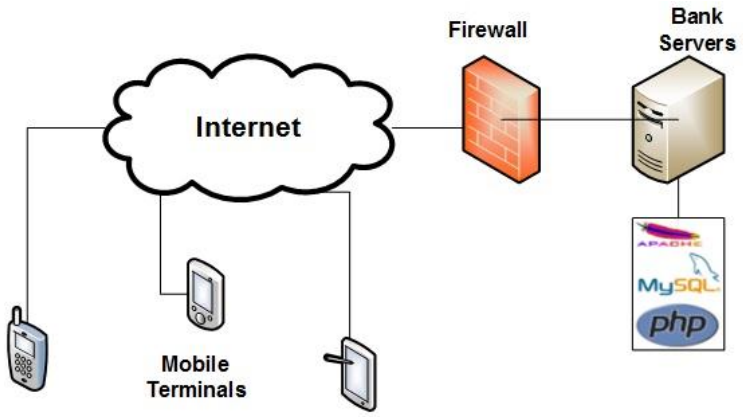
2.2. Landasan Teori

2.2.1. Mobile Banking

Mobile banking merupakan salah satu layanan perbankan yang menerapkan teknologi informasi (Hadi & Novi : 2010). Layanan ini menjadi peluang bagi bank untuk menawarkan nilai tambah kepada pelanggan. *Mobile banking* atau biasa disebut *m-banking* merupakan suatu layanan perbankan yang diberikan oleh pihak bank untuk mendukung kelancaran dan kemudahan kegiatan perbankan. Keefektifan dan keefisienan nasabah untuk melakukan berbagai transaksi *mobile banking* tidak akan berjalan jika tidak didukung oleh telepon seluler dan jaringan internet. Setiap orang yang memiliki *smartphone* dapat memanfaatkan fasilitas ini, untuk bertransaksi di mana saja dan kapan saja dengan mudah. Adanya berbagai kemudahan layanan perbankan tersebut, diharapkan nasabah merasa puas dalam menggunakan berbagai macam jasa yang diberikan oleh pihak bank.

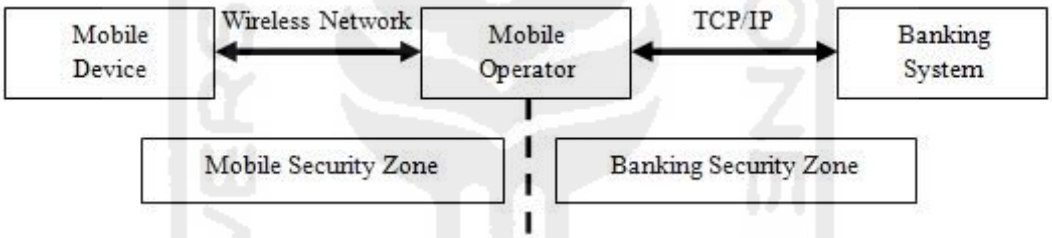
Mobile banking merupakan pengembangan dari sistem *SMS-Banking*. Meskipun sama-sama menggunakan telepon seluler sebagai sarana, *mobile banking* memiliki teknologi yang lebih baru karena menggunakan aplikasi yang harus diunduh dan diinstal ke dalam telepon seluler (*smartphone*), dibandingkan dengan *SMS-banking* yang hanya menggunakan sarana teks melalui SMS. *Mobile banking* adalah salah satu bagian dari *E-banking* yang merupakan layanan informasi perbankan via *wireless* paling baru yang ditawarkan pihak bank dengan menggunakan teknologi *smartphone* untuk mendukung kelancaran dan kemudahan kegiatan transaksi perbankan (Sulistyarini 2012).

Berbagai macam sistem keamanan yang diterapkan ke dalam layanan *mobile banking* baik dari segi perbankan, keamanan berlapis pada aplikasi, bahkan terdapat pula pemanfaatan keamanan pada jaringan yang digunakan untuk terhubung ke internet. Pada Gambar 2.4 merupakan protokol transaksi *mobile banking* secara umum.



Gambar 2.4 Protokol umum transaksi *mobile banking*

Pada Gambar 2.5 berikut ini merupakan contoh pemanfaatan sistem keamanan dari protokol jaringan selular dan keamanan server bank yang terdapat pada transaksi *mobile banking* secara umum.



Gambar 2.5 Bagan pemanfaatan keamanan pada jaringan selular dan server bank

Namun pemanfaatan keamanan dari segi jaringan selular yang digunakan dan sistem keamanan pada server bank tidak dapat mencegah tindak kejahatan pencurian menggunakan aplikasi *mobile banking* jika pelaku dapat menduplikasi hak akses resmi melalui aplikasi. Misalkan pelaku pencurian menggunakan berbagai cara untuk dapat menduplikasi hak akses resmi sehingga sistem keamanan perbankan tidak mengetahui bahwa transaksi yang dilakukan adalah perbuatan pelaku pencurian (tidak resmi), bukan bersumber dari keinginan/tindakan pemilik akun (nasabah) yang resmi. Hal tersebut dapat terjadi, jika pada aplikasi *mobile banking* tersebut tidak dilengkapi dengan sistem keamanan berlipat untuk mencegah atau meminimalisir tindak kejahatan *hacking* atau pencurian menggunakan hak akses yang terduplikasi.

Banyak sistem keamanan yang dapat disematkan ke dalam aplikasi *mobile banking* guna mencegah pengaksesan akun yang bukan bersumber dari pemilik resmi/nasabah. Diantaranya dapat menggunakan keamanan kriptografi, enkripsi, keamanan identifikasi nasabah yang berlapis

dalam setiap akan dilakukannya transaksi menggunakan pin/password yang berbeda-beda (contohnya, seperti pin token fisik pada fasilitas *internet banking*), keamanan pin yang selalu berubah dengan notifikasi SMS dari server perbankan, dan keamanan lainnya. Namun semakin tingginya penerapan sistem keamanan yang berlapis pada aplikasi *mobile banking* sebanding dengan tingginya biaya pembuatan aplikasi atau dalam pemeliharaannya dan pengembangannya. Kembali lagi kepada kebijakan perbankan yang menyediakan fasilitas tersebut untuk tetap memudahkan nasabah dalam bertransaksi tetapi keamanan dan kepercayaan nasabah tetap terjaga.

Dapat pula perbankan melakukan survei terlebih dahulu mengenai tingkat kebutuhan nasabah terhadap fasilitas *mobile banking* sebelum memberikan/me-*launching* aplikasi tersebut. Dengan tujuan untuk mengetahui dan sebagai tolak ukur seberapa pentingnya penerapan keamanan yang berlapis pada aplikasi *mobile banking* yang ditawarkan.

2.2.2. Mobile Forensic

Pada awalnya masyarakat secara awam hanya mengetahui dunia forensika hanya terdapat pada ilmu kedokteran, khususnya di lingkup masyarakat Indonesia. Namun pemahaman dan pembelajaran mengenai dunia forensika saat ini telah merambah ke berbagai aspek yang melekat di kehidupan manusia. Beberapa contoh diantaranya yaitu forensika digital mengulas informasi-informasi penting yang terdapat pada perangkat elektronik digital untuk keperluan tertentu, misalnya informasi yang dapat diperoleh dan digunakan sebagai bukti digital secara sah di hadapan hukum. Ada pula *audio forensic*, *image forensic*, dan lain sebagainya.

Sedangkan ilmu tentang *mobile forensic* merupakan salah satu bagian di dalam ilmu utama *digital forensic*. Pada *mobile forensic* ini adalah ilmu forensika yang berkaitan dengan perangkat-perangkat elektronik yang dapat dibawa ke mana pun secara mudah untuk berpindah tempat (*mobile*). Contohnya telepon seluler, *smartphone*, perangkat GPS, dan lain sebagainya.

Informasi yang dapat digunakan atau yang dapat dianalisa dalam ilmu *mobile forensic* biasanya berupa *history* SMS, *log* panggilan telepon, kontak nomor telepon yang terdapat pada telepon seluler ataupun *smartphone*, *log history* dan informasi penting yang ada di dalam aplikasi *smartphone* guna dijadikan bukti digital, serta berbagai macam informasi lainnya yang berkaitan dengan bukti digital.

Smartphone merupakan sumber dari bukti *forensic*. *Forensic* android adalah bidang di *mobile forensic*, investigasi yang dilakukan berupa pendataan dan analisis data (Walter T. dan Nagoor Meeran, 2015).

2.2.3. Static Forensic

Pada dasarnya proses akuisisi dan investigasi pemecahan kasus yang menggunakan barang bukti digital termasuk ke dalam ilmu *digital forensic*. Terdapat dua pemahaman dasar ilmu mengenai teknik forensika yaitu *live forensic* dan *static forensic*. Tidak ada perbedaan teknik dan metode yang dilakukan antara *live forensic* dengan *static forensic* yaitu identifikasi, penyimpanan, analisa dan presentasi.

Perbedaan pada *live forensic* yaitu analisa yang dilakukan secara *live* atau secara langsung saat perangkat sedang aktif (dalam posisi terhubung ke dalam jaringan). Sedangkan *static forensic* merupakan teknik analisa pada barang bukti secara *off-line*, tidak terhubung ke dalam jaringan dan investigator dapat langsung menangani perangkat barang bukti untuk diakuisisi. Misalnya analisa menggunakan teknik *static forensic* terhadap sebuah *harddisk* dapat langsung dianalisa. Contoh lainnya saat menganalisa perangkat *mobile* (*handphone* atau *smartphone*) dapat dilakukan tanpa terhubung ke dalam jaringan nirkabel.

Forensika tradisional (*static forensic*) dilakukan melalui analisa secara statis, data diawetkan (disimpan melalui proses *cloning* terlebih dahulu) pada media penyimpanan permanen. Tidak semua data diperlukan untuk memahami keadaan (menginvestigasi) dari sistem yang diperiksa (Mrdovic et al. 2009).

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

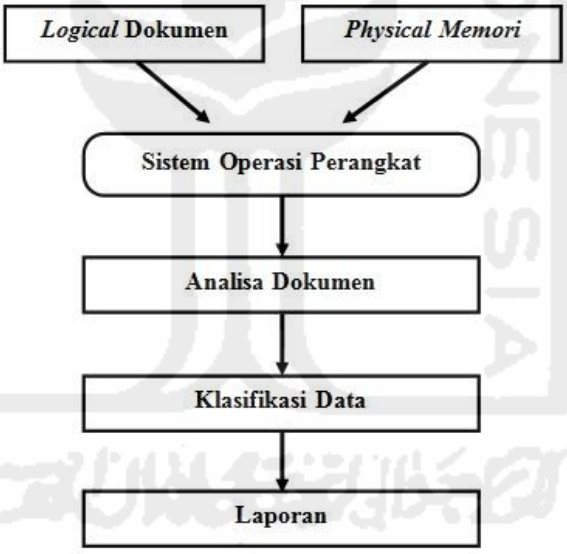
Mobile forensic atau forensika ponsel didefinisikan sebagai ilmu untuk memulihkan bukti potensial digital pada perangkat *mobile*, menggunakan teknik yang sama seperti untuk investigasi forensika digital pada umumnya. *Mobile forensic* merupakan cabang ilmu dari *digital forensic*

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.



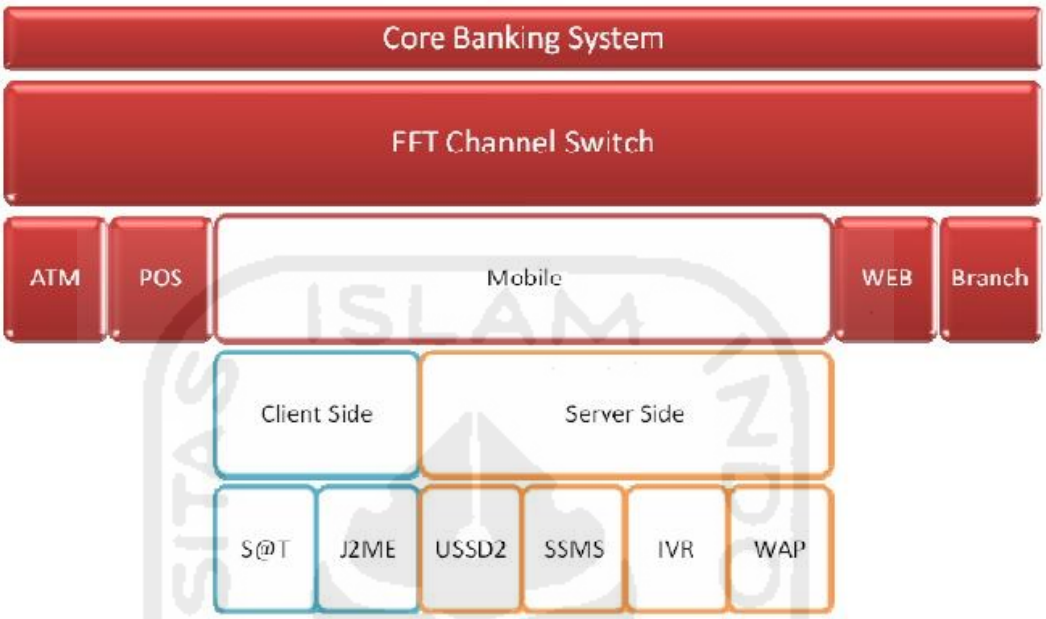
Gambar 3.1 Model analisa *mobile forensic* pada penelitian Qian Zhicong dan tim (2008)

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

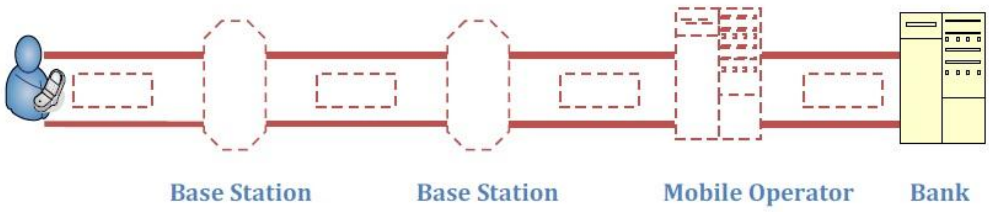
Fasilitas layanan *mobile banking* merupakan salah satu bagian dari inti perbankan, seperti penjelasan dari FinMark Trust (*Mobile Banking Technology Options*, 2007). Merupakan aplikasi

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.

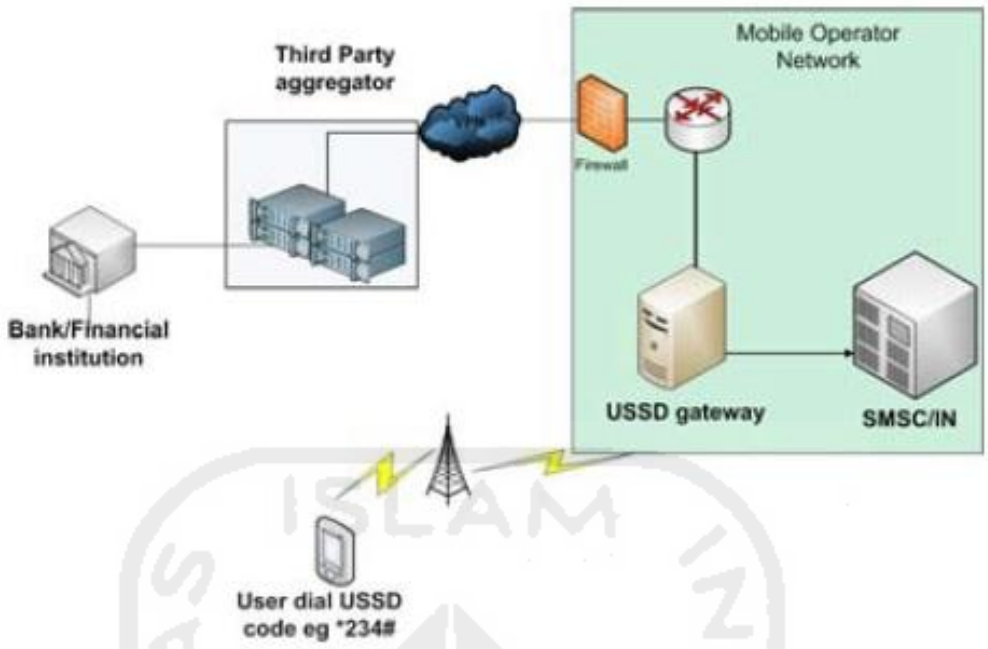


Gambar 3.2 Arsitektur *mobile banking* secara umum
(Sumber : (Overview 2007))

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))



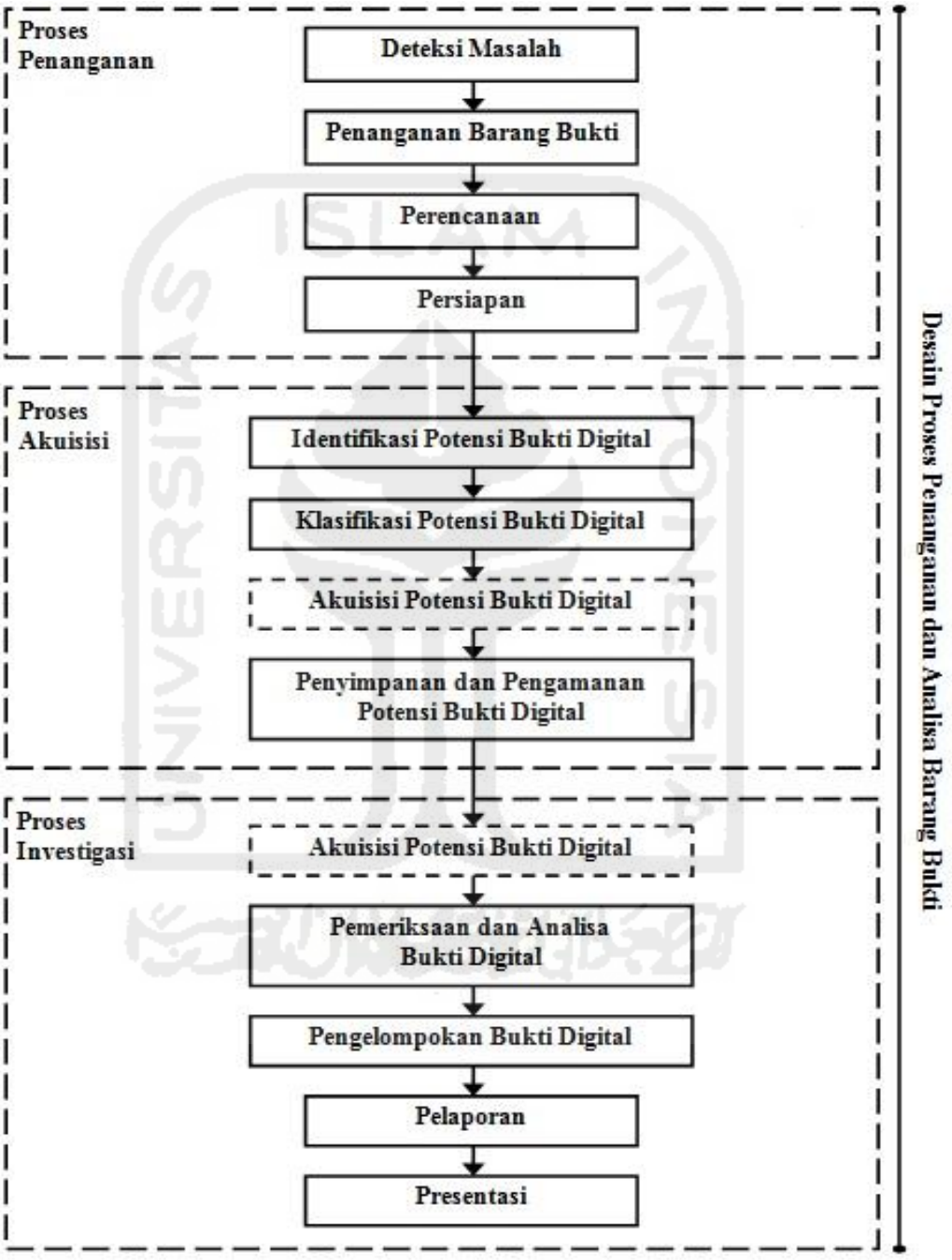
Gambar 3.4 *Basic* topologi jaringan yang digunakan *mobile banking* secara umum
(Sumber : (Trends 2015))

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

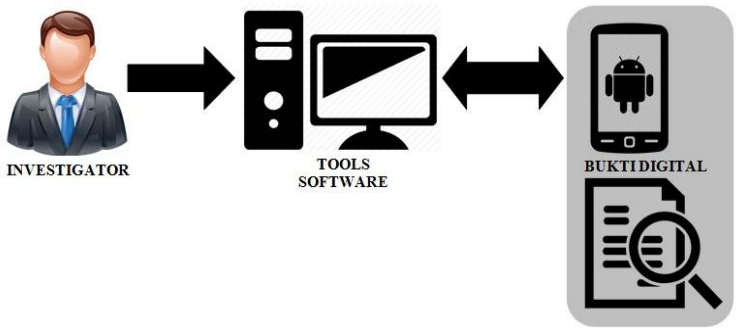
(Mengadopsi dari penelitian (Mumba 2014))

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.

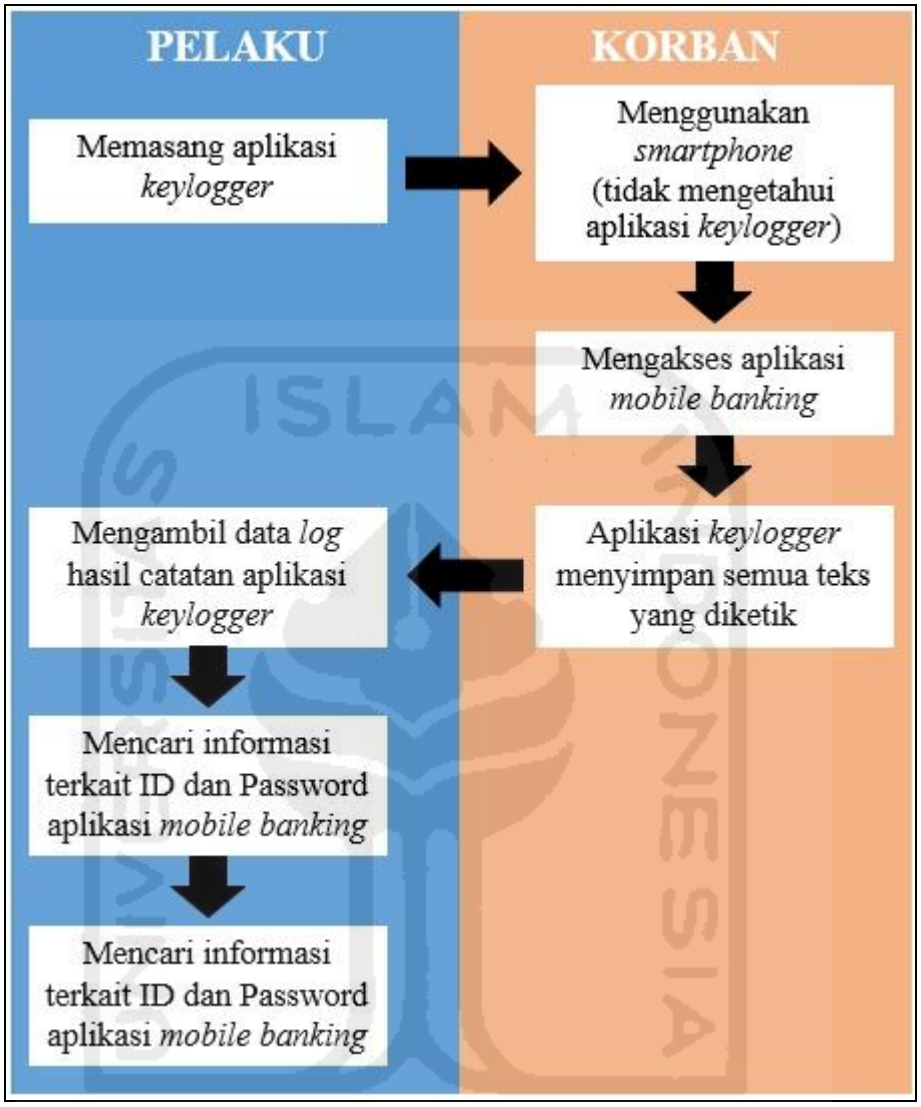
Tindakan akses ilegal atau *fraud* yang akan dilakukan oleh pelaku haruslah menggunakan perangkat *smartphone* milik korban. Karena pada dasarnya sistem kerja aplikasi *mobile banking* jika berganti perangkat harus memerlukan registrasi ulang. Untuk dapat melakukan registrasi ulang tersebut setiap bank 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.

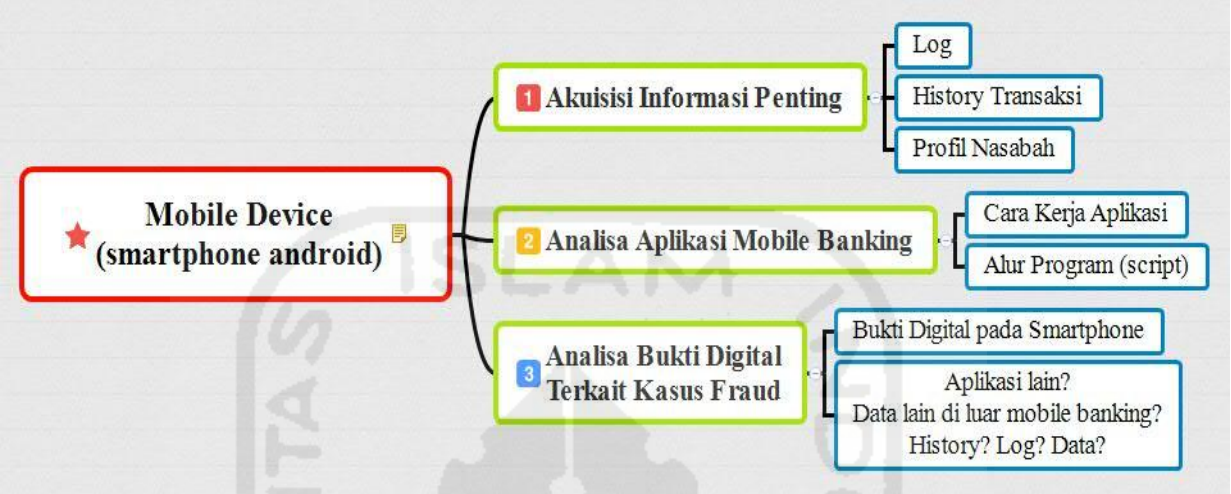
Ilustrasi skenario kasus yang telah dijelaskan pada alur cerita, tergambarkan pada Gambar 3.7.



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			

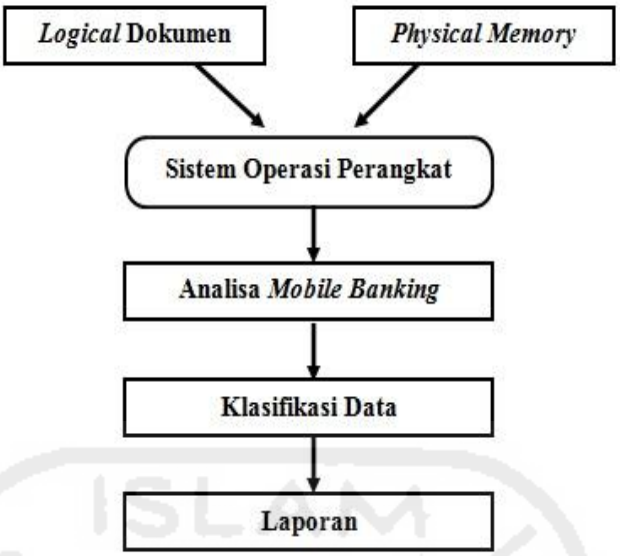
Penjelasan mengenai Tabel 3.1, pada kolom hasil temuan merupakan poin-poin apa saja yang menjadi hasil analisa pencarian data pada aplikasi *mobile banking*. Hal-hal yang diprioritaskan menjadi peran penting di dalam alur kinerja atau alur akses, bermula dari perangkat pendukung *mobile banking* milik 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

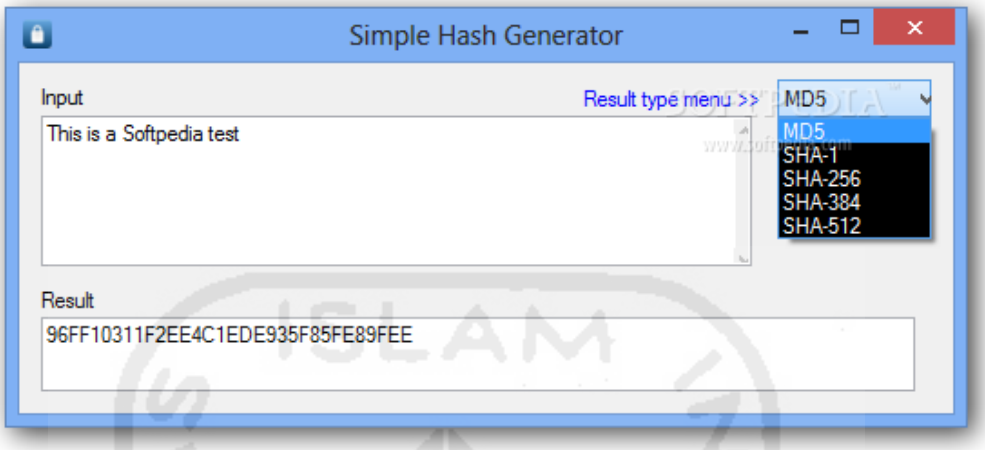
Peneliti terlebih dahulu memisahkan jenis penyimpanan yang digunakan oleh perangkat *smartphone*, antara dokumen *logical* dengan memori fisik. Selanjutnya melakukan analisa terhadap seluruh folder dan data yang terkait dengan aplikasi *mobile banking.* Proses analisa dilakukan secara manual untuk mencari 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.

Bab 4 Hasil dan Pembahasan

4.1. Klasifikasi Komparasi Karakteristik Aplikasi *Mobile Banking*

Peneliti melakukan analisa terhadap tiga aplikasi *mobile banking* yang diterbitkan secara resmi oleh tiga bank masing-masing pemilik layanan *mobile banking* di Indonesia. Pada penelitian ini ketiga aplikasi tersebut diistilahkan dengan sebutan Banking A, Banking B dan Banking C. Beberapa hal terkait dilakukan klasifikasi dan komparasi berfokus pada fasilitas layanan dan fungsi, alur proses, serta data folder terkait instalasi atupun *cache* aplikasi.

4.1.1. Fasilitas layanan dan fungsi-fungsi pada aplikasi

Setiap perbankan memiliki layanan yang berbeda tetapi fungsi utamanya hampir sama. Terutama pada layanan yang disematkan pada layanan aplikasi *mobile banking*. Pemaparan mengenai perbedaan fasilitas dan fungsi layanan tertera pada Tabel 4.1.

Tabel 4.1 Perbedaan fasilitas dan fungsi layanan *mobile banking*

Nama Bank	**Versi Aplikasi**	**Fungsi Layanan Aplikasi**				
		Cek Saldo	**Transfer Dana**	**Kalender Pengingat**	**Lokasi ATM**	**Layanan Pihak 3**
				Seting	Cari	
Banking A	0.6.7	YA	YA	TIDAK	TIDAK	YA
Banking B	1.0.16	YA	YA	YA	YA	YA
Banking C	1.4.4	YA	YA	TIDAK	TIDAK	YA

Tabel 4.1 menjelaskan bahwa setiap *mobile banking* dari ketiga bank yang dianalisa memiliki perbedaan layanan pada fitur aplikasi. Tetapi fungsi dan layanan yang berkaitan dengan kegiatan perbankan maupun layanan transaksi dengan pihak ketiga secara keseluruhan hampir sama.

Layanan utama berkaitan dengan transaksi perbankan memiliki fungsi hampir sama pada ketiga aplikasi *mobile banking* yang diteliti. Contohnya layanan transaksi transfer dana, cek saldo, dan pengecekan *history* transaksi yang pernah dilakukan dalam periode waktu tertentu. Serta fasilitas berkaitan dengan pihak ketiga, seperti pembayaran abonemen tagihan bulanan nasabah, pembelian voucer pulsa telepon seluler, dan lain sebagainya.

Fitur layanan tambahan yang disematkan di dalam aplikasi pada ketiga perbankan memiliki perbedaan. Misalkan kalender pengingat atau fasilitas pengingat waktu tertentu, serta layanan tambahan berupa informasi mengenai alamat lokasi mesin ATM dan kantor cabang / unit terdekat dari lokasi nasabah. Kedua jenis layanan tambahan tersebut disematkan pada aplikasi Banking B, tetapi tidak terdapat di dalam fitur Banking A dan Banking C.

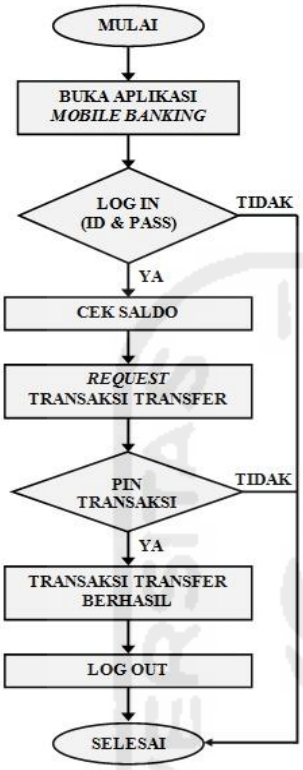
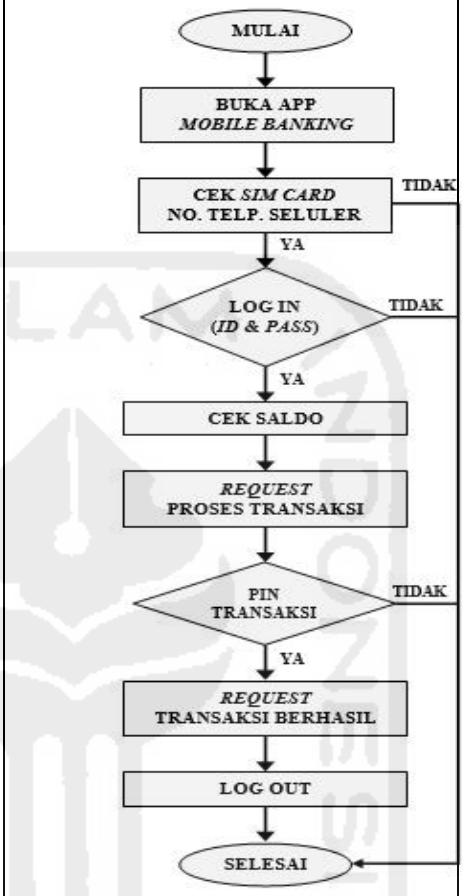
4.1.2. Alur proses aplikasi

Peneliti melakukan analisa terhadap alur proses atau tahapan apa saja dalam penggunaan aplikasi *mobile banking* pada *smartphone* berbasis android. Proses analisa dilakukan secara langsung pada perangkat *smartphone*.

Penjelasan analisa alur proses *mobile banking* disampaikan mengenai poin – poin penting saja atau yang secara umum biasa dilakukan dan digunakan oleh nasabah perbankan. Misalkan langkah *log in*, cek saldo, transaksi perbankan, dan *log out*. Tanpa menjelaskan menu–menu lain yang terdapat di dalam aplikasi. Karena hal tersebut merupakan menu tambahan dan bukan menjadi faktor utama dalam alur proses sebuah aplikasi *mobile banking*.

Analisa tentang alur proses *mobile banking* digambarkan dalam diagram alur pada Tabel 4.2.

Tabel 4.2 Perbandingan perbedaan alur proses aplikasi *mobile banking*

Diagram Alur Proses Aplikasi	
Banking A & Banking B	Banking C
	

Tabel 4.2 memaparkan mengenai alur proses aplikasi layanan *mobile banking* di mana terdapat perbedaan pada ketiga aplikasi tersebut. Pada aplikasi Banking C memiliki level keamanan dalam bentuk proses verifikasi nomor telepon seluler terdaftar saat awal registrasi layanan yang terdapat di dalam perangkat *smartphone*. Fungsi verifikasi nomor telepon seluler tersebut bertujuan agar tidak dapat dilakukan multi-akses pada satu identitas pengguna layanan *mobile banking* dengan menggunakan perangkat *smartphone* berbeda, atau lebih dari satu perangkat. Serta berfungsi sebagai autentikasi akses pengguna yang sah atau legal. Sedangkan pada aplikasi Banking A dan B berbeda dengan Banking C, yaitu tidak terdapat verifikasi nomor telepon seluler. Sehingga masih terdapat *vulnerability* terhadap tindak kejahatan dan masih dapat dilakukan multi-akses dengan menggunakan perangkat *smartphone* lebih dari satu.

Selain perbedaan mengenai verifikasi nomor telepon seluler tersebut, ketiga aplikasi *mobile banking* yang diteliti memiliki kesamaan fungsi yang hampir serupa sebagaimana merupakan dasar layanan yang berkaitan dengan perbankan. Diawali dengan autentikasi hak akses legal berupa ID dan *Password* atau PIN untuk dapat menggunakan layanan pada aplikasi. Kemudian diperlukan pula autentikasi *Password* maupun PIN untuk proses permintaan transaksi pada menu layanan aktivitas perbankan dan menu transaksi tambahan dengan pihak ketiga.

4.1.3. Data folder terkait instalasi atupun *cache* aplikasi

Berdasarkan hasil akuisisi dan proses analisa terhadap perangkat *smartphone* yang diuji mengenai penggunaan ketiga aplikasi layanan *mobile banking*, bahwa tidak ditemukan data folder aplikasi *mobile banking* ataupun folder berisi data-data yang berkaitan dengan aplikasi tersebut. Meskipun terdapat instalasi aplikasi *mobile banking* di dalam perangkat *smartphone* tetapi tidak terdapat folder instalasi pada berkas *file* hasil akuisisi.

Proses tersebut berfungsi sebagai pengamanan terhadap data profil nasabah dan *log* saat mengakses maupun data *history* transaksi yang pernah dilakukan menggunakan ketiga aplikasi *mobile banking*.

4.2. Proses Penanganan Barang Bukti

Mengacu pada Bab 3, Sub Bab 3.5 Metode *Static Forensic*, fase pertama adalah proses penanganan terhadap perangkat *mobile* yang digunakan sebagai alat penunjang aplikasi *mobile banking*. Adapun beberapa langkah yang dilakukan dalam proses penanganan.

4.2.1. Deteksi Masalah

Merupakan tahap awal dalam proses penanganan barang bukti. Haruslah dapat menganalisa apa permasalahan yang sedang ditangani dalam dunia forensika digital. Karena di dalam dasar ilmu forensika digital terdapat beberapa cabang ilmu.

Simulasi kasus pada penelitian ini adalah *fraud* atau pembobolan akses secara ilegal di luar sepengetahuan pemilik akun yang sah. Media yang akan dilakukan akuisisi dan analisa pada penelitian ini adalah sebuah perangkat *mobile* berupa *smartphone* berbasis android. Tindakan *fraud* yang dilakukan adalah membobol akses aplikasi *mobile banking*.

Peneliti bertujuan untuk membuktikan dengan cara analisa terhadap potensi bukti digital di dalam *smartphone* tersebut. Baik berupa bukti data yang menjelaskan catatan tindakan akses

ilegal ataupun temuan data – data penunjang lainnya. Dan melakukan analisa terhadap aplikasi *mobile banking* apakah terdapat celah *vulnerability* yang dapat dimanfaatkan untuk tindakan ilegal.

4.2.2. Penanganan Barang Bukti

Tahap penanganan ini dimaksudkan mengetahui dan memahami cara atau langkah apa saja dalam menangani barang bukti yang akan diproses. Misalkan jika perangkat yang akan diamankan berupa komputer maka bagaimana prosedur tindakan yang tepat. Bila ditemui *harddisk* sebagai potensi bukti maka bagaimana pula prosedur penanganannya. Pada kasus ini potensi bukti digital bersumber dari perangkat *smartphone* pasti penanganannya berbeda dengan perangkat komputer atau *harddisk*.

4.2.3. Perencanaan

Setelah dilakukan proses penanganan terhadap barang bukti berupa perangkat *mobile*, selanjutnya peneliti merencanakan susunan langkah – langkah apa saja yang akan dilakukan untuk mengakuisisi, menganalisa potensi bukti digital, hingga memberikan hasil sebagai bentuk laporan. Proses berikutnya mempersiapkan peralatan pendukung guna membantu proses akuisisi dan analisa potensi bukti digital.

4.2.4. Persiapan

Perencanaan yang telah dilakukan secara akurat akan menentukan langkah – langkah persiapan terperinci untuk selanjutnya dapat diterapkan pada proses akuisisi dan analisa. Guna membantu memudahkan proses – proses pengungkapan bukti digital.

Poin – poin yang perlu diperhatikan dalam mempersiapkan penunjang investigasi antara lain perangkat *hardware*, *mobile forensics tools* atau *software* yang akan digunakan, serta peralatan teknis lapangan dan sumber – sumber pendukung guna mempermudah proses akuisisi dan analisa.

4.3. Proses Akuisisi Bukti Digital

Tahap proses akuisisi berupa tindakan menangani perangkat bukti yang memiliki potensi bukti digital. Dan selanjutnya dilakukan penanganan pada data – data digital di dalam perangkat tersebut. Terdapat beberapa tahapan pada proses akuisisi yang akan dilakukan untuk dapat mengakuisisi potensi bukti digital.

4.3.1. Identifikasi Potensi Bukti Digital

Tahap ini berupa deteksi atau mengidentifikasi perangkat berpotensi bukti digital yang ditangani. Barang bukti apa saja yang terkait dengan kasus harus segera dilakukan penanganan. Tindakan mendeteksi permasalahan haruslah tepat dan akurat. Karena terkait dengan efektifitas dan efisiensi tindak penanganan, analisa, dan pengungkapan barang bukti.

Nasabah atau pelapor memiliki beberapa perangkat *mobile* yang setiap harinya digunakan untuk keperluan dinas maupun pribadi. Salah satu diantaranya digunakan sebagai penunjang kegiatan transaksional. Berupa perangkat *smartphone* berbasis android. Selanjutnya perangkat tersebut ditangani sebagai sumber potensi bukti digital.

4.3.2. Klasifikasi Potensi Bukti Digital

Peneliti memisahkan perangkat *mobile* milik nasabah, antara perangkat yang akan ditangani dengan perangkat yang tidak berpotensi memiliki bukti digital. Selayaknya penanganan bukti berupa perangkat *smartphone* (*mobile*) dilakukan isolasi perangkat dan isolasi jaringan selular menggunakan kantong khusus isolir jaringan.

Gambar 4.1 Ilustrasi penanganan barang bukti berupa perangkat *mobile*

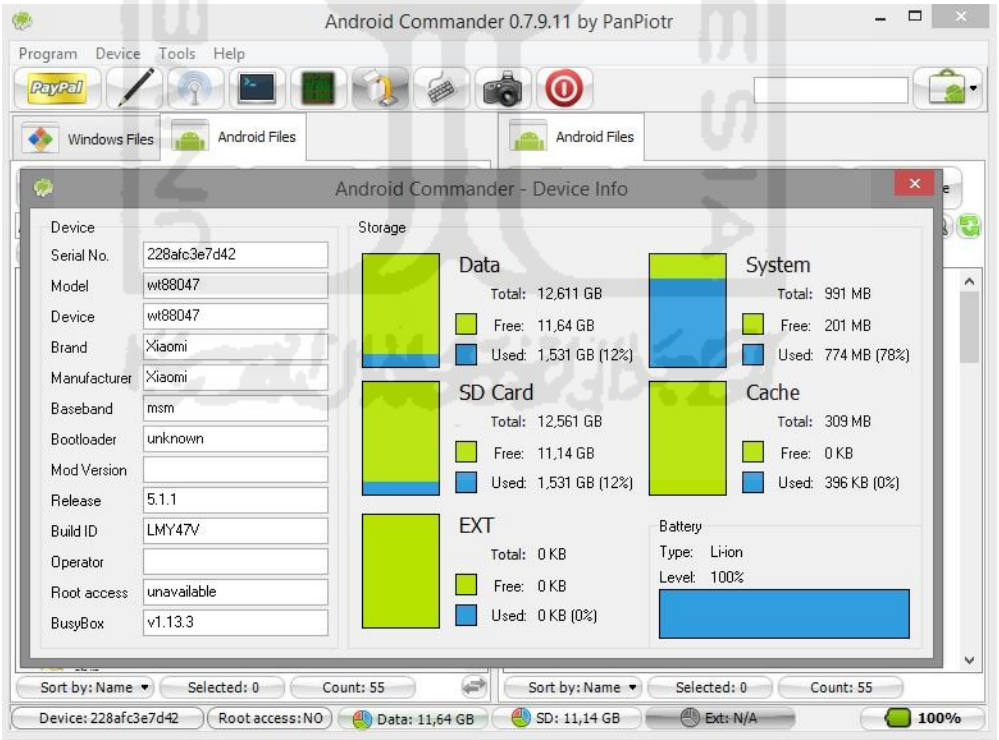
Langkah selanjutnya memberikan label keterangan dan pencatatan penanganan barang bukti sebelum proses pemindahan menuju lokasi penyimpanan. Guna memisahkan antara bukti pada kasus yang sedang ditangani dengan bukti kasus lainnya. Pemberian label keterangan dapat

mengacu dari berbagai sumber tata cara penanganan barang bukti yang pernah dilakukan. Karena belum terdapat standar baku secara nasional ataupun internasional terkait format pencatatan penanganan barang bukti.

Proses pencatatan harus dilakukan secara jelas, baik dari nama, jenis, nomor seri ataupun identitas lain yang melekat pada barang bukti sebagai keterangan penjelas. Serta pencatatan terperinci mengenai petugas yang melakukan tindakan / penanganan terhadap barang bukti.

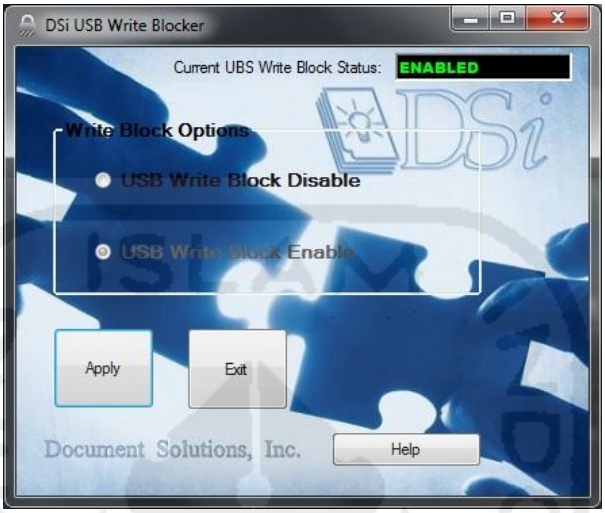
4.3.3. Akuisisi Potensi Bukti Digital

Perencanaan yang telah dilakukan pada proses sebelumnya membahas mengenai perangkat penunjang apa saja yang dibutuhkan guna mendukung proses akuisisi data dan analisa. Peneliti melakukan akuisisi data yang berkaitan dengan aplikasi *mobile banking* secara *logical* pada perangkat *smartphone*. Proses akuisisi data yang dilakukan ditunjang menggunakan *software* Andriller, Android Commander dan FTK Imager digunakan untuk melakukan proses *imaging* data. Proses akuisisi yang bertujuan untuk mengambil data di dalam *smartphone* menggunakan aplikasi Andriller dan Android Commander. Saat dilakukan akuisisi perangkat *smartphone* dalam keadaan *standby*, dan aplikasi *mobile banking* tidak dalam keadaan *online* ke sistem perbankan.



Gambar 4.2 Akuisisi data menggunakan *tool* Android Commander

Secara keseluruhan data yang telah diakuisisi selanjutnya dilakukan tahap *imaging*. Pada tahap proses *imaging* dilakukan untuk meng-*cloning* data, yang sebelumnya dilakukan pengamanan terlebih dahulu menggunakan *tools* berupa USB Write Blocker. Dengan tujuan agar tidak terjadi kontaminasi atau perubahan pada data – data bukti digital.



Gambar 4.3 Aplikasi USB Write Blocker

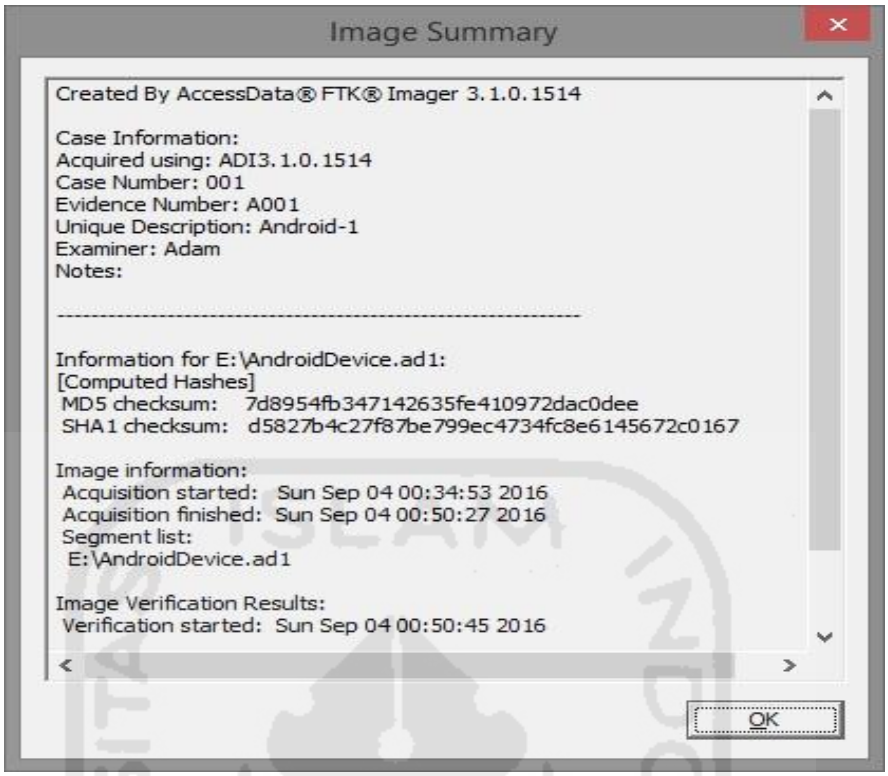
Untuk memastikan keaslian data yang telah diakuisisi, peneliti melakukan pencatatan nilai *hash* pada data hasil *imaging*. Terdapat beberapa informasi penting yang harus dicatat, seperti waktu akuisisi, nilai *hash*, dan ukuran data hasil *imaging*. Karena informasi nilai *hash* hasil *cloning* nantinya akan diverifikasi dengan nilai *hash* pada data hasil analisa.

Proses *cloning* yang dilakukan dengan cara *logical imaging*. Informasi yang dimaksud tertera pada Tabel 4.3.

Tabel 4.3 Pencatatan informasi hasil *imaging*

Nama	AndroidDevice.ad1
Sumber Data	Logical
Waktu Akuisisi	Sun Sep 04 00:34:53 2016
	Sun Sep 04 00:50:27 2016
Nilai *Hash*	MD5 : 7d8954fb347142635fe410972dac0dee
	SHA1 : d5827b4c27f87be799ec4734fc8e6145672c0167
Aplikasi	AccessData® FTK® Imager 3.1.0.1514

Data hasil *imaging* selanjutnya dilakukan uji keaslian atau otentikasi teknik *hashing*, pada penelitian ini menggunakan nilai *hash* MD5 dan SHA1.



Gambar 4.4 Kesimpulan hasil proses data *imaging*

4.3.4. Penyimpanan dan Pengamanan

Potensi bukti digital yang telah melalui proses akuisisi selanjutnya dilakukan penanganan berupa penyimpanan dan pengamanan. Prosedur penyimpanan barang bukti pada umumnya harus disertai pencatatan informasi penting mengenai barang bukti yang telah diakuisisi maupun perangkat sumber bukti tersebut.

Pada kasus ini peneliti menggunakan tabel pencatatan informasi terkait barang bukti untuk tahap penyimpanan dan pengamanan. Tertera pada tabel 4.4.

Tabel 4.4 Pencatatan informasi barang bukti

INFORMASI BARANG BUKTI	
Hari / Tanggal	Senin, 5 September 2016
Nama Petugas	Adam Prayogo Kuncoro

Tabel 4.4 Pencatatan informasi barang bukti (Lanjutan)

INFORMASI BARANG BUKTI		
Nama Barang Bukti	Identitas	Keterangan
Smartphone Android	Tipe : Xiaomi Redmi 2S OS : Lollipop 5.1.1 Warna : Abu–abu	Sumber potensi bukti digital
Micro SD Card	Merek : Visipro Kapasitas : 8 GB Warna : Hitam	Sumber potensi bukti digital
Flashdisk BB 1	Tipe : *flashdrive* Kapasitas : 8 GB Warna : Putih	Berisi data *cloning* (asli) potensi bukti digital
Flashdisk BB 2	Tipe : *flashdrive* Kapasitas : 8 GB Warna : Hijau	Berisi salinan data *cloning* potensi bukti digital yang akan dianalisa
Petugas, (Adam Prayogo Kuncoro)		

Tabel informasi barang bukti tersebut digunakan oleh peneliti berfungsi supaya tidak terjadi kesalahan analisa yang diakibatkan karena tertukarnya barang bukti. Atau jika diperlukan untuk dilakukan akuisisi ulang terhadap potensi bukti digital yang bersumber dari perangkat barang bukti.

Tempat penyimpanan barang bukti berada pada ruangan khusus, di mana tidak sembarang orang ataupun petugas dapat memasuki ruangan tersebut. Untuk memasuki ruang penyimpanan barang bukti harus mengisi formulir yang berisikan informasi khusus. Misalkan data yang diisikan adalah tanggal memasuki ruangan, waktu masuk dan waktu keluar, kepentingan untuk memasuki ruang penyimpanan barang bukti, dan lain sebagainya.

Jika diperlukan pengambilan barang bukti diharuskan memberikan keterangan tertulis di dalam formulir mengenai apa saja yang dibawa oleh petugas terkait. Serta proses peletakan kembali barang bukti ke ruang penyimpanan harus diinformasikan secara lengkap. Supaya tidak terjadi kontaminasi terhadap seluruh barang bukti yang ada di dalam ruang penyimpanan.

Poin tersebut secara umum menjadi prosedur pada proses penanganan barang khususnya pada tahap penyimpanan dan pengamanan. Meskipun belum ada standar baku secara nasional ataupun internasional apa saja poin-poin yang harus disertakan di dalam informasi pencatatan.

4.4. Proses Investigasi Bukti Digital

Tahapan ini dilakukan berdasarkan kemampuan peneliti dalam melakukan proses analisa dan investigasi pada data potensi bukti digital yang sebelumnya telah diakuisisi berasal dari perangkat *smartphone*. Serta didukung beberapa perangkat *hardware* dan *software* yang sesuai dengan keamampuan peneliti.

4.4.1. Pemeriksaan dan Analisa Bukti Digital

Tahap analisis bukti digital didasari pada hasil temuan data yang diakuisisi menggunakan *tool* Android Commander dan Andriller. Berikut ini merupakan penjelasan tahap analisa yang dibedakan pada masing-masing hasil akuisisi.

4.4.1.1. Analisa Data Hasil Akuisisi Menggunakan Android Commander

Proses investigasi terhadap data salinan hasil akuisisi *cloning* perangkat *smartphone* yang menggunakan *software* Android Commander, peneliti menganalisa secara terperinci dan detail. Aplikasi *tool* FTK Imager digunakan untuk membuka salinan data *image* dan memetakan tiap-tiap berkas folder di dalamnya. Data-data folder tersebut peneliti rangkum dalam Tabel 4.5.

Tabel 4.5 Rangkuman salinan data *image* potensi bukti digital

Berkas Folder	Berkas File Isi	Keterangan
acct	uid (folder) $l30 cgroup.clone_children cgroup.procs cgroup.sane_behavior cpuacct.stat cpuacct.usage cpuacct.usage_percpu notify_on_release release_agent	Folder ini memuat data-data yang menginformasikan kinerja sistem android ketika sedang digunakan Hasil : Tidak ditemukan bukti digital terkait
bin	adb_keys	Folder ini memuat data-data mengenai informasi koneksi *debug* antara perangkat *smartphone* dengan komputer Hasil : Tidak ditemukan bukti digital terkait

Tabel 4.5 Rangkuman salinan data *image* potensi bukti digital (Lanjutan)

Berkas Folder	Berkas File Isi	Keterangan
mnt - shell - emulated - 0	.dlprovider (folder) Android (folder) jeejen (folder) libs (folder) miad (folder) MIUI (folder) Movies (folder) Pictures (folder) system (folder) $l30 .profig.os .volume dcpt	Folder ini memuat data-data penyimpanan *internal* yang berada pada perangkat *smartphone* beserta konfigurasi aplikasi yang tersimpan Hasil : Tidak ditemukan bukti digital terkait
proc	327 (folder) asound (folder) bus (folder) driver (folder) fs (folder) irq (folder) scsi (folder) sys (folder) sysvipc (folder) touchscreen (folder) tty (folder) $l30 buddyinfo cgroups consoles cpuinfo crypto devices diskstats execdomains fb filesystems ft5x0x-debug	Folder ini memuat data-data mengenai konfigurasi proses sistem android. Berisi folder-folder yang berkaitan dengan identitas proses Hasil : Tidak ditemukan bukti digital terkait
res - images - charger	$l30 battery_fail.png battery_scale_0.png battery_scale_1.png battery_scale_2.png battery_scale_3.png battery_scale_4.png battery_scale_5.png	Folder ini memuat data-data mengenai gambar atau animasi yang digunakan saat perangkat android melakukan pengisian ulang baterai Hasil : Tidak ditemukan bukti digital terkait

Tabel 4.5 Rangkuman salinan data *image* potensi bukti digital (Lanjutan)

Berkas Folder	Berkas File Isi	Keterangan
storage	sdcard 1 (folder)	Folder ini memuat data-data penyimpanan memori *external* atau kartu *microSD* Hasil : Tidak ditemukan bukti digital
sys	bus (folder) devices (folder) fs (folder)	Folder ini memuat data-data mengenai Hasil : Tidak ditemukan bukti digital terkait
system	app (folder) bin (folder) etc (folder) fonts (folder) framework (folder) lib (folder) media (folder) priv-app (folder) tts (folder) usr (folder) vendor (folder) xbin (folder)	Folder ini memuat data-data aplikasi, konfigurasi aplikasi, perijinan akses aplikasi terhadap sistem, serta *library* pendukung sistem operasi android Hasil : Tidak ditemukan bukti digital terkait
(direktori luar)	$l30 default.prop file_contexts property_contexts seapp_contexts selinux_version sepolicy service_contexts ueventd.qcom.rc ueventd.rc unlock_key verity_key	Folder ini memuat data-data yang berkaitan dengan konfigurasi dari sistem android Hasil : Tidak ditemukan bukti digital terkait

Peneliti menganalisa salinan data *image cloning* dengan hasil tidak terdapat data artefak yang mendukung sebagai bukti digital mengenai aplikasi *mobile banking*. Bahkan pada data *image cloning* dengan teknik akuisisi *smartphone* terhubung secara *online* tetap tidak terdapat data artefak pendukung bukti digital.

Pembahasan pada hasil analisa terhadap data *image* akuisisi perangkat *smartphone* android, peneliti menarik kesimpulan bahwa aplikasi *mobile banking* beserta direktori penyimpanan di dalam perangkat *smartphone* tidak terdapat data-data penting yang berkaitan dengan akun nasabah, identitas beserta kunci akses, catatan *log* akses aplikasi, catatan transaksi perbankan

maupun transaksi layanan pihak ketiga, serta tidak terdapat data penting lainnya yang dapat dijadikan celah keamanan *mobile banking*.

Selanjutnya peneliti melakukan *decompiling* atau pembedahan secara digital terhadap aplikasi *mobile banking* menggunakan *tool* aplikasi APK Tool. Dengan tujuan untuk mencari tahu bagimana cara kerja sistem aplikasi. Serta mencari *script* perintah penyimpanan data *cache* transaksi, info identitas nasabah, *log* akses nasabah, dan informasi penting lainnya yang dapat dijadikan petunjuk penelitian untuk menemukan artefak data pendukung bukti digital.

Langkah peneliti dalam melakukan *decompiling* aplikasi *mobile banking* sekedar membaca dan memahami alur kerja dan data petunjuk yang mengarah kepada potensi bukti digital. Hasil *decompile* pada aplikasi *mobile banking* terangkum dalam Tabel 4.6.

Tabel 4.6 Hasil *decompile* aplikasi *mobile banking*

Berkas Folder	Berkas File Isi	Keterangan
assets	font (folder) html (folder) user_tnc_en_files (folder) user_tnc_in_files (folder) panduan.html user_tnc_en.htm user_tnc_in.htm	Berisi data pendukung susunan tampilan aplikasi *mobile banking* (Tidak ditemukan data yang mengarah pada *script* alur kerja sistem)
original	META-INF (folder) AndroidManifest.xml	Berisi data lisensi perijinan penerbitan aplikasi (Tidak ditemukan data yang mengarah pada *script* alur kerja sistem)
res	anim (folder) color (folder) drawable (folder) … layout (folder) … menu (folder) raw (folder) values (folder) … xml (folder)	Berisi data pendukung susunan tampilan aplikasi *mobile banking* (Tidak ditemukan data yang mengarah pada *script* alur kerja sistem)
Unknown	myinfosys (folder) … - muamalat (folder) … - properties (folder) … - application.properties	Berisi data-data penting sebagai akses aplikasi (Ditemukan data penting sebagai alur proses aplikasi)
(direktori luar)	AndroidManifest.xml apktool.yml classes.dex	Berisi data-data penting sebagai akses aplikasi (Ditemukan data penting sebagai alur proses aplikasi)

Analisa peneliti terhadap data-data hasil *decompile* mendapatkan beberapa data penunjang yang mengarahkan kepada *script* atau perintah alur proses aplikasi *mobile banking*. Data yang ditemukan berada pada folder **unknown – myinfosys – properties** dengan nama *file* **application.properties** berisi *script* mengenai informasi variabel *link* akses perintah yang dapat menghubungkan antara aplikasi *mobile banking* dengan sistem pusat perbankan. Data penting kedua adalah **AndroidManifest.xml** terdapat di direktori luar. Merupakan *file* penting yang berisi *script* manifest atau *script* ijin akses pada sistem perangkat android untuk mengakses hal-hal yang terkait antara aplikasi *mobile banking* dengan sistem pusat perbankan.

Menurut analisa pada penelitian ini, *file* **application.properties** memiliki keterkaitan dalam satu alur perintah akses terhadap *file* **AndroidManifest.xml**. Pada *file* **application.properties** merupakan data yang berisi informasi variabel *link* untuk menghubungkan perintah akses *mobile banking* dengan server perbankan. Sedangkan *file* **AndroidManifest.xml** berisi *script* ijin akses terhadap sistem perangkat android untuk menghubungkan konten *link* di dalam **application.properties**. Penjabaran isi yang bersumber dari *file* **application.properties** mengenai konfigurasi akses aplikasi *mobile banking* akan peneliti tuliskan pada Tabel 4.7.

Tabel 4.7 Daftar isi *file* **application.properties**

Daftar Isi *File* application.properties	
dictionary.url = net.myinfosys.json.mobile.GetDictionary login.url = net.myinfosys.json.mobile.DoLogin logout.url = net.myinfosys.json.mobile.DoLogout exchangeRate.url = net.myinfosys.json.mobile.Get ExchangeRate changeLanguage.url = net.myinfosys.json.mobile.Change Language atmLocator.url = net.myinfosys.json.mobile.GetAtmsByRange branchLocator.url = net.myinfosys.json.mobile.Get BranchByRange nisbah.url = net.myinfosys.json.mobile.Get Nisbah balenceInquiry.url = net.myinfosys.json.mobile.Do BalanceInquiry	doPaymentAirlines.url = net.myinfosys.json.mobile.DoPaymentAirlines doInquiryPaymentInternet.url = net.myinfosys.json.mobile.DoInquiryPaymentI nternet doPaymentInternet.url = net.myinfosys.json.mobile.DoPayment Internet doInquiryPaymentPaidTv.url = net.myinfosys.json.mobile.DoInquiry PaymentPaidTv doPaymentPaidTv.url = net.myinfosys.json.mobile.DoPayment PaidTv doInquiryPaymentPublicUtility.url = net.myinfosys.json.mobile.DoInquiry PaymentPublicUtility doPaymentPublicUtility.url = net.myinfosys.json.mobile.DoPayment PublicUtility

Tabel 4.7 Daftar isi *file* **application.properties** (Lanjutan)

Daftar Isi *File* application.properties	
bankList.url = net.myinfosys.json.mobile.GetBankCode	createFavouriteTransfer.url = net.myinfosys.json.mobile.CreateFavoriteTransfer
mobileDataService.url = net.myinfosys.json.mobile.Get MobileDataService	createFavoritePayment.url = net.myinfosys.json.mobile.CreateFavoritePayment
challegeCode.url = net.myinfosys.json.mobile.Get ChallengeCode	getFavouritePaymentAndTopup.url = net.myinfosys.json.mobile.GetFavorite PaymentAndTopup
inquiryToAccount.url = net.myinfosys.json.mobile.Do InquiryToAccount	getFavouriteTransfer.url = net.myinfosys.json.mobile.GetFavorite Transfer
transferInternal.url = net.myinfosys.json.mobile.DoTransfer Internal	doInquiryPaymentInsurance.url = net.myinfosys.json.mobile.DoInquiry PaymentInsurance
operatorSelular.url = net.myinfosys.json.mobile.GetOperatorSelular	doPaymentInsurance.url = net.myinfosys.json.mobile.DoPayment Insurance
registrasi.url = net.myinfosys.json.mobile.VerifikasiRegistrasi	createFavoriteZakat.url = net.myinfosys.json.mobile.CreateFavorite Zakat
doTopUp.url = net.myinfosys.json.mobile.DoTopup	getFavoriteZakat.url = net.myinfosys.json.mobile.GetFavoriteZakat
getTin.url = net.myinfosys.json.mobile.GetTin	doDeleteFavoriteZakat.url = net.myinfosys.json.mobile.DoDelete FavoriteZakat
doInquiryPaymentTelkom.url = net.myinfosys.json.mobile.Do InquiryPaymentTelco	doDeleteFavoriteTransfer.url = net.myinfosys.json.mobile.DoDelete FavoriteTransfer
changeUsername.url = net.myinfosys.json.mobile.Change Username	doDeleteFavoritePaymentAndTopup.url = net.myinfosys.json.mobile.DoDelete FavoritePaymentAndTopup
changePassword.url = net.myinfosys.json.mobile.ChangePassword	getAuthKey.url = net.myinfosys.json.mobile.GetAuthKey
matchNumPhone.url = net.myinfosys.json.mobile.MatchNumPhone	hideRelatedAccount.url = net.myinfosys.json.mobile.DoHideRelated Account
doZakat.url = net.myinfosys.json.mobile.DoZis	getEntertainment.url = net.myinfosys.json.mobile.GetEntertainment
getRelatedAccount.url = net.myinfosys.json.mobile.Get RelatedAccountMobile	getPackageTv.url = net.myinfosys.json.mobile.GetPackageTv
getChannelTv.url = net.myinfosys.json.mobile.GetChannelTv	getPrayersTimes.url = net.myinfosys.json.mobile.GetPrayersTimes
doInquiryTransfer.url = net.myinfosys.json.mobile.DoInquiryTransfer	
doTransferNetwork.url = net.myinfosys.json.mobile.DoTransfer Network	

Tabel 4.7 Daftar isi *file* **application.properties** (Lanjutan)

Daftar Isi *File* application.properties	
doTransferRtgs.url = net.myinfosys.json.mobile.DoTransferRtgs	getPromotion.url = net.myinfosys.json.mobile.GetPromotion
doTransferSkn.url = net.myinfosys.json.mobile.DoTransferSknGen2	getPromotImage.url = net.myinfosys.json.mobile.GetPromotIma
doPaymentTelco.url = net.myinfosys.json.mobile.DoPaymentTelco	doInquiryPaymentPln.url = net.myinfosys.json.mobile.DoInquiryPaymentPln
getHistoryDetailInquiry.url = net.myinfosys.json.mobile.GetHistoryDetailInquiry	doPaymentPln.url = net.myinfosys.json.mobile.DoPaymentPln
doPaymentVirtualAccount.url = net.myinfosys.json.mobile.DoPaymentVirtualAccount	getVoucherPln.url = net.myinfosys.json.mobile.GetVoucher
	doInquiryVirtualAccount.url = net.myinfosys.json.mobile.DoInquiryVirtualAccount
	doPlnManualAdvice.url = net.myinfosys.json.mobile.DoManual

Pemaparan mengenai isi Tabel 4.7 selanjutnya akan peneliti lakukan klasifikasi pada proses pengelompokan sub bahasan tahap **klasifikasi data hasil decompile 4.4.1.2**. Dikarenakan terdapat beberapa informasi *link* akses yang penting sebagai perintah proses transaksi antara aplikasi *mobile banking* dengan server perbankan. Peneliti akan mengklasifikasikan kategori *script* bersifat otentikasi akses, layanan menu transaksi pihak ketiga, dan *library* sebagai *script* pemanggil fasilitas tambahan.

Bersumber dari data *script* **application.properties** yang telah diklasifikasikan, peneliti akan menganalisa apa saja kode perintah pada aplikasi untuk melakukan akses transaksi perbankan, perintah untuk melakukan otentikasi hak akses yang sah, ataupun otentikasi hal lain berkaitan dengan akses resmi. Serta dapat mengetahui apakah terdapat perintah proses untuk melakukan penyimpanan data-data penting terkait akun nasabah, catatan transaksional, dan lain sebagainya. Sehingga peneliti dapat mengambil kesimpulan mengenai penelitian *mobile forensics* ini.

Pembahasan mengenai *file* **AndroidManifest.xml** peneliti paparkan tampilan *screenshot* pada Gambar 4.5. Serta peneliti berikan penjelasan fungsi atau peran *file* tersebut di dalam sistem aplikasi *mobile banking*.

```
- <manifest android:installLocation="auto" package="net.myinfosys.muamalat.activity" platformBuildVersionCode="21"
  platformBuildVersionName="5.0.1-1624448">
    <supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true"
    android:resizeable="true" android:smallScreens="true" android:xlargeScreens="true"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-feature android:glEsVersion="0x20000" android:required="true"/>
    <uses-feature android:name="android.hardware.telephony" android:required="false"/>
  + <application android:allowBackup="true" android:configChanges="locale" android:hardwareAccelerated="false"
    android:icon="@drawable/ic_launcher" android:label="@string/app_name"
    android:name="net.myinfosys.muamalat.activity.MobileBankingApplication" android:screenOrientation="portrait"
    android:theme="@style/Theme.PermataDefault"></application>
  </manifest>
```

Gambar 4.5 Tampilan *script* file AndroidManifest.xml

File **AndroidManifest.xml** merupakan informasi pusat atau utama pada aplikasi *mobile banking*. Memiliki fungsi seperti gudangnya informasi untuk aplikasi tersebut. Berperan sebagai pemberi akses *permission* agar dapat diaktifkan dan digunakan pada perangkat android.

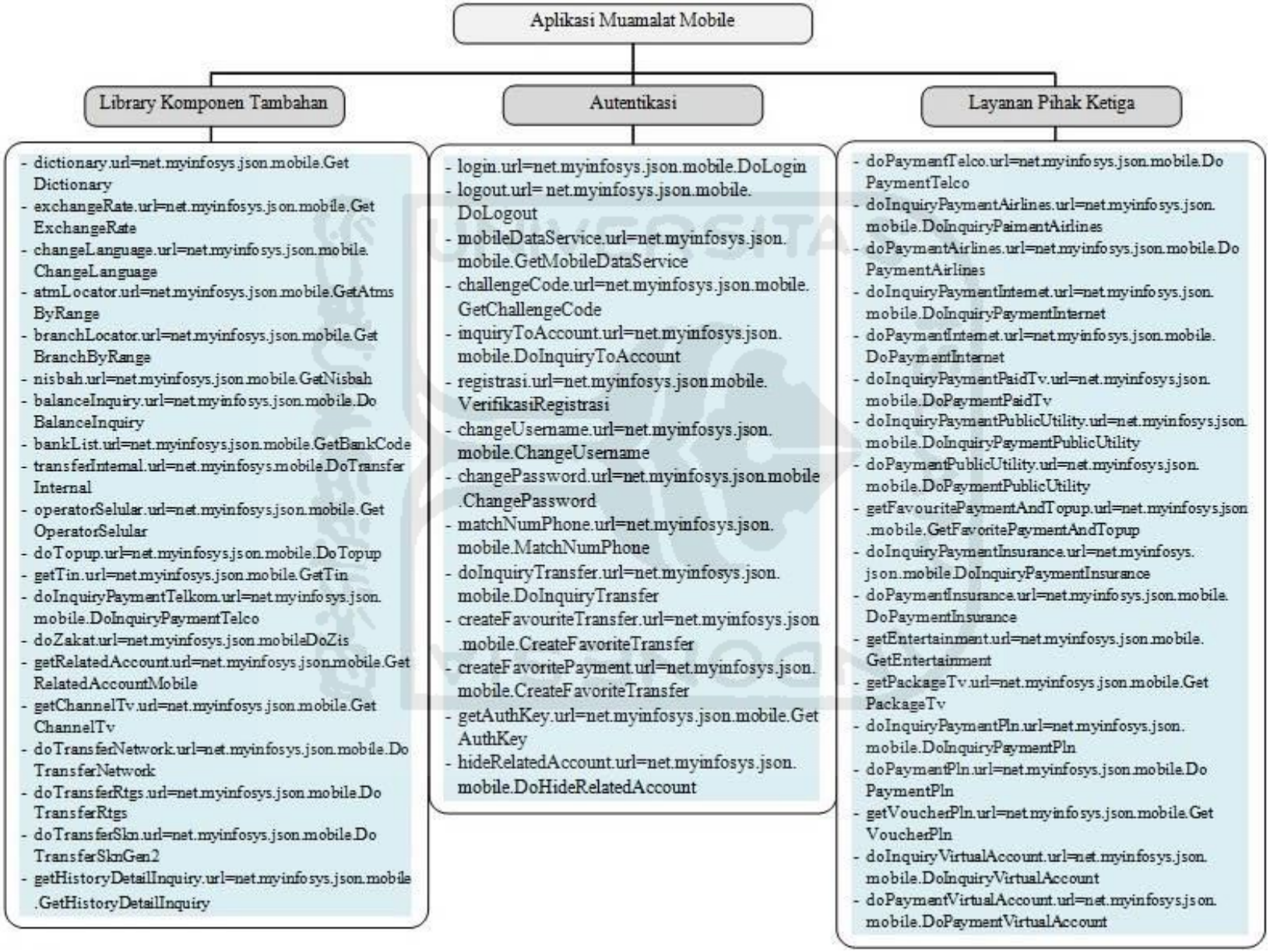
Berdasarkan hasil analisa, di dalam *file* **AndroidManifest.xml** berisi *script* perintah perijinan *library* aplikasi atau *uses permission* dengan fungsi agar barisan perintah di dalam direktori aplikasi *mobile banking* dapat dijalankan pada sistem android. Terdapat 14 (empat belas) perintah perijinan aplikasi dengan fungsi yang berbeda-beda. Masing-masing perintah *uses permission* diantaranya berfungsi sebagai jembatan akses untuk terhubung ke jalur internet melalui jaringan seluler maupun *wifi*, membaca direktori aplikasi terdapat pada memori *internal* atau *external*, mengirimkan perintah registrasi melalui nomor telepon seluler yang telah didaftarkan kemudian aplikasi membaca pesan singkat atau SMS yang diterima berisi kode aktifasi saat registrasi *mobile banking*, serta terdapat perintah-perintah perijinan aplikasi yang berkaitan dengan fitur layanan tambahan lainnya.

Bersumber pada *script* perintah *file* **AndroidManifest.xml**, peneliti mengambil kesimpulan analisa bahwa aplikasi *mobile banking* Muamalat Mobile tidak melakukan perintah berupa penyimpanan data penting yang berkaitan dengan akun nasabah seperti profil, identitas akses

aplikasi *mobile banking*, perubahan kunci akses dan sebagainya. Tidak terdapat perintah penyimpanan *history* transaksi perbankan maupun transaksi keuangan dengan layanan tambahan pihak ketiga.

4.4.1.2.Klasifikasi Data Hasil *Decompile*

Mengacu pada sub proses investigasi, tahap **Analisa data hasil akuisisi menggunakan Android Commander** poin **4.4.1.1**, peneliti melakukan pengelompokan data pada *file* **application.properties** hasil *decompile* aplikasi *mobile banking* menjadi tiga jenis. Diantaranya kolom **Library Komponen Tambahan, Autentikasi**, dan **Layanan Pihak Ketiga**. Dengan tiga kolom tersebut untuk membedakan jenis perintah-perintah dasar pada sistem aplikasi *mobile banking*. Peneliti membuat pengelompokan pada Gambar 4.8.



Gambar 4.6 Bagan klasifikasi *file* application.properties

Tujuan peneliti melakukan pengelompokan pada Gambar 4.6 adalah supaya mempermudah dalam menganalisa perintah-perintah dasar alur proses aplikasi *mobile banking*. Guna mencari pertunjuk serta membuktikan bahwa tidak terdapat *script* perintah dasar aplikasi untuk memproses penyimpanan data-data penting yang berkaitan dengan akun pribadi nasabah, akun akses, dan catatan transaksi perbankan ataupun layanan lain di dalam direktori yang masih menjadi bagian dari aplikasi *mobile banking*.

Kolom **Autentikasi** pada Gambar 4.6 merupakan kumpulan *script* perintah untuk menjalankan komponen aplikasi yang berfungsi sebagai autentikasi atau pengesahan hak akses sebelum pengguna melakukan akses tahap lanjut terhadap fitur layanan yang terdapat di dalam aplikasi *mobile banking*. Misalkan autentikasi akses ketika proses *login*, akses keamanan kunci transaksi, serta proses autentikasi lainnya.

Pada kolom **Library** merupakan kumpulan *script* perintah untuk menjalankan komponen aplikasi yang bersifat layanan resmi dari perbankan kepada nasabah sebagai pengguna fasilitas *mobile banking*. Beberapa contoh fasilitas tersebut diantaranya nasabah dapat mengakses di mana saja lokasi layanan ATM ataupun kantor cabang terdekat bersumber dari lokasi perangkat *mobile* dengan kondisi mengaktifkan seting GPS. Layanan pembayaran zakat dapat dilakukan hanya menggunakan fasilitas aplikasi *mobile banking* untuk mempermudah keperluan nasabah. Serta nasabah dapat mengakses informasi layanan apa saja yang diberikan oleh bank dalam melakukan pembayaran secara *online*, misalkan pembayaran tagihan bulanan ataupun untuk berbelanja keperluan lainnya. Dan beberapa layanan tambahan lain yang dapat dengan mudah digunakan atau diakses oleh nasabah.

Kolom **Layanan Pihak Ketiga** adalah kumpulan *script* perintah untuk menjalankan komponen aplikasi yang berkaitan dengan fasilitas layanan tambahan dari bank untuk nasabah pengguna *mobile banking*. Fasilitas layanan bank tersebut berfungsi untuk memudahkan nasabah melakukan transaksi periodik kepada pihak ketiga sebagai pemberi layanan personal nasabah. Misalkan layanan pembayaran tagihan listrik PLN, pembayaran ataupun pembelian layanan telekomunikasi, pembayaran layanan *booking* tiket kereta maupun pesawat, serta terdapat akses pembayaran *online* penyedia layanan personal lainnya dengan tujuan untuk memudahkan nasabah pengguna layanan *mobile banking*.

Setelah dilakukan pengelompokan dan analisa terhadap daftar *script* perintah yang bersumber pada *file* **application.properties**, peneliti menyimpulkan bahwa aplikasi Muamalat Mobile tidak memproses penyimpanan data penting terkait akun dan catatan akses transaksi

nasabah pengguna layanan *mobile banking* ke dalam direktori aplikasi secara *offline*. Bahkan cara kerja *script* perintah tersebut hanya melakukan *request* akses dari perangkat *mobile* android kepada sistem server perbankan. Atau dapat diartikan hanya berfungsi sebatas layanan penjembatan permintaan akses transaksional antara nasabah dengan sistem perbankan.

4.4.1.3. Analisa Data Hasil Akuisisi Menggunakan Andriller

Tahap ini menggunakan *software* Andriller untuk melakukan proses akuisisi secara *logical* dari perangkat *smartphone* yang diteliti. Dimaksudkan untuk mencari bukti-bukti temuan terkait *file* atau informasi yang dapat dijadikan bukti digital terhadap tindak kejahatan. Data-data yang telah diakuisisi ditampilkan pada Tabel 4.8 berikut.

Tabel 4.8 Rangkuman data hasil akuisisi menggunakan Andriller

Berkas Folder	Berkas File Isi	Keterangan
db	_backup_ (folder) Archived History, Archived History-journal, browser2.db, contacts2.db, downloads.db, downloads.db-journal, EmailProvider.db, EmailProvider.db-journal, EmailProviderBody.db, EmailProviderBody.db-journal, flattened-data, History, History-journal, Login Data, Login Data-journal, logs.db, logs.db-journal, webview.db	Folder ini memuat data-data yang berisi informasi penting di dalam *smartphone* berupa *database* Hasil : Tidak ditemukan bukti digital terkait
Shared	0 (folder), Android (folder), DCIM (folder), **Download (folder)**, Sounds (folder), UCDownloads (folder), app-release.apk, **de.giuliomvr.log_v1** _581ba1_0.apk, Framaroot.apk, key.log, penjahad.log	Folder ini memuat data-data penyimpanan memori perangkat *smartphone* Hasil : Ditemukan bukti digital berupa ***file log*** yang bersumber dari aplikasi ***keylogger*** Ditemukan *file* aplikasi ***root*** dan ***keylogger*** dalam bentuk ***file* .apk** sebelum dilakukan instalasi

Tabel 4.8 Rangkuman data hasil akuisisi menggunakan Andriller (Lanjutan)

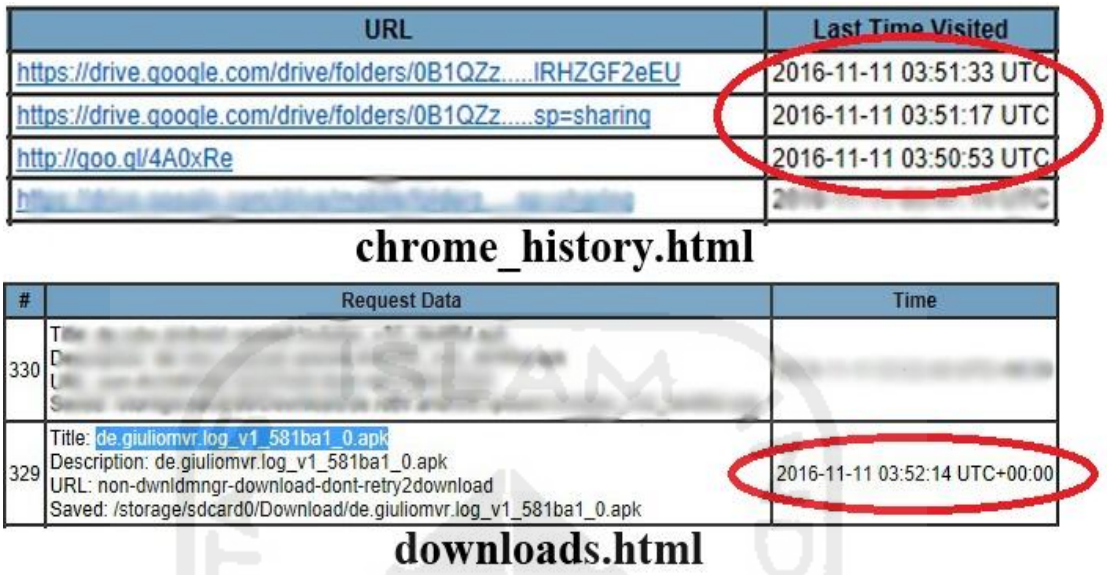
Berkas Folder	Berkas File Isi	Keterangan
(direktori luar)	backup.ab (*file image*), browser_history.html, **chrome_history.html**, chrome_password.html, contacts.html, DataStore.tar, **downloads.html**, log-errors.log, REPORT.html, REPORT.xlsx, sec_call_logs.html, sec_sms_snippets.html, Storage.html, wifi_passwords.html	Merupakan daftar berkas yang berisi data rekam aplikasi atau *cache* di dalam perangkat *smartphone* Hasil : Ditemukan berkas penting terkait tindak kejahatan *fraud*

Proses analisa terhadap data akuisisi yang menggunakan *tool* Andriller memperoleh hasil berupa informasi data-data penting berkaitan dengan tindak kejahatan *fraud*. Bukti-bukti yang dapat menjelaskan bagaimana cara pelaku mendapatkan informasi mengenai akun akses aplikasi layanan *mobile banking* milik korban.

Bukti pertama yaitu ditemukan data *cache* pada *file* **chrome_history.html**. Di dalamnya terdapat informasi bahwa pelaku mengakses sebuah alamat *website* (google drive) untuk menunduh *file* aplikasi *keylogger* yang kemudian diinstal pada perangkat *smartphone* korban. Alamat *website* tersebut diasumsikan menjadi bagian dari rencana pelaku untuk dapat memasukkan aplikasi *keylogger* ke dalam *smartphone* korban tanpa harus melakukan akses pemindahan data menggunakan penyimpanan *external* ataupun akses *file* menggunakan perangkat laptop atau komputer. Aplikasi *keylogger* digunakan oleh pelaku untuk menyimpan semua informasi yang diketik melalui *keyboard virtual* perangkat *smartphone* korban.

Bukti kedua merupakan data *history download* dengan nama *file* **downloads.html**. Di dalam *file* tersebut terdapat informasi yang menunjukkan perangkat *smartphone* korban pernah mengunduh sebuah *file* aplikasi android dengan nama **de.giuliomvr.log_v1_581ba1_0.apk**. *File* aplikasi tersebut diasumsikan sebagai bentuk *file* mentah sebelum diinstal ke dalam *smartphone* korban dan selanjutnya menjadi aplikasi *keylogger*. Asumsi tersebut bersumber dari informasi waktu akses atau *timestamp* pada data **chrome_history.html** dan **downloads.html**. Terjadinya proses akses menggunakan aplikasi **chrome** dan informasi proses unduhan aplikasi dilakukan dalam kurun waktu yang cukup dekat. Hanya terdapat selisih waktu sekitar 2 (dua) menit antara

akses *website* dengan proses mengunduh aplikasi. Temuan bukti berupa selisih waktu akses dan unduh tersebut dapat dilihat pada Gambar 4.7 berikut.



URL	Last Time Visited
https://drive.google.com/drive/folders/0B1QZz.....IRHZGF2eEU	2016-11-11 03:51:33 UTC
https://drive.google.com/drive/folders/0B1QZz.....sp=sharing	2016-11-11 03:51:17 UTC
http://goo.gl/4A0xRe	2016-11-11 03:50:53 UTC
[redacted]	[redacted]

chrome_history.html

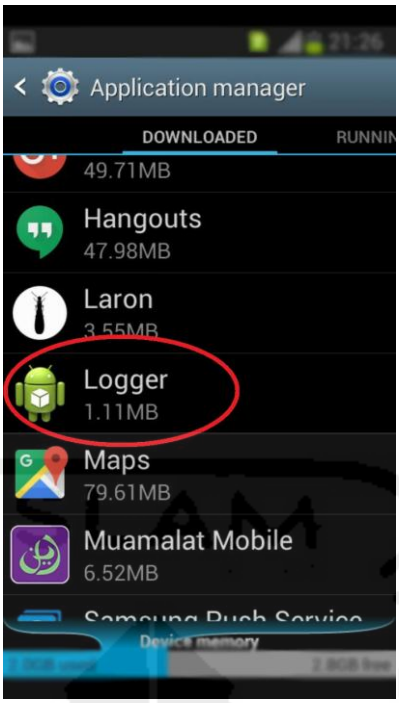
#	Request Data	Time
330	[redacted]	[redacted]
329	Title: de.giuliomvr.log_v1_581ba1_0.apk Description: de.giuliomvr.log_v1_581ba1_0.apk URL: non-dwnldmngr-download-dont-retry2download Saved: /storage/sdcard0/Download/de.giuliomvr.log_v1_581ba1_0.apk	2016-11-11 03:52:14 UTC+00:00

downloads.html

Gambar 4.7 Temuan bukti selisih waktu akses *website* dan proses unduh

Bukti ketiga adalah temuan aplikasi android yang masih mentah atau masih dalam bentuk *file .apk* dengan nama **de.giuliomvr.log_v1_581ba1_0.apk**. Temuan bukti digital tersebut berada di dalam penyimpanan internal perangkat *smartphone* dengan penjelasan direktori **Shared** > **0** > **Download** > **de.giuliomvr.log_v1_581ba1_0.apk**. *File* aplikasi yang tersimpan di dalam folder **Download** tersebut menunjukkan bahwa telah terjadi proses unduh pada perangkat *smartphone*.

Bukti keempat ditemukan pada perangkat *smartphone* milik korban, tepatnya di dalam daftar aplikasi terinstal. Terdapat sebuah aplikasi yang sebelumnya tidak pernah dilakukan instalasi oleh korban. Aplikasi dengan nama **Logger** diyakini sebagai aplikasi *keylogger* yang berfungsi untuk menyimpan semua informasi yang diketik melalui *keyboard virtual* perangkat *smartphone* korban. Dengan menggunakan aplikasi tersebut seluruh hal yang diketik oleh korban di dalam *smartphone* akan tersimpan, bahkan hingga informasi penting terkait akun pribadi, khususnya akun akses aplikasi layanan *mobile banking* yang sudah diincar oleh pelaku. Gambar 4.8 merupakan tampilan *screenshot* yang diambil dari *smartphone* milik korban.



Gambar 4.8 Tampilan *screenshot* bukti instalasi aplikasi **Logger**

Bukti kelima yaitu temuan data penting berupa *file* dengan nama **key.log** yang ditemukan di dalam penyimpanan *internal*. Data tersebut merupakan *file* yang berisi informasi tersimpan seluruh hasil ketikan dari *virtual keyboard* perangkat *smartphone* android milik korban setelah terinstal aplikasi *keylogger*. Ditemukan informasi berisi ID akun dan *password* untuk mengakses aplikasi layanan *mobile banking* korban.

4.4.2. Pengelompokan Data Temuan Bukti Digital

Tahap pengelompokan data temuan bukti digital ini dimaksudkan untuk mempermudah alur analisa yang bersumber dari proses analisis data hasil akuisisi menggunakan *tool* Andriller. Temuan bukti pertama adalah *file cache* yang bersumber dari aplikasi **chrome** *browser* dengan nama *file* **chrome_history.html**. Informasi yang diperoleh menunjukkan bahwa pelaku menggunakan **chrome** *browser* untuk mengunduh aplikasi *keylogger*. Data *history* dari *file* **chrome_history.html** dapat dilihat pada Gambar 4.9 berikut.

Page title	URL	Last Time Visited	Frequency
Google Drive	https://drive.google.com/drive/folders/0B1QZz...IRHZGE2eEU	2016-11-11 03:51:33 UTC	3
apk - Google Drive	https://drive.google.com/drive/folders/0B1QZz.....sp=sharing	2016-11-11 03:51:17 UTC	2
apk - Google Drive	http://goo.gl/4A0xRe	2016-11-11 03:50:53 UTC	1
apk - Google Drive	https://drive.google.com/drive/mobile/folders.....sp=sharing	2016-11-11 03:47:14 UTC	1
Kalian semua suci aku penuh dosa - Google Search	https://www.google.co.id/search?site=&oq=Kal.....enuh+dosa	2016-11-11 03:46:32 UTC	1
Google	http://google.com/	2016-11-10 15:27:05 UTC	3
Google	http://www.google.co.id/?gws_rd=cr&ei=oJEkWJejK8bwvAT65pXoBA	2016-11-10 15:27:05 UTC	1
Google	https://www.google.co.id/?gws_rd=cr,ssl&ei=oJ.....vAT65pXoBA	2016-11-10 15:27:05 UTC	1

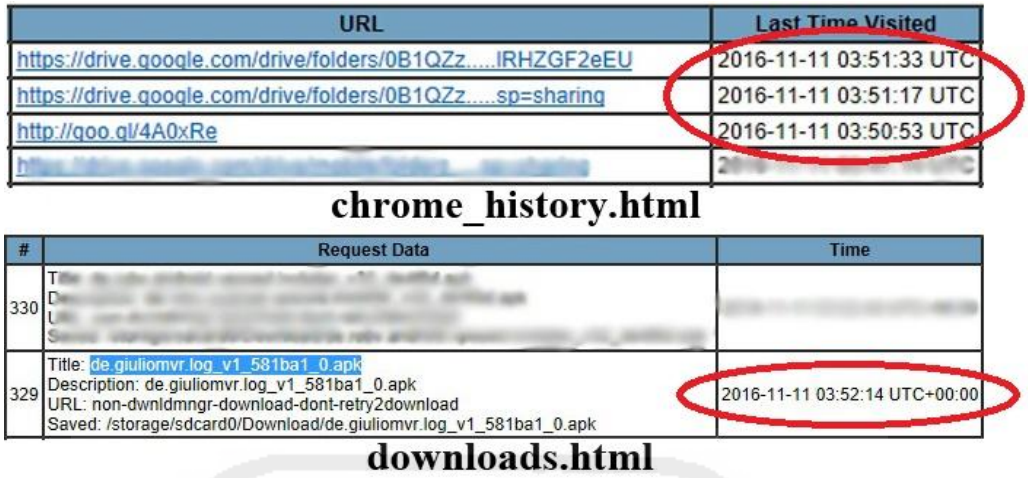
Gambar 4.9 Tampilan informasi di dalam *file* **chrome_history.html**

Bukti digital kedua diperoleh informasi bersumber dari *file history* unduhan di perangkat *smartphone* milik korban dengan nama *file* **downloads.html**. *File* aplikasi mentah *keylogger* yang diinstal tertera di daftar unduhan dengan nama **de.giuliomvr.log_v1_581ba1_0.apk**. Tampilan informasi mengenai *history* unduhan aplikasi *keylogger* terdapat pada Gambar 4.10.

#	Request Data	Requesting App	Size	Status	Time
330	[redacted]	Unknown	711.8 KB	200	[redacted]
319	Title: de.giuliomvr.log_v1_581ba1_0.apk Description: de.giuliomvr.log_v1_581ba1_0.apk URL: non-dwnldmngr-download-dont-retry2download Saved: /storage/sdcard0/Download/de.giuliomvr.log_v1_581ba1_0.apk	Unknown	305.7 KB	200	2016-11-11 03:52:14 UTC+00:00
321	[redacted]	[redacted]	143.3 KB	489	[redacted]

Gambar 4.10 Tampilan informasi unduhan di dalam *file* **downloads.html**

Diasumsikan bahwa aplikasi *keylogger* yang terinstal di dalam *smartphone* korban dilakukan oleh pelaku dengan mengunduh terlebih dahulu menggunakan **chrome** *browser* melalui sebuah alamat *website* **google drive**. Analisa tersebut didasari dari temuan informasi tentang catatan waktu akses pada *browser* **chrome** dengan waktu mengunduh aplikasi yang berdekatan. Telah terjadi akses *browsing* terhadap sebuah alamat *website* **google drive** pada tanggal 11-11-2016, waktu pukul 03:51. Sedangkan proses mengunduh aplikasi *keylogger* terjadi pada tanggal 11-11-2016, waktu pukul 03:52. Informasi tentang *timestamp* kedua hal tersebut dapat dilihat pada Gambar 4.11.



URL	Last Time Visited
https://drive.google.com/drive/folders/0B1QZz.....IRHZGF2eEU	2016-11-11 03:51:33 UTC
https://drive.google.com/drive/folders/0B1QZz.....sp=sharing	2016-11-11 03:51:17 UTC
http://goo.gl/4A0xRe	2016-11-11 03:50:53 UTC
[redacted]	[redacted]

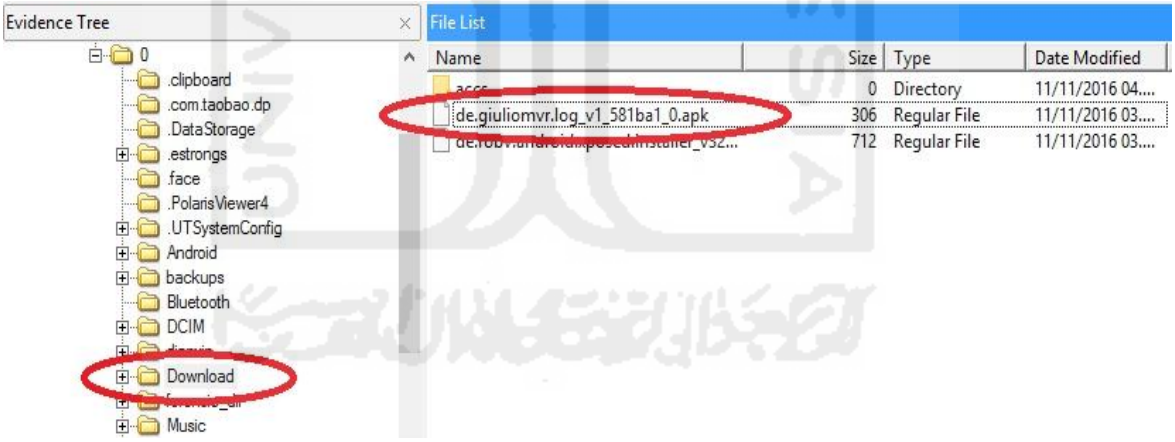
chrome_history.html

#	Request Data	Time
330	[redacted]	[redacted]
329	Title: de.giuliomvr.log_v1_581ba1_0.apk Description: de.giuliomvr.log_v1_581ba1_0.apk URL: non-dwnldmngr-download-dont-retry2download Saved: /storage/sdcard0/Download/de.giuliomvr.log_v1_581ba1_0.apk	2016-11-11 03:52:14 UTC+00:00

downloads.html

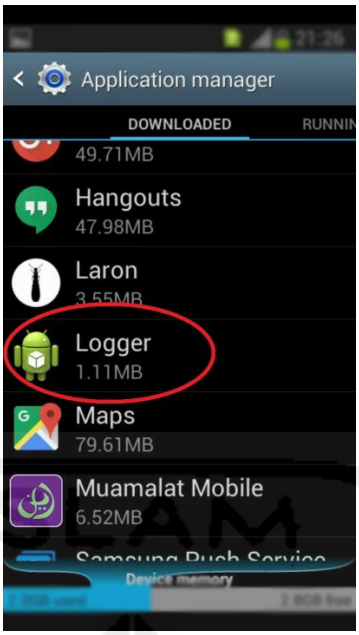
Gambar 4.11 Temuan bukti selisih waktu akses *website* dan proses unduh

Temuan bukti digital ketiga berupa aplikasi awal *keylogger* berekstensi *file* .apk atau aplikasi untuk android dengan nama *file* **de.giuliomvr.log_v1_581ba1_0.apk**. Aplikasi tersebut berada di dalam memori internal *smartphone* milik korban dengan alamat direktori folder **Shared** > **0** > **Download** > **de.giuliomvr.log_v1_581ba1_0.apk**. Temuan *file* tersebut menunjukkan bahwa pernah dilakukan proses unduhan di dalam *smartphonen*, dan diasumsikan proses tersebut dilakukan oleh pelaku. Temuan bukti ketiga terlihat pada Gambar 4.12.



Gambar 4.12 Temuan bukti aplikasi *keylogger* di dalam *folder* Download

Bukti digital keempat yaitu ditemukan aplikasi *keylogger* yang terinstal di perangkat *smartphone* milik korban berada dalam daftar aplikasi dengan nama **Logger**. Korban tidak pernah melakukan instalasi terhadap aplikasi tersebut selama menggunakan *smartphone* yang diteliti. Daftar aplikasi terinstal di perangkat *smartphone* milik korban, khususnya yang terdapat aplikasi **Logger** ditampilkan pada Gambar 4.13 berikut.



Gambar 4.13 Tampilan *screenshot* bukti instalasi aplikasi Logger

Temuan bukti digital kelima adalah *file* **key.log**, merupakan inti informasi penting yang menjadi kunci bukti. Karena berisi informasi mengenai ID dan *password* akun layanan *mobile banking* milik korban. Melalui *file* **key.log** digunakan oleh pelaku untuk mendapatkan akses akun yang asli. Informasi mengenai temuan bukti digital di dalam *file* **key.log** tersaji pada Gambar 4.14.

9911	23.24.20	>net.myinfosys.muamalat.activity>adampray690
9912	23.24.20	>net.myinfosys.muamalat.activity>adampray6902
9913	23.24.24	>net.myinfosys.muamalat.activity>P
9914	23.24.24	>net.myinfosys.muamalat.activity>Pa
9915	23.24.25	>net.myinfosys.muamalat.activity>Pas
9916	23.24.25	>net.myinfosys.muamalat.activity>Pasc
9917	23.24.25	>net.myinfosys.muamalat.activity>Pasca
9918	23.24.25	>net.myinfosys.muamalat.activity>Pascas
9919	23.24.26	>net.myinfosys.muamalat.activity>Pascasa
9920	23.24.26	>net.myinfosys.muamalat.activity>Pascasar
9921	23.24.26	>net.myinfosys.muamalat.activity>Pascasarj
9922	23.24.26	>net.myinfosys.muamalat.activity>Pascasarja
9923	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan
9924	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan4
9925	23.24.35	>net.myinfosys.muamalat.activity>0
9926	23.24.35	>net.myinfosys.muamalat.activity>15/12/2016
9927	23.24.35	>net.myinfosys.muamalat.activity>1
9928	23.24.36	>net.myinfosys.muamalat.activity>15/12/2016

Gambar 4.14 Bukti digital berupa ID dan *password* akses

Gambar 4.14 merupakan tampilan informasi mengenai temuan catatan *keylogger* yang diberi tanda panah dimaksudkan secara khusus menunjukkan keberadaan temuan bukti digital mengenai akses akun aplikasi layanan *mobile banking*. Terdapat catatan waktu akses pada tanggal 15/12/2016, jam 23.24.35 merupakan akses yang dilakukan oleh korban. Dan informasi tersebut diperkirakan digunakan oleh pelaku dalam mengakses *mobile banking* milik korban.

Informasi mengenai ID akun *mobile banking* milik korban yang diperoleh dari *file* **key.log** tertera "23.24.20 > net.myinfosys.muamalat. activity > adampray6902". Menunjukkan bahwa ID akses aplikasi adalah **adampray6902**. Temuan bukti berikutnya adalah *password* akun *mobile banking*. Tertera informasi "23.24.27 > net.myinfosys .muamalat.activity > Pascasarjan4". *Password* yang diperoleh bersumber dari data temuan yaitu **Pascasarjan4**.

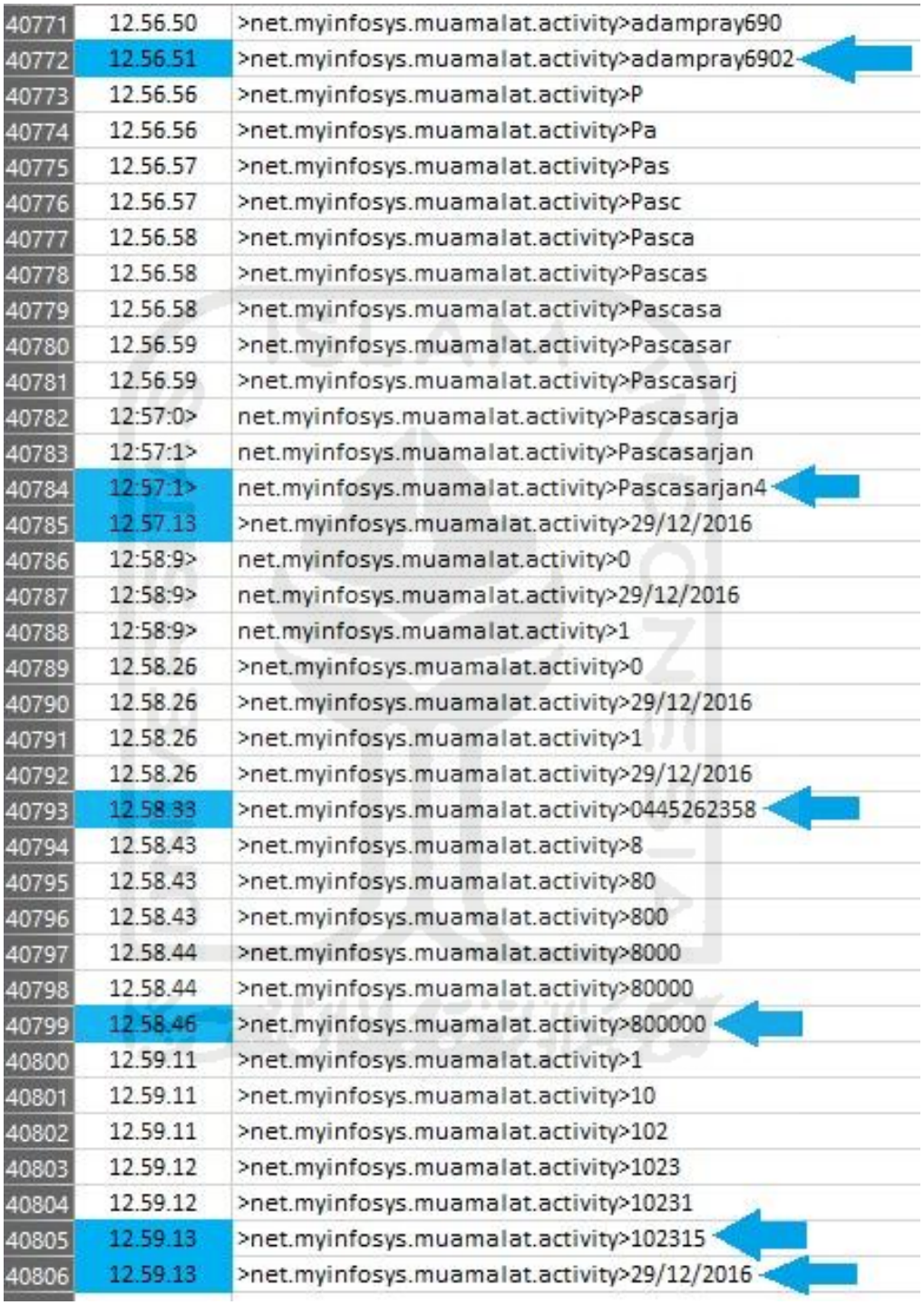
Bukti berupa informasi penting tentang PIN akses transaksi diperoleh dari *file* **key.log**. Tertera informasi "23.24.56 > net.myinfosys.muamalat. activity > 102315". PIN akses *request* transaksi yang diperoleh adalah **102315**. Bukti informasi mengenai PIN akses transaksi dapat dilihat pada Gambar 4.15.

9923	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan
9924	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan4
9925	23.24.35	>net.myinfosys.muamalat.activity>0
9926	23.24.35	>net.myinfosys.muamalat.activity>15/12/2016
9927	23.24.35	>net.myinfosys.muamalat.activity>1
9928	23.24.36	>net.myinfosys.muamalat.activity>15/12/2016
9929	23.24.42	>net.myinfosys.muamalat.activity>5260379595
9930	23.24.55	>net.myinfosys.muamalat.activity>1
9931	23.24.55	>net.myinfosys.muamalat.activity>10
9932	23.24.55	>net.myinfosys.muamalat.activity>102
9933	23.24.56	>net.myinfosys.muamalat.activity>1023
9934	23.24.56	>net.myinfosys.muamalat.activity>10231
9935	23.24.56	>net.myinfosys.muamalat.activity>102315

Gambar 4.15 Bukti digital berupa PIN akses transaksi *mobile banking*

Bersumber dari informasi catatan aktivitas akses terhadap aplikasi *mobile banking* yang dilakukan oleh korban, selanjutnya pelaku menggunakan akses tersebut untuk mencuri uang korban dengan cara mengirimkan uang *via* transfer. Penjelasan mengenai temuan bukti digital yang telah dilakukan oleh pelaku akan dipaparkan beserta dengan penjelasan bahwa benar adanya

catatan yang terdapat pada *file* **key.log** merupakan tindakan yang berasal dari aplikasi *mobile banking*.



40771	12.56.50	>net.myinfosys.muamalat.activity>adampray690
40772	12.56.51	>net.myinfosys.muamalat.activity>adampray6902
40773	12.56.56	>net.myinfosys.muamalat.activity>P
40774	12.56.56	>net.myinfosys.muamalat.activity>Pa
40775	12.56.57	>net.myinfosys.muamalat.activity>Pas
40776	12.56.57	>net.myinfosys.muamalat.activity>Pasc
40777	12.56.58	>net.myinfosys.muamalat.activity>Pasca
40778	12.56.58	>net.myinfosys.muamalat.activity>Pascas
40779	12.56.58	>net.myinfosys.muamalat.activity>Pascasa
40780	12.56.59	>net.myinfosys.muamalat.activity>Pascasar
40781	12.56.59	>net.myinfosys.muamalat.activity>Pascasarj
40782	12:57:0>	net.myinfosys.muamalat.activity>Pascasarja
40783	12:57:1>	net.myinfosys.muamalat.activity>Pascasarjan
40784	12:57:1>	net.myinfosys.muamalat.activity>Pascasarjan4
40785	12.57.13	>net.myinfosys.muamalat.activity>29/12/2016
40786	12:58:9>	net.myinfosys.muamalat.activity>0
40787	12:58:9>	net.myinfosys.muamalat.activity>29/12/2016
40788	12:58:9>	net.myinfosys.muamalat.activity>1
40789	12.58.26	>net.myinfosys.muamalat.activity>0
40790	12.58.26	>net.myinfosys.muamalat.activity>29/12/2016
40791	12.58.26	>net.myinfosys.muamalat.activity>1
40792	12.58.26	>net.myinfosys.muamalat.activity>29/12/2016
40793	12.58.33	>net.myinfosys.muamalat.activity>0445262358
40794	12.58.43	>net.myinfosys.muamalat.activity>8
40795	12.58.43	>net.myinfosys.muamalat.activity>80
40796	12.58.43	>net.myinfosys.muamalat.activity>800
40797	12.58.44	>net.myinfosys.muamalat.activity>8000
40798	12.58.44	>net.myinfosys.muamalat.activity>80000
40799	12.58.46	>net.myinfosys.muamalat.activity>800000
40800	12.59.11	>net.myinfosys.muamalat.activity>1
40801	12.59.11	>net.myinfosys.muamalat.activity>10
40802	12.59.11	>net.myinfosys.muamalat.activity>102
40803	12.59.12	>net.myinfosys.muamalat.activity>1023
40804	12.59.12	>net.myinfosys.muamalat.activity>10231
40805	12.59.13	>net.myinfosys.muamalat.activity>102315
40806	12.59.13	>net.myinfosys.muamalat.activity>29/12/2016

Gambar 4.16 Bukti digital akses aplikasi *mobile banking* oleh pelaku

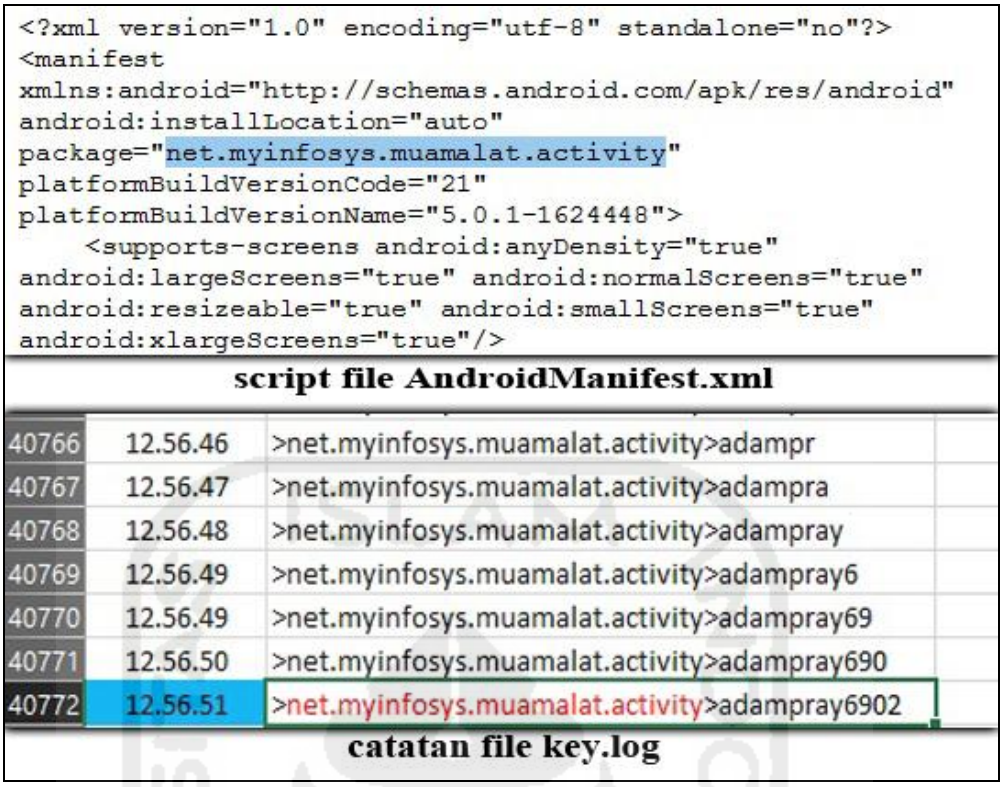
Paparan Gambar 4.16 merupakan temuan bukti digital hasil kejahatan pelaku dalam menggunakan akses akun *mobile banking* milik korban secara ilegal. Tindakan tersebut dilakukan oleh pelaku pada saat korban lengah terhadap pengawasan perangkat *smartphone* miliknya.

Tindakan akses ilegal atau *fraud* terhadap akun *mobile banking* korban yang dilakukan oleh pelaku dapat dibuktikan pada tampilan Gambar 4.16. Bahwa telah dilakukan akses pada tanggal 29 Desember 2016 dan waktu sekitar pukul 12.57 sebagaimana terlampir pada temuan bukti catatan *file* **key.log** tertulis ">net.myinfosys.muamalat.activity >29/12/2016". Akses tersebut diduga dilakukan oleh pelaku, karena korban tidak melakukan akses *mobile banking* pada tanggal dan waktu tersebut.

Pelaku melakukan akses aplikasi *mobile banking* menggunakan ID akun **adampray6902** dan *password* **Pascasarjan4** milik korban. Selanjutnya pelaku melakukan transfer dana di rekening milik korban dengan nominal **Rp 800.000,-** (delapan ratus ribu rupiah) dengan nomor rekening tujuan **0445262358**. PIN akses untuk pengesahan permintaan transfer tertera dengan nomor **102315**. Bukti-bukti tersebut dipaparkan pada Gambar 4.16 dengan tanda panah sebagai penanda.

Pembuktian keabsahan bahwa akses *fraud* yang dilakukan oleh pelaku memang menggunakan aplikasi layanan *mobile banking* milik korban dapat dicocokkan pada sumber akses di dalam catatan *file* **key.log** dengan *script* perintah akses pada hasil *decompile* aplikasi. Pada catatan *record* di dalam *file* **key.log** tertulis sumber yang tersimpan adalah "net.myinfosys.muamalat.activity". Keterangan tersebut merupakan salah satu *script* perintah akses yang terdapat di dalam struktur perintah aplikasi *mobile banking*.

Sehingga dapat disimpulkan bahwa memang benar tindakan akses akun secara ilegal dan pencurian dana dengan cara transfer yang dilakukan oleh pelaku bersumber dari aplikasi *mobile banking*. Pembuktian tersebut terilustrasikan pada Gambar 4.17 dengan cara mencocokkan kedua hasil temuan bukti yang bersumber pada dua data berbeda.



Gambar 4.17 Kecocokan kedua bukti dari dua *file* berbeda

Pemaparan ilustrasi pada Gambar 4.17 merupakan penjelasan mengenai bukti temuan yang terdapat di dalam *file* **key.log** dengan deskripsi ”net.myinfosys.muamalat.activity” sesuai dengan salah satu *script* perintah pada aplikasi *mobile banking* yang telah dilakukan proses *decompile* atau pembedahan program.

4.4.3. Pelaporan Hasil

Setelah selesai dilakukan investigasi dan analisa terhadap perangkat *mobile* yang digunakan sebagai media penunjang fasilitas *mobile banking*, peneliti membahas hasil utama dari rangkaian proses yang telah dilakukan. Meskipun terdapat kendala pada kasus nyata, namun urutan proses telah dilakukan sesuai dengan rencana dan mengacu pada penelitian terdahulu yang pernah dilakukan.

4.4.3.1. Hasil Investigasi Data Aplikasi *Mobile Banking*

Berdasarkan pada hasil investigasi dan analisa terhadap data *image* hasil proses *cloning* pada perangkat bukti dan diperkuat dengan data hasil *decompile* aplikasi *mobile banking*, peneliti menyimpulkan bahwa tidak ditemukan artefak data bukti digital yang dapat digunakan. Pada

penelitian ini aplikasi tersebut hanya melakukan perintah *request* transaksi oleh nasabah kepada sistem server perbankan yang selanjutnya ditampilkan pada layar perangkat *smartphone*, tanpa melakukan penyimpanan atau pencatatan data-data penting terkait identitas akses *mobile banking*, *log* akses, maupun *history* transaksi yang pernah dilakukan.

4.4.3.2. Hasil Investigasi Data Akuisisi *Smartphone*

Bersumber pada tahap analisa data data hasil akuisisi menggunakan Andriller dan tahap pengelompokan data temuan bukti digital, didapatkan hasil berupa beberapa informasi bukti digital terkait tindak kejahatan *fraud* yang mengincar aplikasi layanan *mobile banking* dengan serangkaian proses terencana untuk mendapatkan informasi penting mengenai akun akses layanan. Diasumsikan pelaku melakukan serangkaian proses tahapan demi mendapatkan informasi akun akses dan berhasil melakukan transfer dana yang merugikan korban dengan memanfaatkan situasi pada saat korban lengah terhadap perangkat *smartphone* yang digunakannya.

Beberapa bukti digital yang ditemukan telah disusun guna menjelaskan asumsi bagaimana proses tindak kejahatan *fraud* tersebut dilakukan. Serta menjelaskan apa saja bukti informasi terkait akun akses yang telah didapatkan oleh pelaku.

4.5. Komparasi Hasil Dengan Penelitian Terdahulu

Hasil pengujian dan analisa pada penelitian ini terhadap aplikasi *mobile banking* menerangkan bahwa tidak terdapat atau tidak tersimpan informasi penting sebagai data bukti digital yang berkaitan dengan catatan akses yang pernah dilakukan. Sehingga aplikasi *mobile banking* tersebut memiliki tingkat keamanan yang prima dari segi sistem pengamanan aplikasi. Tetapi tindak kejahatan *fraud* yang terjadi menggunakan aplikasi ketiga, dengan fungsi melakukan penyimpanan terhadap seluruh informasi hasil ketikan dari *virtual keyboard* di dalam perangkat *smartphone*.

Informasi yang menyimpan kata-kata hasil penulisan atau ketikan dari *virtual keyboard* tersebut selanjutnya dimanfaatkan oleh pelaku untuk melakukan tindak kejahatan *fraud*. Meskipun kemungkinan tetap terdapat kesulitan bagi pelaku untuk memanfaatkan keadaan pada saat korban lengah terhadap pengawasan *smartphone* miliknya.

Hasil analisa yang dilakukan peneliti terhadap aplikasi *mobile banking* ini memiliki kesimpulan yang hampir sama dengan penelitian (Nosrati 2015) menyimpulkan bahwa aplikasi

mobile banking yang mereka teliti memiliki sistem pengamanan berupa autentikasi dan autorisasi tanpa melakukan penyimpanan informasi penting terkait *history* akses.

Berbeda dengan penelitian (Simate 2013) yang meneliti sistem keamanan dari segi penyedia layanan jaringan pada sebuah layanan *mobile banking* yang masih perlu pembenahan. Karena saat itu (tahun 2013) hampir seluruh penyedia layanan seluler masih menggunakan sinyal data jaringan 2G. Di mana peneliti menyatakan bahwa sistem keamanan pada jaringan 3G lebih aman dan kompleks untuk digunakan sebagai jalur data layanan *mobile banking*.

Bab 5 Kesimpulan dan Saran

5.1. Kesimpulan

Setelah peneliti melakukan rangkaian penelitian dan analisa terhadap sebuah aplikasi *mobile banking*, dapat diambil kesimpulan bahwa sistem perintah dasar pada alur proses aplikasi *mobile banking* tidak melakukan perintah penyimpanan data penting milik nasabah sebagai akses legal dan sah. Sehingga di dalam perangkat *smartphone* tidak ditemukan data penting yang dapat digunakan sebagai potensi bukti digital ataupun celah keamanan. Di dalam direktori data yang berkaitan dengan aplikasi *mobile banking* tidak tersimpan catatan akun pengguna atau nasabah, *log* aktifitas penggunaan aplikasi, *history* transaksi, serta data penting lain yang berkaitan dengan otentikasi akses aplikasi.

Kesimpulan tersebut didukung berdasarkan analisa terhadap data hasil *decompile* atau pembedahan proses aplikasi *mobile banking*. Pada *script* perintah kerja aplikasi hanya melakukan *request* akses terhadap layanan yang disediakan oleh perbankan melalui aplikasi. Dan fungsi aplikasi *mobile banking* hanya sebagai perantara akses tanpa melakukan penyimpanan informasi yang telah diakses oleh nasabah.

Kesimpulan berikutnya adalah tindak kejahatan *fraud* yang terjadi tidak secara langsung mencari informasi pada objek aplikasi *mobile banking*. Melainkan menggunakan aplikasi berupa *keylogger* dengan tujuan untuk mendapatkan semua informasi yang tersimpan hasil dari penulisan atau ketikan pada *virtual keyboard* di dalam perangkat *smartphone*. Kemudian pelaku memanfaatkan informasi akun akses aplikasi *mobile banking* tersebut untuk mencuri uang milik korban yang berada di rekening bank dengan cara transfer dana. Meskipun kemungkinan tetap terdapat kesulitan bagi pelaku untuk memanfaatkan keadaan pada saat korban lengah terhadap pengawasan *smartphone* miliknya.

5.2. Kritik dan Saran

Penelitian dengan judul Pengembangan *Mobile Forensics* Pada Aplikasi *Mobile Banking* Menggunakan Metode *Static Forensics* dapat dikatakan telah selesai. Namun pada penelitian ini

diharapkan menuai kritik dan saran guna membangun penelitian selanjutnya yang berkaitan dengan *mobile forensics* khususnya dengan tema penelitian tentang aplikasi ataupun layanan *mobile banking*.

5.2.1. Kritik

Peneliti mengharapkan kritik yang dikhususkan pada topik yang berkaitan dengan *literature review*, penelitian terdahulu sebagai acuan serta sumber untuk dapat dikembangkan pada penelitian berikutnya. Karena pada penelitian ini masih dianggap kurang memenuhi jawaban untuk mendapati informasi atau data yang dapat digunakan sebagai bukti digital, baik dalam langkah akuisisi maupun analisa.

5.2.2. Saran

Saran merupakan media untuk menyampaikan kekurangan peneliti dalam melakukan proses dan menyelesaikan penelitian. Sehingga diharapkan banyak saran dari para pembaca maupun peneliti mengenai bidang terkait dalam penelitian ini. Serta masih terbatasnya *tools* atau aplikasi pendukung penelitian mengenai *mobile forensics* yang peneliti ketehaui perlu penambahan informasi mengenai hal tersebut bersumber dari penelitian yang lain. Untuk penelitian berikutnya dapat pula melakukan akuisisi secara fisik dengan harapan adanya temuan bukti-bukti digital yang berkaitan langsung terhadap aplikasi *mobile banking*.

Daftar Pustaka

Bojjagani, S., 2015. SSMBP : A Secure SMS-based Mobile Banking Protocol with Formal Verification. , pp.252–259.

Cho, T., Kim, Y. & Han, S., 2013. Potential Vulnerability Analysis of Mobile Banking Applications. , (2012), pp.1114–1115.

Hadi, S. & Indonesia, U.I., Faktor-Faktor Yang Mempengaruhi Penggunaan. , pp.55–67.

Hussain, A., Abubakar, H.I. & Hashim, N.B., 2015. Evaluating mobile banking application: Usability dimensions and measurements. *Conference Proceedings - 6th International Conference on Information Technology and Multimedia at UNITEN: Cultivating Creativity and Enabling Technology Through the Internet of Things, ICIMU 2014*, (1), pp.136–140.

Mrdovic, S., Huseinovic, A. & Zajko, E., 2009. Combining static and live digital forensic analysis in virtual environment. *IEEE International Symposium on Information, Communication and Automation Technologies (ICAT)*, pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5348415.

Mumba, E.R., 2014. Mobile Forensics using the Harmonised Digital Forensic Investigation Process.

Narendiran, C., Rabara, S.A. & Rajendran, N., 2009. Public key infrastructure for mobile banking security. *2009 Global Mobile Congress*, pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5295898.

Nosrati, L., 2015. Security assessment of Mobile- Banking. , pp.1--5.

Overview, A., 2007. Mobile Banking Technology Options. , (August).

Panja, B. et al., 2013. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. *2013 International Conference on Collaboration Technologies and Systems (CTS)*, pp.397–403. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6567261.

Purwanegara, M., Apriningsih, A. & Andika, F., 2014. Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes. *Procedia -Social and Behavioral Sciences*, 115(Iicies 2013), pp.147–155. Available at: http://dx.doi.org/10.1016/j.sbspro.2014.02.423.

Qian, Z., Luo, D. & Wu, S., 2008. Analysis and design of a mobile forensic software system based on AT commands. *2008 IEEE International Symposium on Knowledge Acquisition and Modeling Workshop Proceedings, KAM 2008*, (60704042), pp.597–600.

Simate, Z., 2013. Evaluation of Mobile Network Security. *Information Science, Computing and Telecommunications (PACT), 2013 Pan African International Conference*, pp.170–175. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7055108.

To, W. & Lai, L.S.L., 2017. Mobile Banking and Payment in China. , (June 2013). Trends, G., 2015. Mobile Banking. , (July).

Zefferer, T. & Teufl, P., 2013. Policy-based Security Assessment of Mobile End-user Devices - An Alternative to Mobile Device Management Solutions for Android Smartphones. *International Conference on Security and Cryptography*, pp.347–354. Available at: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0004509903470354.