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.

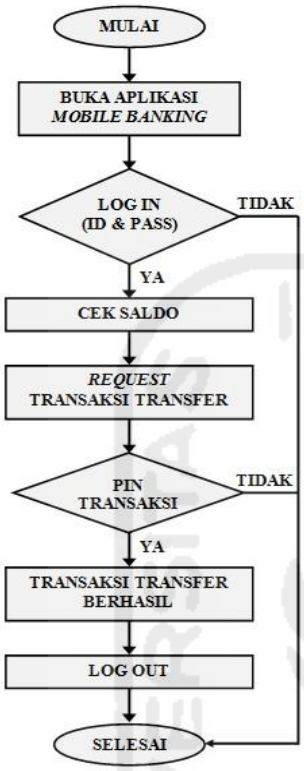
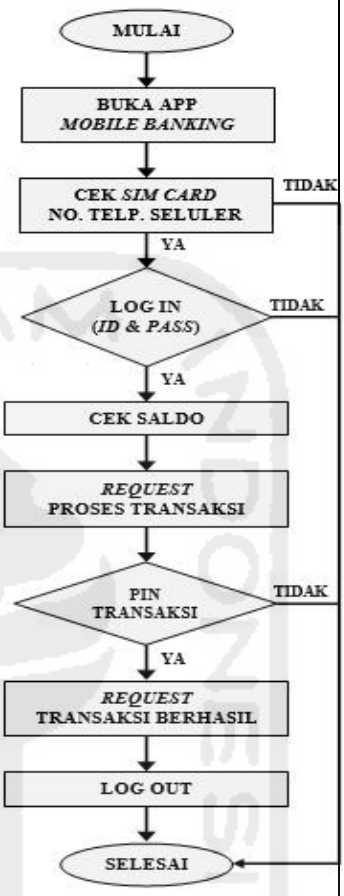
4.1.2. Alur proses aplikasi

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*

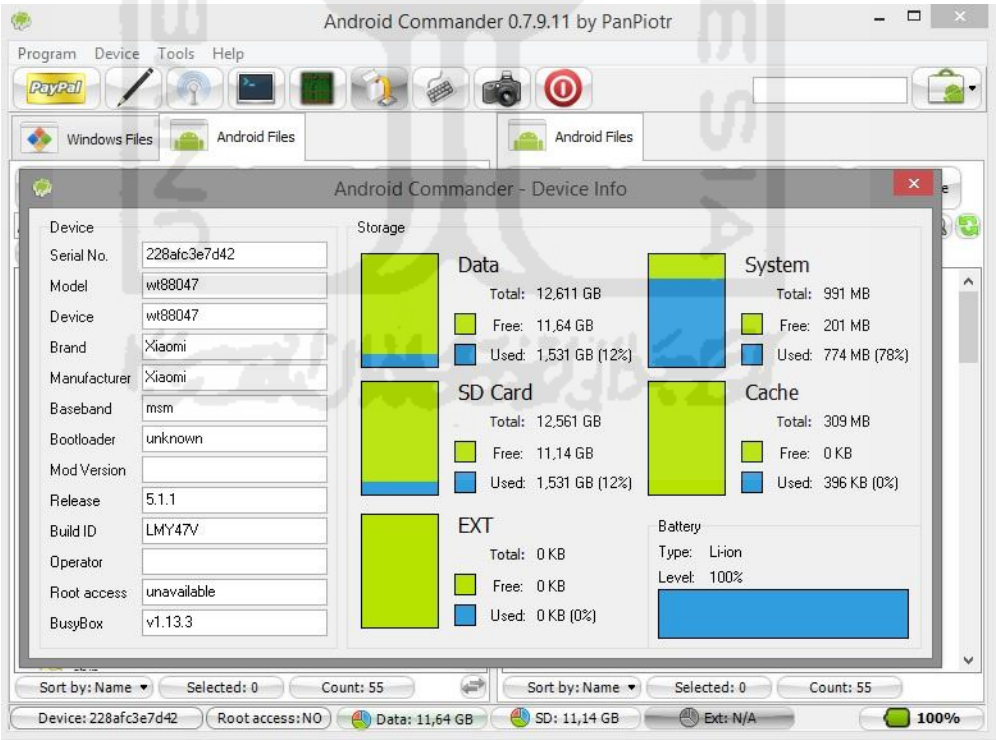
Langkah selanjutnya memberikan label keterangan dan pencatatan penanganan barang bukti sebelum proses pemindahan menuju lokasi penyimpanan. Guna memisahkan antara bukti pada kasus yang sedang ditangani dengan bukti kasus lainnya. Pemberian label keterangan dapat

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.

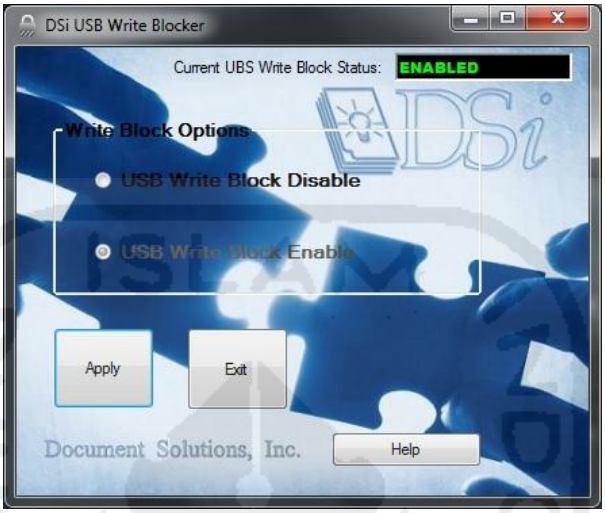
4.3.3. Akuisisi Potensi Bukti Digital

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

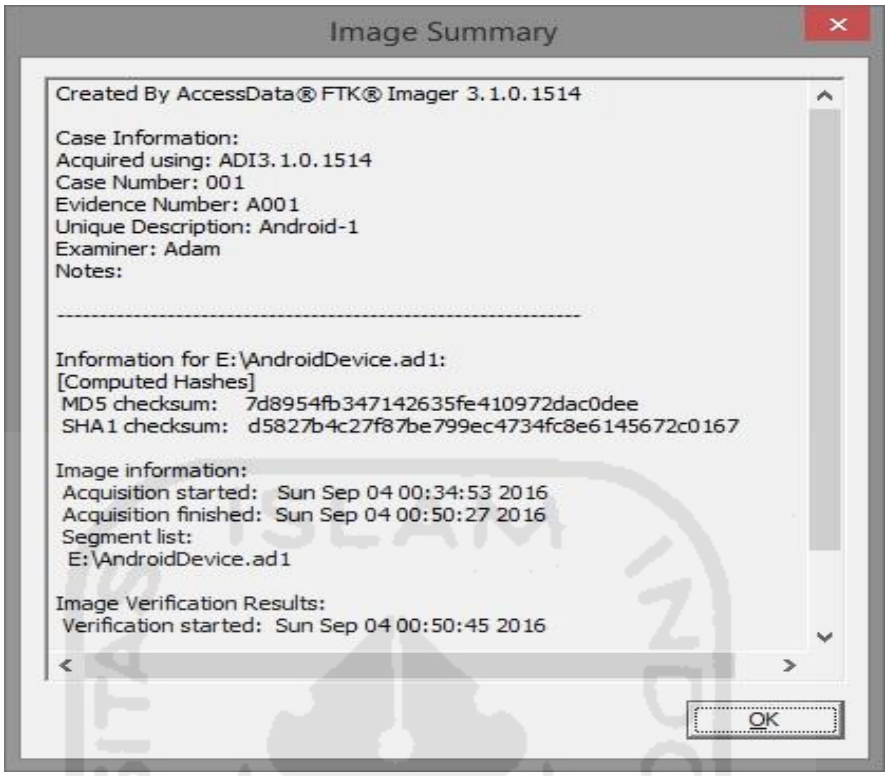
Untuk memastikan keaslian data yang telah diakuisisi, peneliti melakukan pencatatan nilai *hash* pada data hasil *imaging*. Terdapat beberapa informasi penting yang harus dicatat, seperti waktu akuisisi, nilai *hash*, dan ukuran data hasil *imaging*. Karena informasi nilai *hash* hasil *cloning* nantinya 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.Do TransferRtgs doTransferSkn.url = net.myinfosys.json.mobile.Do TransferSknGen2 doPaymentTelco.url = net.myinfosys.json.mobile.Do PaymentTelco getHistoryDetailInquiry.url = net.myinfosys.json.mobile.Get HistoryDetailInquiry doPaymentVirtualAccount.url = net.myinfosys.json.mobile.DoPayment VirtualAccount	getPromotion.url = net.myinfosys.json.mobile.GetPromotion getPromotImage.url = net.myinfosys.json.mobile.GetPromotIma doInquiryPaymentPln.url = net.myinfosys.json.mobile.DoInquiry PaymentPln doPaymentPln.url = net.myinfosys.json.mobile.DoPaymentPln getVoucherPln.url = net.myinfosys.json.mobile.GetVoucher doInquiryVirtualAccount.url = net.myinfosys.json.mobile.DoInquiry VirtualAccount 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.

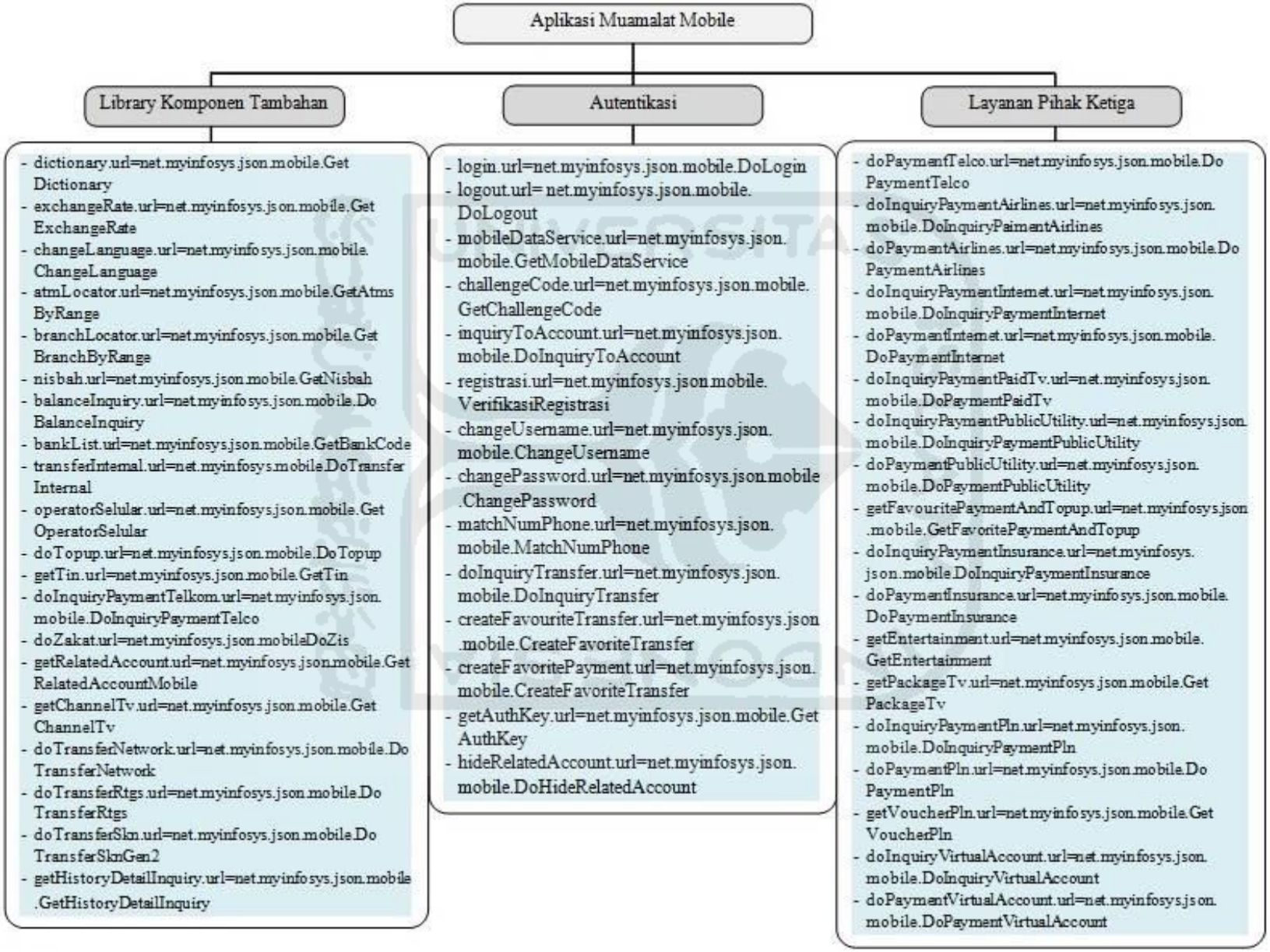
Berdasarkan hasil analisa, di dalam *file* **AndroidManifest.xml** berisi *script* perintah perijinan *library* aplikasi atau *uses permission* dengan fungsi agar barisan perintah di dalam direktori aplikasi *mobile banking* dapat dijalankan pada sistem android. Terdapat 14 (empat belas) perintah perijinan 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
[illegible]	[illegible]

chrome_history.html

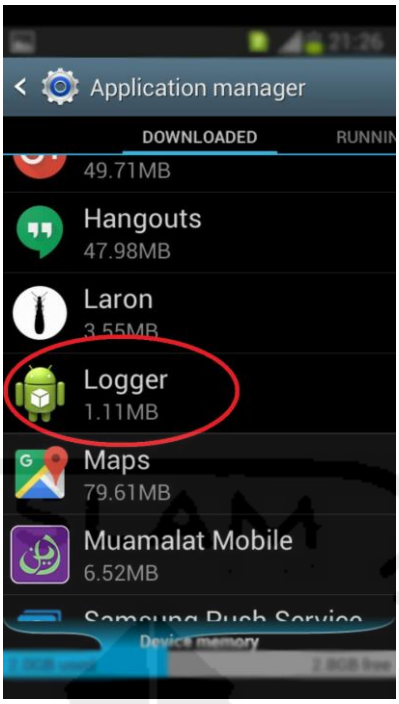
#	Request Data	Time
330	[illegible]	[illegible]
329	Title: de.giuliomvr.log_v1_581ba1_0.apk Description: de.giuliomvr.log_v1_581ba1_0.apk URL: non-dwnldmngr-download-dont-retry2download Saved: /storage/sdcard0/Download/de.giuliomvr.log_v1_581ba1_0.apk	2016-11-11 03:52:14 UTC+00:00

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...IRHZGF2eFU	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=Kali.....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	[illegible]	Unknown	711.8 KB	200	[illegible]
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	[illegible]	com.google.android	145.3 KB	489	[illegible]

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
[illegible]	[illegible]

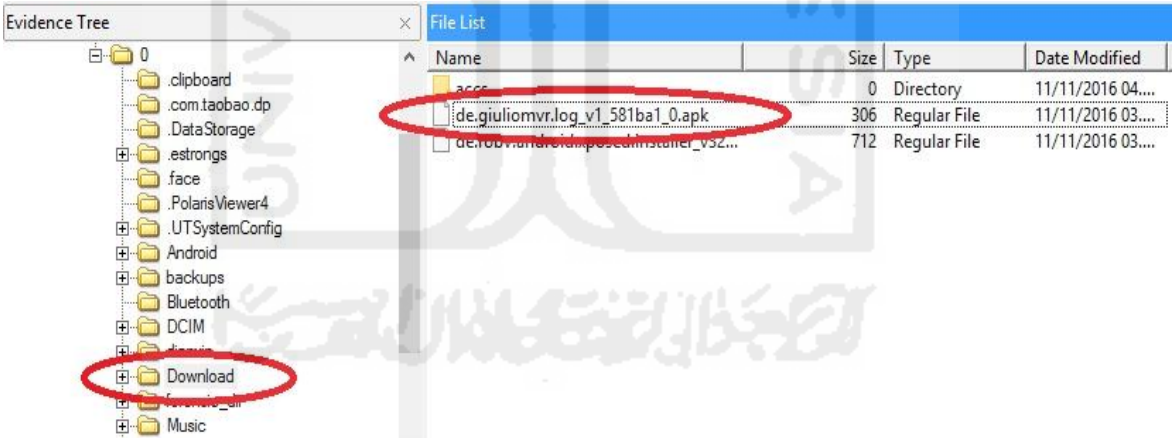
chrome_history.html

#	Request Data	Time
330	[illegible]	[illegible]
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

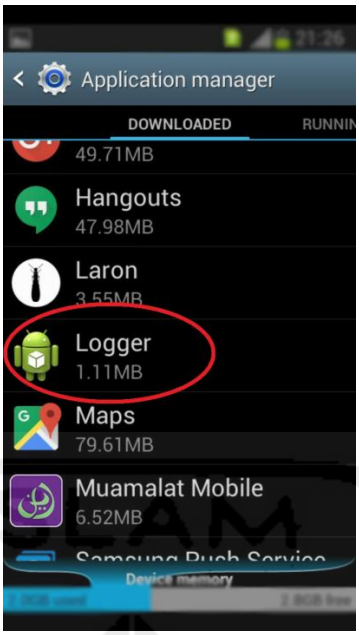
Gambar 4.11 Temuan bukti selisih waktu akses *website* dan proses unduh

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.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
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"/>
```

script file AndroidManifest.xml

40766	12.56.46	>net.myinfosys.muamalat.activity>adampr
40767	12.56.47	>net.myinfosys.muamalat.activity>adampra
40768	12.56.48	>net.myinfosys.muamalat.activity>adampray
40769	12.56.49	>net.myinfosys.muamalat.activity>adampray6
40770	12.56.49	>net.myinfosys.muamalat.activity>adampray69
40771	12.56.50	>net.myinfosys.muamalat.activity>adampray690
40772	12.56.51	>net.myinfosys.muamalat.activity>adampray6902

catatan file key.log

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*.