Jurnal Ilmiah Sinus (JIS) Vol : 18, No. 1, Januari 2020
ISSN (Print) : 1693-1173, ISSN (Online): 2548-4028

Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid

Hendro Wijayanto[1)], Dedy Hariyadi[2)], Abdul Haris Muhammad [3)]
[1)] Program Studi Teknik Informatika, STMIK Sinar Nusantara
[2)] Program Studi Teknologi Informasi, Universitas Jendral Achmad Yani Yogyakarta
[3)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Maluku Utara
[1)] hendro@sinus.ac.id, [2)] dedy@unjaya.ac.id, [3)] abdulharis@ummu.ac.id

ABSTRACT

Penetration of internet usage in Indonesia has increased by 10.12% from 2017 to 2018. This has led to very rapid technological growth, such as the growth of online loan services or Financial Technology (Fintech). This condition makes the emergence of illegal fintech services built by certain groups to reap profits. Illegal fintech service providers stand building applications with a lot of personal data requested at registration. Starting from personal data, family, work up to banking are accompanied by photo evidence and contact numbers. Hybrid analysis is needed to see the extent in which the fintech application treats customer data. In this technique, there are static analysis and dynamic analysis. Static analysis is used to see the extent in which the fintech application runs on Smartphone devices with required data and other policies. Dynamic analysis is used to view the activity of tiles and permissions of fintech applications from source code, malware analysis, and permission analysis. Hybrid analysis results show that all fintech applications have a huge potential for misuse of customer's personal data. This is indicated by the existence of a data collection URL that can be accessed by the public, there are malware activities, READ_PHONE_STATE and READ_CONTACS permissions so that fintech application providers freely monitor all contact activities, locations on the customer's Smartphone. The results of the analysis can be used to recommend fintech service users to be careful of fintech applications. Moreover, it can be used as a reference for making illegal fintech detection frameworks.

Keywords : *Digital Forensic Analysis, Hybrid Analysis, Fintech, Personal Data, Data Breach*

I. PENDAHULUAN

Negara Indonesia merupakan negara berkembang dengan tingkat perkembangan yang sangat tinggi dibanding dengan negara di Asia Tenggara. Khususnya dibidang teknologi informasi dan internet. Hal ini terasa dari beberapa kebijakan pemerintah yang mendorong masyarakatnya menggunakan teknologi, mulai dari sektor pendidikan, bisnis, transportasi dan lainnya. Bahkan fenomena politik tak lepas dari keterkaitan teknologi informasi. Masyarakat tingkat menengah-bawah pun harus siap dengan perkembangan yang begitu pesat. Semua ini terbukti dari survey Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2018 dalam hal penetrasi dan perilaku pengguna internet Indonesia. Dalam laporannya terdapat peningkatan perubahan pengguna internet dari 54,68% di tahun 2017 menjadi 64,8% di tahun 2018, seperti Tabel 1

Tabel 1. Penetrasi Pengguna Internet Indonesia (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2018)

Tahun	2017	2018
Populasi Penduduk (juta)	262	264, 16
Pengguna Internet (juta)	143,26	171,17
Persentase (%)	54,68 %	64,8 %

Dari penetrasi pengguna internet tersebut, Pulau Jawa berkontribusi sebesar 55,7% dari total sebaran pengguna internet di seluruh Indonesia. Dari hasil survey yang sama pula, 93,9 % pengguna internet di Indonesia tehubung dengan *Smartphone* setiap hari.

Dengan tingginya angka penguna internet ini, banyak bermunculan industri *Financial Technology (Fintech)* dimana perkembangannya sudah dimulai dari tahun 2015. Hadirnya Asosiasi Fintech Indonesia (AFI) bertujuan menyediakan partner bisnis dan dapat terbentuknya *Bank Indonesia Fintech Office* di tahun 2016. Selain itu juga dapat menjadi wadah regulasi *fintech* yang dapat diawasi oleh Otoritas Jasa Keuangan Indonesia (OJK). Otoritas Jasa Keuangan sendiri sudah mengeluarkan peraturan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, yang didalamnya berisi penyelenggara, kegiatan usaha, batas pinjaman, sampai dengan mitigasi resiko. Inilah yang menjadi pesatnya industri *fintech* di Indonesia.

Seiringnya waktu, industri *fintech* di Indonesia mulai menjamur dengan minimnya pengawasan yang ketat. Otoritas Jasa Keuangan sendiri merilis terdapat sebanyak 404 *fintech* ilegal di Desember 2018, dimana dibulan November 2018 terdapat 1130 pengaduan korban *fintech* ilegal. Dengan jenis pelanggaran mulai dari denda keterlambatan yang tinggi, komisi/bunga tinggi dan teror yang dilakukan oleh perusahaan *fintech*. Di internet sudah banyak aplikasi-aplikasi *fintech* bersebaran bebas. Bahkan di aplikasi *Playstore Android* banyak ditemukan aplikasi *fintech*. Minimnya kesadaran masyarakat terhadap rentannya penyalahgunaan data pribadi, menjadi alasan mudahnya melakukan pengajuan pinjaman atau pembiayaan online lewat aplikasi *fintech*. Aplikasi *fintech* yang banyak bertebaran inilah dapat menimbulkan potensi resiko penyalahgunaan data pribadi yang diupload pada saat pengajuan pembiayaan. Apalagi proses pembuatan dan pengembangan aplikasi sangat mudah dilakukan tanpa harus memiliki pengalaman *programming*. Dari kejadian inilah muncul permasalahan yang menjadi topik besar penelitian ini. Yaitu bagaimana pola aplikasi *fintech* dalam menyebarkan informasi/data pribadi nasabah ke pihak ketiga sehingga dapat memicu kejahatan dunia maya. Hasil dari analisis ini nantinya dapat digunakan untuk pembuatan *framework security assessment* dalam hal keamanan data pribadi di aplikasi *fintech*. Selain dari hal tersebut, dapat digunakan untuk acuan dalam mengenali ciri-ciri *fintech illegal* yang dapat merugikan masyarakat.

II. TINJAUAN PUSTAKA

Seseorang yang dapat diidentifikasi adalah seseorang yang dapat dikenali secara langsung maupun tidak langsung berdasarkan nomor tanda pengenal atau berdasarkan faktor spesifik dari identifikasi fisik, psikologi, mental, budaya atau sosial. Perlindungan data pribadi dalam bidang perbankan telah diatur dalam Pasal 40 Undang-undang Nomor 10 Tahun 1998 tentang perbankan. Berdasarkan ketentuan tersebut bank wajib merahasiakan keterangan mengenai nasabah (Dewi Rosadi & Gumelar Pratama, 2018).

Data-data pribadi berkenaan dengan kependudukan dan demografis di Indonesia seperti NIK, E-KTP dan KK sangat penting dilindungi agar tidak mudah dieksploitasi. Ada beberapa bentuk penyalahgunaan data seperti penjualan data, data *profiling*, tujuan pemasaran, penelitian, bahkan termasuk pemantauan/*spionase*. Yang lebih berbahaya penyalahgunaan data pribadi untuk tindak kriminal seperti pembuatan akun palsu, penipuan, pencucian uang, pemerasan dan transaksi ilegal (Sautunnida, 2018).

 DOI : https://doi.org/10.30646/sinus.v18i1.433

Berdasarkan sumber dari Otoritas Jasa Keuangan (OJK) Indonesia, bahwa *fintech* ilegal memiliki ciri-ciri sebagai berikut :

1. Tidak memiliki izin resmi
2. Tidak ada identitas pengurus dan alamat
3. Pemberian pinjaman sangat mudah
4. Informasi bunga biaya pinjam dan denda tidak jelas
5. Bunga /biaya pinjam tidak terbatas
6. Total pengembalian (termasuk denda) tidak terbatas
7. Penagihan tidak ada batas waktu
8. Tidak ada layanan pengaduan
9. Akses ke seluruh data yang ada di ponsel
10. Ancaman teror kekerasan, penghinaan, pencemaran nama baik, menyebarkan foto/video pribadi, dan menyebarkan identitas pribadi

Penggunaan data pribadi yang dikelola untuk maksud tertentu tidak boleh tanpa persetujuan subjek data, digunakan untuk maksud lain selain daripada maksud untuk mana data pribadi terebut digunakan. Data pribadi tidak boleh diperlakukan atau digunakan secara bertentangan dengan maksud penggunaannya. Semua langkah akses data yang diperlukan, perlu ditempuh oleh pengelola data untuk mencegah akses data, pemrosesan data, perubahan data, pengungkapan data serta perusakan data yang dapat merugikan nasabah (Rosadi, 2017).

Software reengineering adalah pemeriksaan dan perubahan terhadap sebuah subyek sistem untuk menyusun kembali ke dalam sebuah bentuk yang baru sesuai bentuk yang baru tersebut. Proses rekayasa ulang ini mencakup 4 (empat) tujuan, yaitu *Understanding (predictive), Repairing (corrective), Improving (perfective)* dan *Evolving (adaptive)*. Sedangkan *Reengineering* terdiri dari dua proses utama, yaitu *reverse* dan *forward engineering*. *Reverse engineering* merupakan proses yang tidak melibatkan perubahan sistem. Sebuah sistem *software* dianalisis untuk mengekstrak informasi dari *software*, maka pilihan yang harus dilakukan adalah antara analisis statis dan dinamik (Rahmadani, Raharjana, & Taufik, 2015).

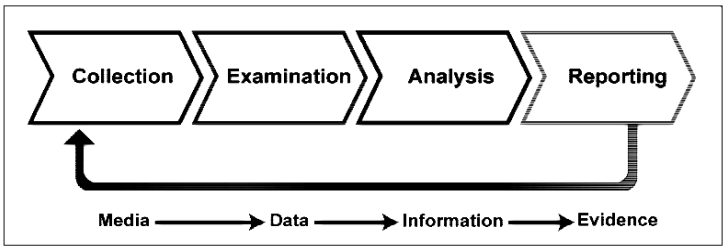
Analisis statis merupakan teknik pengumpulan data secara manual. Dimana setiap sistem atau aplikasi dibuka sumber *source code*-nya dan karakteristik *string*-nya. Biasanya teknik analisis statis ini hanya melibatkan sedikit *tools* dan menghasilkan data analisis yang sedikit. Oleh karena itu untuk memperbanyak data yang dibutuhkan, diperlukan metodologi lain, yaitu analisis dinamis. Analisis dinamis melibatkan aplikasi atau sering disebut dengan proses *reengineering*. Analisis ini memungkinkan sistem/aplikasi dijalankan seperti keadaan sesungguhnya dan dapat dianalisa pola, data serta teknik yang digunakan (Lin, Chen, Zhu, Yang, & Wei, 2018).

Dalam sebuah aplikasi terdapat kategori dimana aplikasi tersebut dikatakan aman dari penyalahgunaan data (Mark, 2013), yaitu :

1. Kontrol akses aplikasi yang memastikan identitas di autentikasi dan di otorisasi untuk melihat data yang dilindungi melalui aplikasi.
2. Aplikasi harus memastikan keamanan koneksi antara pengguna, database dan aplikasi.
3. Audit dan pencatatan aktifitas untuk memberikan pelaporan yang valid dan tidak valid setiap aktifitas dalam aplikasi.
4. Kode aplikasi dan manajemen konfigurasi yang memastikan kode tersebut aman.

Kategori inilah yang menjadi ukuran data pengguna aplikasi dijamin keamanannya dari penyalahgunaan pihak luar maupun dalam sistem aplikasi.

Digital forensik merupakan metode ilmiah yang digunakan untuk pengumpulan data informasi, identifikasi analisis, interpretasi dan penyajian bukti digital yang berasal dari sumber digital, dengan tujuan memfasilitasi pelaporan atau mengantisipasi tindakan kejahatan dunia maya (Palmer, 2001).



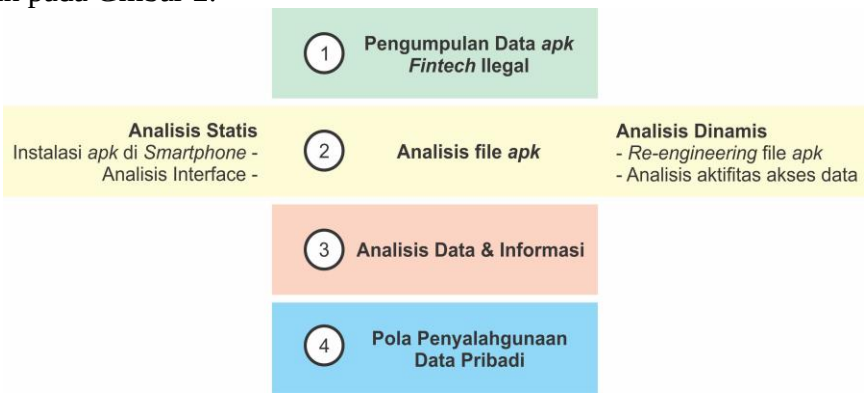
Gambar 1. Digital Forensic Process (Baryamureeba & Tushabe, 2004)

Dalam digital forensik, terdapat 4 (empat) langkah untuk menemukan bukti digital atau kesimpulan dari suatu kejahatan dunia maya.

1. *Collection*. Yaitu proses pencarian barang bukti berupa temuan-temuan, pengakuan barang bukti dan dokumentasi.
2. *Examination*. Pada proses ini data akan ditarik keterkaitannya dengan data lain, kesesuaian, kejelasan dan relevansinya.
3. *Analysis*. Melakukan pemeriksaan data yang sesuai, membandingkan, menemukan dan menghasilkan fakta-fakta.
4. *Reporting*. Penulisan laporan uraian dari hasil pemeriksaan dan analisis dari seluruh penyelidikan.

III. METODE PENELITIAN

Metode yang digunakan untuk menganalisis aplikasi *fintech* adalah menggunakan teknik hibrid. Dimana teknik ini tidak lepas dari teknik dasar Digital Forensik dalam melakukan analisis seperti ditunjukkan pada Gambar 1. Alur dari metode penelitian ditunjukkan pada Gmbar 2.



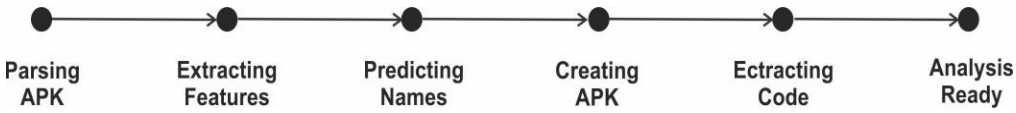
Gambar 2. Metode Analisis Hibrid *File apk fintech* illegal

File yang dianalisis adalah file dengan ekstensi *apk* atau paket *Android Package File*. Dimana file *apk* merupakan file berkas yang digunakan oleh *Smartphone* android sebelum dilakukan instalasi. Adapun tahapan analisis hibrid yaitu :

 DOI : https://doi.org/10.30646/sinus.v18i1.433

Tahap 1 Pengumpulan data *apk fintech* ilegal. Pengambilan data aplikasi dilakukan dengan cara mendownload langsung *file apk fintech* ilegal yang dirilis oleh Otoritas Jasa Keuangan (OJK) Indonesia. Dalam penelitian ini digunakan 5 sampel data aplikasi *fintech* berekstensi *apk*.

Tahap 2 Analisis *file apk*. Dalam proses analisis dilakukan menggunakan model hibrid. Dimana didalamnya terdapat analisis statis dan analisis dinamis. Pada tahapan analisis statis, aplikasi *apk* dicoba di install langsung di dalam *Smartphone* kemudian dilakukan analisis interface dan data yang dimasukkan. Sedangkan analisis dinamis dilakukan dengan cara melakukan *re-engineering source code* dan analisis keamanan proses berjalannya aplikasi fintech serta aktifitas *malware*. Proses *re-engineering* dapat ditunjukkan pada Gambar 3



Gambar 3. Proses *Re-Engineering File apk*

Tahap 3 Analisis data dan informasi. Tahapan ini dilakukan setelah *file apk* ditemukan data-data dan informasi terkait penyalahgunaan data nasabah/pengguna aplikasi *fintech*. Data dan informasi ini akan menggambarkan karakteristik masing-masing aplikasi *fintech* dalam proses mengambil data pribadi pengguna. Mulai dari data KTP, data kerabat/keluarga, data kontak yang berada di *smartphone*, data perbankan, model penyebaran data pribadi di internet, sampai dengan data dan informasi perilaku aplikasi dalam *Smartphone*.

Tahap 4 Pola penyalahgunaan data pribadi. Setelah ditemukan ciri dan model aplikasi *fintech* dalam mencuri dan menyebarluaskan data pribadi nasabahnya, akan dikelompokkan dan dapat ditarik kesimpulan berupa pola penyalahgunaan data pribadi nasabah *fintech*.

IV. HASIL DAN PEMBAHASAN

Dalam penelitian ini, digunakan lima data sampel aplikasi *fintech* ilegal berbasis Android yang didapat dari rilis resmi Otoritas Jasa Keuangan (OJK) dan di unduh dari *URL Web* maupun *Play Store Google*. Beberapa aplikasi memang sudah tidak ada atau dihapus dari *Play Store* atas otoritas keamanan Indonesia untuk meminimalisir terjadinya korban penyalahgunaan data pribadi. Tetapi aplikasi masih dapat diperoleh lewat URL web *fintech* ilegal tersebut atau lewat *apk bucket* dan *apk pure*.

4.1 Analis Statis Aplikasi *Fintech* Ilegal Android *apk*

Analisis statis diawali dengan meng-*install* aplikasi kedalam *Smartphone* Android. Dalam penelitian ini tidak menggunakan emulator karena dimungkinkan hasil analisis kurang akurat. Disebabkan di dalam emulator tidak terdapat nomor telepon dan pencatatan lokasi sebagai syarat utama verifikasi masuk ke aplikasi. Analisis *interface* diperlukan untuk melihat sejauh mana aplikasi meminta data nasabah dalam proses pengajuan pinjaman *online*. Adapun hasil dari analisis statis ditunjukkan pada Tabel 2 berikut

Tabel 2. Hasil Analisis Statis Aplikasi *Fintech* Ilegal

Data / Informasi	**(1) Uang Now**	**(2) Duit Kita**	**(3) Dompet Kredit**	**(4) Raja Uang**	**(5) Mitra Dana**
Developer	Hemm Picken	Denise Scioneaux	Colman Scot	NA	KSP Mitra Dana Nusantara
URL Web	http://uangnow.com/	NA	NA	http://www.rajauang.mobi/	http://www.mitradana nusantara.com
Nama File	com.bbdd.cabjagbbagcfef_ 2019-06-11.apk	DuitKita kredit lancar hidup lancar Cepat_v1.0.11. 42418_ apkpure.com	com.beomargin. DompetKredit _2018-09-28	mobi.uangraja. android_ 2018-09-19	anda.mcvbmxb.jsdgh_ 2019-06-15
Kebijakan Privasi dan Penggunaan Data	Ada	Ada	Tidak Jelas / Tidak Ada	Tidak Jelas / Tidak Ada	Tidak Jelas / Tidak Ada
Informasi Pinjaman & Bunga	1. Jumlah Pinjaman Rp. 1.000.000,- s.d Rp. 2.000.000,- 2. Bunga Tidak Dijelaskan 3. Jangka Waktu 7 hari untuk semua plaform	1. Jumlah Pinjaman Rp. 1.000.000,- s.d Rp. 15.000.000,- 2. Bunga Tidak Dijelaskan 3. Jangka Waktu tidak dijelaskan	1. Jumlah Pinjaman Rp. 1.000.000,- s.d Rp. 10.000.000,- 2. Bunga Tidak Dijelaskan 3. Jangka Waktu 7 - 14 hari	1. Jumlah Pinjaman Rp. 600.000,- s.d Rp. 2.000.000,- 2. Bunga Tidak Dijelaskan 3. Jangka Waktu 7 - 14 hari	1. Jumlah Pinjaman Rp. 1.000.000,- 2. Bunga 0.07% 3. Jangka Waktu 14 hari
Data Pribadi	1. NIK 2. Nama lengkap 3. Tempat & tanggal lahir 4. Alamat lengkap 5. Jenis kelamin 6. Agama 7. Status 8. Hunian/Rumah	1. NIK 2. Nama lengkap 3. Tempat & tanggal lahir 4. Alamat lengkap 5. Jenis kelamin 6. Agama 7. Status 8. Hunian/Rumah 9. NPWP	1. NIK 2. Nama lengkap 3. Tempat & tanggal lahir 4. Alamat lengkap 5. Jenis kelamin 6. Agama 7. Status	1. NIK 2. Nama lengkap 3. Tempat & tanggal lahir 4. Alamat lengkap 5. Jenis kelamin 6. Agama 7. Status	1. NIK 2. Nama lengkap 3. Tempat & tanggal lahir 4. Alamat lengkap 5. Jenis kelamin 6. Agama 7. Status
Data Keluarga	1. Ibu Kandung 2. Saudara Sekandung 3. Jumlah Anak	1. Ibu Kandung 2. Saudara Sekandung 3. Jumlah Anak	1. Ibu Kandung	1. Ibu Kandung 2. Saudara Sekandung	1. Ibu Kandung 2. Saudara Sekandung
Data Kontak Telepon	1. Ayah Kandung 2. Ibu Kandung 3. Kerabat Dekat Minimal 2	1. Ibu Kandung 2. Kerabat Dekat Minimal 3	1. Ibu Kandung 2. Kerabat Dekat Minimal 2	1. Ibu Kandung 2. Kerabat Dekat Minimal 2	1. Ibu Kandung 2. Kerabat Dekat Minimal 3
Data Pekerjaan	1. Instansi 2. Alamat Instansi 3. Telp Instansi 4. Posisi Pekerjaan 5. Lama Pekerjaan 6. Gaji	1. Instansi 2. Alamat Instansi 3. Telp Instansi 4. Posisi Pekerjaan 5. Lama Pekerjaan 6. Gaji	1. Instansi 2. Alamat Instansi 3. Telp Instansi 4. Posisi Pekerjaan 5. Lama Pekerjaan 6. Gaji	1. Instansi 2. Alamat Instansi 3. Telp Instansi 4. Posisi Pekerjaan 5. Lama Pekerjaan 6. Gaji	1. Instansi 2. Alamat Instansi 3. Telp Instansi 4. Posisi Pekerjaan 5. Lama Pekerjaan 6. Gaji
Data Perbankan dan Lainnya	Tidak Ada	1. Rekening Tabunga Bank Lain 2. Kartu Kredit	Tidak Ada	Tidak Ada	Rekening Tabungan Bank Lain
Data File Upload	1. Foto Pribadi & KTP	1. Foto Pribadi & KTP 2. Foto NPWP 3. Foto Whatsapp	1. Foto Pribadi & KTP	1. Foto Pribadi & KTP	1. Foto Pribadi & KTP
Data Agunan	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada
Data Media Sosial	1. Whatsapp 2. Facebook	1. Whatsapp 2. Email 3. Facebook 3. Instagram	Tidak Ada	Tidak Ada	1. Facebook 2. Instagram 3. Whatsapp
Verifikasi SMS/ Telp	SMS	SMS	SMS	SMS dan Telp	SMS
Verifikasi Lokasi	GPS	GPS	GPS	GPS	GPS
Verifikasi Video Call	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada
Model Pencairan & Pengembalian	Transfer Bank	Transfer Bank	Transfer Bank	Transfer Bank	Transfer Bank

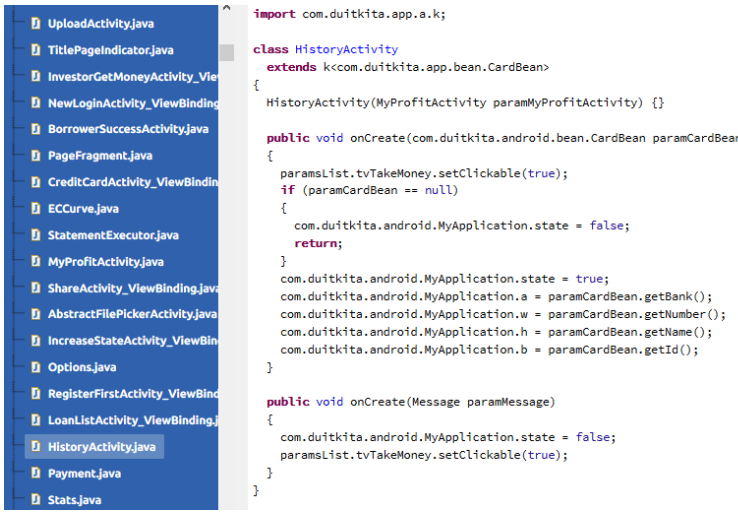
Dari hasil analisis statis Tabel 2 diatas dapat ditarik kesimpulan bahwa terdapat data penting dan proses penting yang seharusnya melalui verifikasi dan dokumentasi. Kebijakan privasi dan penggunaan data merupakan ukuran pertama yang harus disiapkan oleh penyedia layanan pinjaman online. Kebijakan ini merupakan sebuah perjanjian awal dalam penggunaan dan transaksi data informasi yang diberikan oleh calon peminjam. Dari kelima sampel diatas, hanya 2 yang memberikan informasi kebijakan privasi data. Akan tetapi hal ini tidak menjadi ukuran pasti bahwa penyedia layanan akan menjaga dengan benar data pribadi tersebut. Kebijakan tersebut akan berpengaruh terhadap kerahasiaan data pribadi, data keluarga, data kontak, data pekerjaan, data perbankan dan data media sosial. Selain itu layanan verifikasi *video call* juga tidak disediakan di aplikasi pinjaman *online*. Verifikasi *video call* merupakan cara penyedia layanan untuk memastikan bahwa calon peminjam yakin dengan layanan yang diberikan. Selain itu, penggunaan verifikasi *video call* ini akan meminimalisir penggunaan data calon peminjam *online*.

4.2 Analis Dinamis Aplikasi *Fintech* Ilegal Android *apk*

Analisis dinamis dilakukan menggunakan 2 (dua) cara. Pertama yaitu menggunakan teknik *re-engineering file apk*, yang nantinya merubah file apk menjadi file *source code* untuk dapat dianalisis alur sistemnya. Sedangkan yang kedua menggunakan teknik analisis proses genetik, atau sering disebut *Genetik Malware Analysis*. Teknik ini akan melihat proses apk apakah mengandung aktifitas mencurigakan dalam pencurian data informasi atau tidak.

4.2.1 *Re-enginering File apk*

Tahapan proses *re-engineering dari file apk* menjadi source code dapat dilihat pada Gambar 3. *Re-engineering* atau *Deobfuscation* dalam penelitian ini menggunakan *tools apk-deguard*

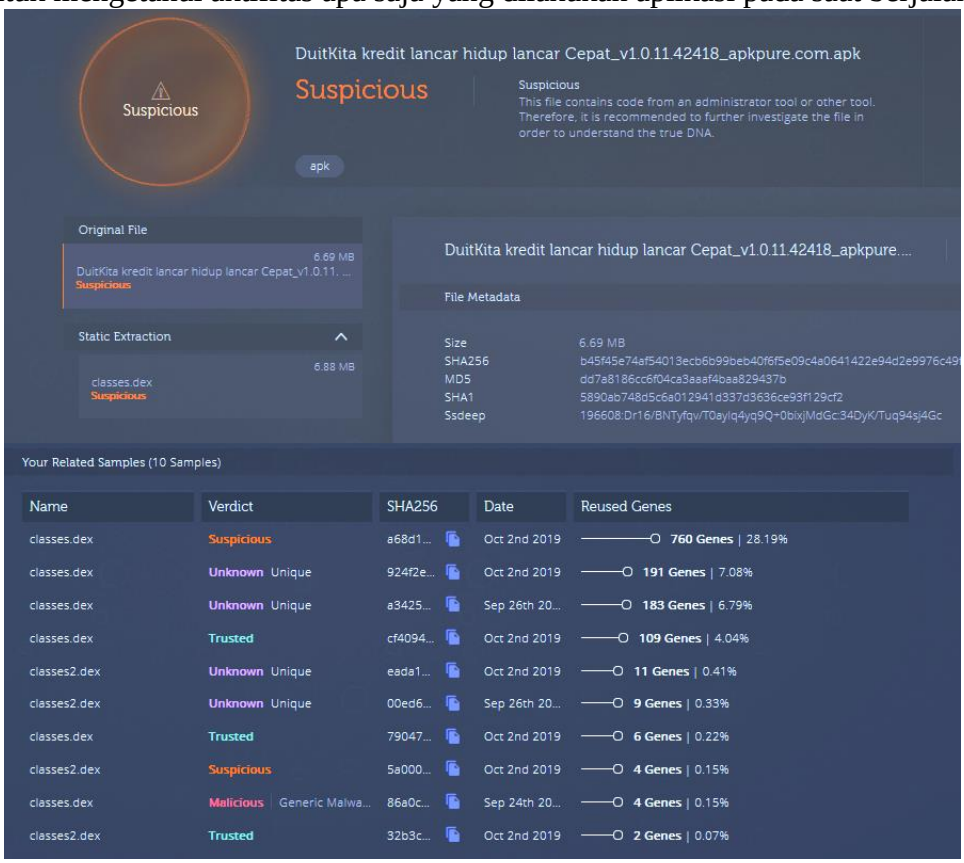


Gambar 4. *Deobfuscation file apk fintech* ilegal

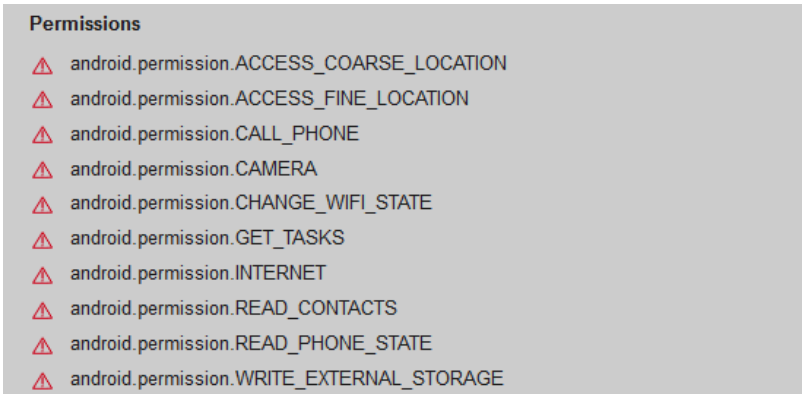
Proses *deobfuscation* menunjukkan bahwa sampel aplikasi menunjukkan alamat *URL* admin mereka dan bahkan melakukan verifikasi data perbankan seperti data Kartu Kredit. Karena beberapa alamat *URL* sampel aplikasi ini sudah diblokir, dibutuhkan akses *proxy* untuk dapat masuk ke dalamnya. Beberapa *URL* juga mulai dinonaktifkan demi keamanan nasabah *fintech*.

4.2.2 Analisis Aktifitas Genetik

Analisis genetik dilakukan untuk melihat aktifitas yang menyerupai aktifitas *backdoor*, *malware* dan *virus*. Dimana aktifitas tersebut dapat memicu pencurian data. Analisis menggunakan *tools Intezer*, dan *Virustotal*. Selain itu juga dapat untuk mengetahui aktifitas apa saja yang dilakukan aplikasi pada saat berjalan.



Gambar 5. Analisis Aktifitas Genetik dengan Intezer



Gambar 6. Analisis *Permision* dengan Virustotal

Berdasarkan analisis Gambar 5 dan Gambar 6, bahwa ternyata aplikasi *fintech* ilegal ini mengandung aktifitas *malware* yang sengaja diciptakan oleh *Administrator fintech* untuk dapat mengambil data lebih banyak dari nasabah *fintech*. Aktifitas ini dapat dikatakan ilegal karena vendor aplikasi dapat membuka informasi/berkas utuh dari data personal nasabah. Kesimpulan hasil analisis dinamis dapat ditunjukkan pada Tabel 3. Dalam Tabel 3 dapat ditunjukkan

perbandingan antar aplikasi *fintech* dalam hal sejauh mana aplikasi tersebut mampu mengambil data / informasi pengguna *fintech*.

Tabel 3. Hasil Analisis Dinamis Aplikasi *Fintech* Ilegal

Data / Informasi	(1) Uang Now	(2) Duit Kita	(3) Dompet Kredit	(4) Raja Uang	(5) Mitra Dana
Akses Data (apk-deguard)	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka
Aktifitas Malware (Intezer)	Mencurigakan	Mencurigakan	Terpercaya	Mencurigakan	Mencurigakan
Permissions (Virus Total)	1. ACCESS_COARSE_LOCATION 2. ACCESS_FINE_LOCATION 3. CAMERA 4. INTERNET **5. READ_CONTACTS** **6. READ_PHONE_STATE** 7. WRITE_EXTERNAL_STORAGE	1. ACCESS_COARSE_LOCATION 2. ACCESS_FINE_LOCATION 3. CALL_PHONE 4. CAMERA 5. CHANGE_WIFI_STATE 6. GET_TASKS 7. NTERNET **8. READ_CONTACTS** **9. READ_PHONE_STATE** 10. WRITE_EXTERNAL_STORAGE	1. CAMERA 2. GET_TASKS 3. INTERNET **4. READ_PHONE_STATE** 5. WRITE_EXTERNAL_STORAGE	1. ACCESS_COARSE_LOCATION 2. ACCESS_FINE_LOCATION 3. CAMERA 4. GET_TASKS 5. INTERNET 6. READ_CALL_LOG **7. READ_CONTACTS** **8. READ_PHONE_STATE** 9. READ_SMS 10. RECORD_AUDIO 11. WRITE_EXTERNAL_STORAGE	1. ACCESS_COARSE_LOCATION 2. ACCESS_FINE_LOCATION 3. CALL_PHONE 4. CAMERA 5. CHANGE_WIFI_STATE 6. INTERNET **7. READ_CONTACTS** **8. READ_PHONE_STATE** 9. READ_PROFILE 10. RECORD_AUDIO 11. SYSTEM_ALERT_WINDOW 12. WRITE_EXTERNAL_STORAGE

Permissions dalam sebuah sistem adalah pemberian izin aplikasi terhadap informasi dan data yang ada di dalam *Smartphone*. Dari Tabel 3 diketahui bahwa semua aplikasi *fintech* meminta *permission* untuk melakukan pembacaan penyimpanan di *Smartphone*, yaitu *permission READ_PHONE_CONTACTS*. Selain itu juga terdapat permintaan izin untuk pembacaan daftar kontak telepon yang tersimpan di *Smartphone*, yaitu *READ_CONTACTS*. Hal ini dapat disimpulkan bahwa data informasi yang tersimpan dalam *Smartphone* dapat diakses oleh vendor/administrator *fintech*, ketika di dalam *Smartphone* terinstall aplikasi tersebut. Sehingga berpotensi data informasi yang seharusnya tidak dibutuhkan untuk syarat pengajuan pinjaman, dapat diambil oleh vendor *fintech* ilegal.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian ini dapat disimpulkan bawha :

1. Aplikasi pinjaman *online* atau *fintech* ilegal memberikan kemudahan dalam bertransaksi dengan banyak data pribadi yang diperlukan untuk pendaftaran. Selain itu meniadakan *Video Call* sebagai salah satu persyaratan untuk mengganti verifikasi langsung dengan calon nasabah sesuai yang disyaratkan oleh Otoritas Jasa Keuangan (OJK) membuat aplikasi *fintech* rentn penyalahgunaan data pribadi.

2. Mudahnya vendor / administrator *fintech* mengambil data nasabah selain data yang dimasukkan ketika melakukan registrasi *fintech*. Hal ini terbukti dari *Permission* aplikasi Android *fintech*. Seluruh sampel aplikasi memberikan *permission READ_PHONE_STATE* dan *READ_CONTACS* sehingga penyedia aplikasi fintech dengan leluasa memantau seluruh aktifitas *contact* di *Smartphone* nasabah.

5.2 Saran

Dengan mudahnya penyalahgunaan data pribadi di aplikasi *fintech*, perlu dibuat *framework assessment* aplikasi *fintech* yang dapat digunakan sebelum aplikasi diupload di *Play Store* atau internet. Perlu juga membangun kesadaran masyarakat terhadap pentingnya perlindungan data pribadi dengan cara melakukan sosialisasi terhadap ciri-ciri aplikasi *fintech* ilegal.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2018). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia*. Indonesia.

Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *Proceedings of the Digital Forensic Research Conference, DFRWS 2004 USA*, 1–9.

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/vej.2916

Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. *Digital Investigation*, *26*, S59–S66. https://doi.org/10.1016/j.diin.2018.04.012

Mark, R.-O. (2013). *Information Security The Complete Reference, Second Edition*. 896. Retrieved from www.it-ebooks.info/book/3340

Palmer, G. L. (2001). *A Road Map for Digital Forensic Research*.

Rahmadani, V. S., Raharjana, I. K., & Taufik, T. (2015). Penerapan Reverse Engineering Dalam Penentuan Pola Interaksi Sequence Diagram Pada Sampel Aplikasi Android. *Journal of Information Systems Engineering and Business Intelligence*, *1*(1), 25. https://doi.org/10.20473/jisebi.1.1.25-32

Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya. *Sosiohumaniora*, *19*(3), 206–212.

Sautunnida, L. (2018). Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384.