Jurnal TIKomSiN, Vol. 9, No. 2, Oktober 2021 ISSN Cetak : 2338-4018
DOI: https://doi.org/10.30646/tikomsin.v9i2.572 ISSN Online : 2620-7532

Analisis Forensik Pada Aplikasi Peduli Lindungi Terhadap Kebocoran Data Pribadi

Hendro Wijayanto[1)]; Daryono[2)]; Siti Nasiroh[3)]
[1)]Program Studi Informatika, STMIK Sinar Nusantara
[2)]Program Studi Pendidikan Teknologi Informasi, Universitas Slamet Riyadi
[3)]Program Studi Informatika, Universitas Perwira Purbalingga
[1)]hendro@sinus.ac.id; [2)]cahkra2010@gmail.com; [3)]nasiroh.pwt@gmail.com[3]

ABSTRACT

Peduli Lindungi Application is an application coming from the Ministry of Communication and Information Technology Indonesia which has function to tracking and stop spread of Coronavirus Disease (COVID-19). Its application has personal data which includes, registration number, date of birth, full name, address and telephone number. However, Peduli Lindungi Application is one of the factors which are caused of personal data breach. Digital forensics is a scientific field that has functions to find out facts and finding a crime case. It wishes that will get directions whether this application is safety or not. The researchers hope that the people will not be afraid to use Peduli Lindungi Application and also can support the government programs to prevent the spread of Covid-19. The result of forensic analysis with static and dynamic analysis models, it shows that Peduli Lindungi Application is safe to used and it is not as dangerous applications. The results of this analysis show that Peduli Lindungi application has their own permission configurations based on the users. There is no malware in the script or activities and there is no database and data stored in smartphone memory as well as some encrypted program data. Personal data breach is caused by lacking of people knowledge to protect their personal data. Moreover , sometimes people forget to protect their security of their smartphones.

Keywords*: Mobile forensic, Digital forensic, Peduli lindungi application, Covid-19*

I. PENDAHULUAN

Tahun 2021 merupakan tahun kedua Pandemi *Coronavirus Disease 2019 (Covid-19)* melanda Negara Indonesia pada khususnya. Hal ini memberikan dampak yang signifikan terhadap berbagai macam sektor. Dimana banyak kegiatan-kegiatan yang dialihkan menjadi kegiatan daring. Sehingga penggunaan teknologi informasi dan komputer mengalami peningkatan. Ini berdampak terhadap semakin tingginya serangan kejahatan siber. Dalam studi kesiapan kejahatan siber menunjukkan tingkat kesiapan pengguna teknologi informasi dan komputer sebesar 3,3 dari total skala 5 atau masuk di kategori rentan [1].

Di sisi lain Pemerintah Republik Indonesia mengeluarkan aplikasi Peduli Lindungi sebagai bentuk upaya pencegahan dan monitoring penyebaran *Covid-19* serta program vaksinasi nasional. Akan tetapi hal ini menyebabkan keteledoran pengguna aplikasi Peduli Lindungi dalam hal perlindungan data pribadi. Dilansir CNN Indonesia tanggal 4 September 2021 ramai diperbincangkan atas bocornya Nomor Induk Kependudukan (NIK) Presiden Republik Indonesia dan beberapa juta data masyarakat Indonesia. Hal ini menjadi sorotan penting ditengah-tengah perancangan Undang-undang Perlindungan Data Pribadi (PDP) [2]. Bahkan sebagian kalangan menyebutkan bahwa potensi kebocoran data terjadi pada aplikasi Peduli Lindungi.

Peduli Lindungi merupakan aplikasi yang diterbitkan resmi oleh Kominfo, Kemenkes, BUMN dan Komite Penanganan Covid-19 dan Pemulihan Ekonomi Nasional. Aplikasi tersebut dapat diunduh secara resmi di *Play Store* bagi pengguna *Android* dan *App Store* bagi pengguna *iOS*. Disatu sisi keberadaannya membantu pemerintah dalam penanganan penyebaran *Covid-19* dan vaksinasi, tetapi disisi lain tingkat kepercayaan masyarakat terkait aplikasi tersebut sangat minim. Mengingat banyak data pribadi yang bocor khususnya identitas pribadi.

Forensik merupakan proses keilmuan yang dapat menjawab pertanyaan berdasarkan fakta-fakta yang ditemukan [3]. *Mobile Forensik* merupakan salah satu cabang *Digital Forensik* dalam menganalisa barang bukti yang berbentuk *mobile*. File aplikasi juga dapat dianalisis dengan berbagai macam metode seperti statis, dinamis serta hibrid untuk dapat

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

diketahui seperti apa proses kerja dari aplikasi *mobile* tersebut dalam memperlakukan data[4]. Dengan adanya keilmuan ini, nantinya dapat digunakan untuk menguji seperti apa aplikasi Peduli Lindungi terhadap kebocoran data pribadi. Apakah memang dari kelalaian pengguna sendiri atau dari aplikasi yang digunakan.

II. TINJAUAN PUSTAKA

2.1. Aplikasi Peduli Lindungi

Peduli Lindungi adalah aplikasi yang dikembangkan untuk membantu instansi pemerintah terkait dalam melakukan pelacakan untuk menghentikan penyebaran *Coronavirus Disease (Covid-19).* Aplikasi ini mengandalkan partisipasi masyarakat untuk saling membagikan data lokasinya saat bepergian agar penelusuran riwayat kontak dengan penderita *Covid-19* dapat dilakukan. Pengguna aplikasi juga akan mendapatkan notifikasi jika berada di keramaian atau berada di zona merah, yaitu area atau kelurahan yang sudah terdata bahwa ada orang yang terinfeksi *Covid-19* positif atau ada Pasien Dalam Pengawasan [5].

2.2. Perolehan dan Pengumpulan Data Aplikasi Peduli Lindungi

Berdasarkan laman pedulilindungi.id, terdapat beberapa kebijakan perolehan dan pengumpulan data pengguna. Data tersebut adalah

1. **Informasi Kebutuhan Registrasi** yang meliputi Nomor Induk Kependudukan (NIK), nama lengkap, tanggal lahir, dan nomor HP
2. **Informasi Data Perangkat** yang meliputi lokasi geografis, waktu dan tempat.
3. **Photo Media dan File** yang meliputi foto galeri.

Pengguna dapat membatalkan *permission*/izin aplikasi Peduli Lindungi kapanpun lewat menu setting di *Smartphone* [5].

2.3. Data Pribadi

Di Negara Indonesia sudah memiliki aturan klasifikasi yang dimaksud dengan data pribadi yang dituangkan dalam undang-undang dan rancangan undang-undang. Adapun masing-masing undang-undang dapat ditunjukkan pada Tabel 1.

Tabel 1. Data Pribadi yang harus dilindungi

Undang-Undang No.23 Tahun 2006 Pasal 84	Undang-Undang No.24 Tahun 2013 Pasal 84	Rancangan Undang-Undang Pelindungan Data Pribadi (PDP) Pasal 3
a) Nomor Kartu Keluarga (KK) **b)** Nomor Induk Kependudukan (NIK) **c)** Tanggal bulan dan tahun lahir **d)** Keterangan tentang kecacatan fisik atau mental **e)** NIK Ibu Kandung **f)** NIK Ayah g) Catatan peristiwa penting	a) Keterangan tentang cacat fisik atau mental b) Sidik jari c) Iris mata d) Tanda tangan e) Elemen data lainnya yang merupakan aib seseorang	Data Pribadi Umum a) Nama lengkap b) Jenis kelamin c) Kewarganegaraan d) Agama Data Pribadi Spesifik a) Data dan informasi kesehatan b) Data biometrik c) Data genetik d) Orientasi seksual e) Pandangan politik f) Catatan kejahatan g) Data anak h) Data keuangan

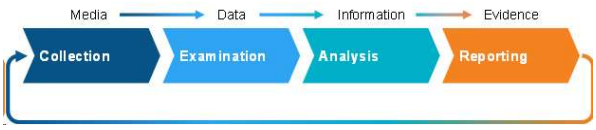
Jika dilihat dari Tabel 1, data pribadi merupakan data-data profil yang melekat pada diri sendiri dan riwayat profil diri. Termasuk didalamnya historis keluarga. Terdapat perbedaan antara Undang-undang kependudukan dan pelindungan data pribadi. Tetapi pada dasarnya data yang harus dilindungi memiliki makna kesamaan.

2.4. Digital Forensic

Digital Forensic merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara ilmiah (*scientific*) hingga didapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut [6][7].

The National Institute of Standards and Technology (NIST) mendefinisikan *Digital Forensic* sebagai "ilmu terapan untuk mengidentifikasi insiden, pengumpulan, pemeriksaan dan analisis bukti digital"[8]. Sebagian peneliti lainnya mendefinisikan *digital forensic* adalah prosedur pemeriksaan sistem komputer untuk mencari bukti yang berpotensi dapat dijadikan alat bukti hukum.

Berdasarkan *The National Institute of Standards and Technology (NIST) Digital Forensic* dapat dijabarkan menjadi 4 (empat) proses, yaitu seperti Gambar 1



Gambar 1. Proses Digital Forensik [9][8]

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

Dari Gambar 1 dapat dijelaskan proses *Digital Forensic* sebagai berikut :

1. ***Collection.*** Tahapan pertama adalah pengumpulan media baik digital maupun elektronik yang berpotensi dapat digunakan sebagai alat bukti
2. ***Examination.*** Melakukan duplikasi, pencarian, dan pemilihan data-data yang diperlukan
3. ***Analysis.*** Melakukan analisis data yang telah diperoleh sehingga memunculkan hasil dari proses forensik
4. ***Reporting.*** Melakukan pelaporan hasil analisis yang siap dipresentasikan atau dipertanggung jawabkan didepan hukum.

2.5. Mobile Forensic

Cabang *Digital Forensic* dengan alat analisis berupa *smartphone* disebut dengan *Mobile Forensic*. Dimana teknik analisanya dibagi menjadi 3 (tiga) macam, yaitu *Manual Acquisition, Physical Acquisition* dan *Logical Acquisition*. *Manual Acquisition* adalah metodologi akuisisi yang paling mudah dimana untuk pengambilan data, langsung bersentuhan dengan perangkat *Smartphone*, membuka data secara langsung untuk mengambil informasi yang dibutuhkan. Teknik ini dapat bekerja di semua jenis ponsel pintar, selama *smartphone* tidak dalam keadaan dikunci. *Logical acquisition* adalah mengambil objek yang berada di partisi logis dari memori *Smartphone*. Jadi, *logical acquisition* tidak mengambil data yang terletak di luar partisi logis, seperti ruang yang tidak terisi. Sebagian besar metode yang ada digunakan dalam *mobile forensic* mengikuti pendekatan *logical acquisition*. *Physical acquisition* adalah cara mendapatkan informasi dengan melakukan duplikat (*copy*) seluruh data dari memori *chip smartphone* ke memori fisik, seperti *SD Card* dan sejenisnya. *Tools* yang sering digunakan adalah *Flasher box* dan *Joint Test Action Group (JTAG)* [10].

III. METODE PENELITIAN

Analisis aplikasi APK Peduli Lindungi tidak terlepas dari proses *Digital Forensic*. Metodologi yang digunakan adalah metode *hybrid analysis*, dimana penggabungan antara analisis statis dan dinamis. Adapun alur analisis dari metode yang digunakan tampak seperti Gambar 2.

Gambar 2. Metode Analisis APK PeduliLindungi

Dari gambar 2 dapat diuraikan alur metode analisis potensi kebocoran data pripadi pada aplikasi PeduliLindungi sebagai berikut :

1. Pengambilan file *xapk* aplikasi PeduliLindungi versi 3.4.6 di *Android Play Store* (Versi terakhir bulan September 2021)
2. Analisis Statis. Dilakukan dengan mengekstrak file **PeduliLindungi_v3.4.6.xapk** sehingga diperoleh hasil *script* program dan kemudian dilakukan analisis. Dari analisis bahasa pemrograman akan diketahui seperti apa bentuk proses data disimpan atau diolah.
3. Analisis Dinamis. Dilakukan dengan menjalankan file **PeduliLindungi_v3.4.6.xapk** dengan model *Sanbox* (dijalankan diruang virtual). Sehingga diketahui proses aplikasi saat berjalan dan melakukan proses yang sebenarnya. Pada tahapan ini akan diketahui apakan ada malware yang sengaja disisipkan dan bekerja ataukah tidak.
4. Hasil analisis potensi kebocoran Data Pribadi. Di tahapan ini akan diperoleh apakah terdapat potensi kebocoran data pribadi pengguna dengan adanya kesengajaan membocorkan dari pihak pembuat aplikasi ataukah tidak.

Kriteria pengukuran potensi kebocoran data pada Aplikasi Peduli Lindungi dilihat dari izin aplikasi, *permission*, adanya *malware*, enkripsi

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

data, data, *file*, dan *database*.

Pada proses analisis secara statis dan dinamis tidak mengikat terkait urutan prosesnya. Pada dasarnya tahap analisis statis dan dinamis dapat dilakukan secara bersamaan. Beberapa *Tools* analisis akan memberikan informasi baik sisi analisis statis maupun analisis dinamis.

IV. HASIL DAN PEMBAHASAN

File aplikasi Peduli Lindungi di download langsung dari *Google Playstore* dengan nama file **PeduliLindungi_v3.4.6.xapk** yang dikeluarkan resmi oleh Kementrian Komunikasi dan Informatika Republik Indonesia. Akan dilakukan analisis dengan metode statis dan dinamis dengan menggunakan *tools Decompiler, Virustotal,* dan *Intezer*

4.1. Decompiler

File **PeduliLindungi_v3.4.6.xapk** memiliki ekstensi sedikit berbeda dengan file apk pada umumnya. Yang menjadi perbedaan terletak pada ekstensi *xapk*. Dimana *xapk* merupakan aplikasi *Android Extra APK*. Didalam *xapk* terdapat banyak file *apk*. Ini dimaksudkan karena *file xapk* memiliki kemampuan *installer* dengan *file* besar.

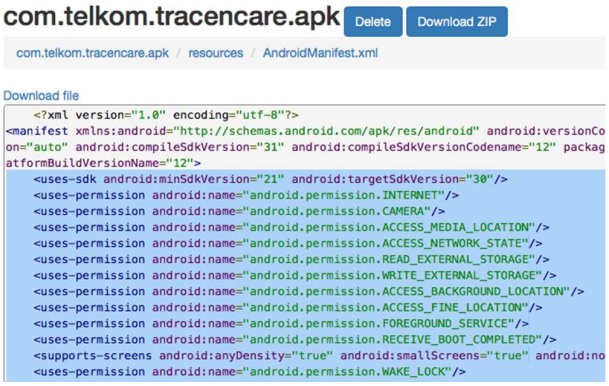
Proses *decompiler* dilakukan untuk mengekstrak isi dari file **PeduliLindungi_v.3.4.6.xapk** sehingga dapat dilihat script yang ada didalamnya. Hasil *decompiler* ditunjukkan pada Gambar 3.

Gambar 3 Hasil Decompiler aplikasi Peduli Lindungi

Hasil analisis dengan cara decompiler menunjukkan hasil bahwa script kode program utama terletak pada **config.arm64_v8a.apk** yang mana berisi konfigurasi aplikasi dengan sistem, dan **com.telkom.tracencare.apk** yang berisi kode program utama dari aplikasi Peduli Lindungi (dapat ditunjukkan pada Gambar 4). Selain keduanya, berisi konfigurasi bahasa *User Interface* aplikasi Peduli Lindungi.

Dari hasil analisis kedua file *apk* tersebut diperoleh hasil bahwa :

a) Terdapat konfigurasi permission untuk perangkat yang diakses oleh aplikasi Peduli Lindungi. Ditunjukkan pada Gambar 4.



Gambar 4. Konfigurasi *Permission*

Dari Gambar 4 terlihat pengaturan hak akses atau *permission* perangkat yang akan diakses oleh aplikasi Android Peduli Lindungi. Penjelasan hak akses (*permission*) ditunjukkan pada Tabel 2

Tabel 2. Hak Akses Aplikasi Peduli Lindungi

Permission (Hak Akses)	Keterangan
INTERNET	Fungsi hak akses yang digunakan untuk mengakses koneksi internet di *Smartphone* android.
CAMERA	Fungsi hak akses yang digunakan untuk mengakses perangkat kamera di *Smartphone* android.
ACCESS_ MEDIA_ LOCATION	Fungsi hak akses yang digunakan untuk mengakses media *Smartphone* android yang meliputi perangkat audio-video. Dikombinasikan dengan perangkat-perangkat yang menggunakan perangkat *audio-video* seperti kamera, *microphone*, speaker, dan lainnya.
ACCESS_ NETWORK_ STATE	Fungsi hak akses untuk dapat menggunakan perangkat jaringan. Sehingga memungkinkan untuk terkoneksi dengan

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

Permission (Hak Akses)	Keterangan
	internet di perangkat *Smartphone* android.
READ_ EXTERNAL_ STORAGE	Fungsi hak akses untuk dapat membaca perangkat penyimpanan eksternal di *Smartphone* android.
WRITE_ EXTERNAL_ STORAGE	Fungsi hak akses untuk dapat menulis data pada perangkat penyimpanan eksternal di *Smartphone* android.
ACCESS_ BACKGROUND_ LOCATION	Fungsi hak akses untuk mengakses perangkat lokasi di *smartphone* android dan menjalankan dalam mode sembunyi
ACCESS_ FINE_ LOCATION	Fungsi hak akses untuk mengakses perangkat lokasi di *smartphone* android
FOREGROUND_ SERVICE	Fungsi hak akses untuk mengatur notifikasi atau pesan yang dikeluarkan oleh aplikasi Peduli Lindungi
RECEIVE_ BOOT_ COMPLETED	Fungsi hak akses untuk mengatur otomatisasi *start service.* Sehingga memungkinkan aplikasi Peduli Lindungi berjalan setelah *smartphone* menyala

Jika dilihat dari Tabel 2 diatas, dapat diketahui bahwa informasi dan data di smartphone dimungkinkan terjadi kebocoran lewat kamera dan akses perangkat penyimpanan.

b) Aplikasi Peduli Lindungi merupakan aplikasi *Front End* yang mengakses server dengan berbasis *Web Service* sehingga tidak memerlukan database dan data yang menetap di perangkat *Smartphone*. Host aplikasi ditunjukkan pada Gambar 5.

c)

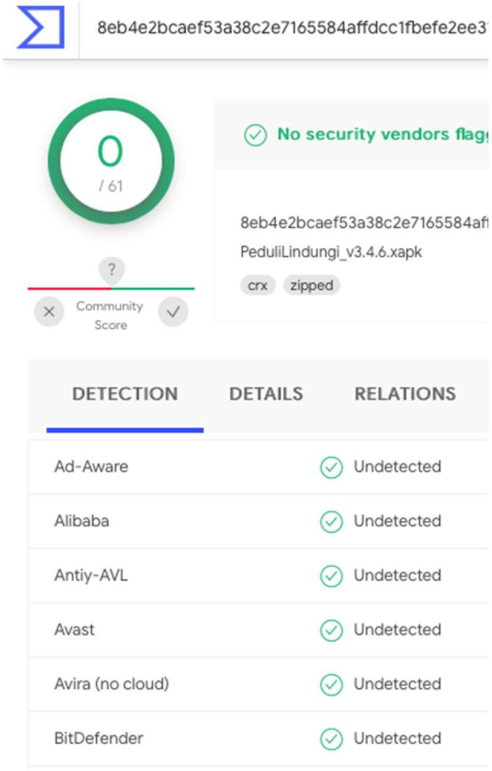
```
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.BROWSABLE"/>
<category android:name="android.intent.category.DEFAULT"/>
<data android:scheme="https" android:host="pdl.id" android:pathPrefix="/c"/>
<data android:scheme="https" android:host="dev.pdl.id" android:pathPrefix="/c"/>
<data android:scheme="https" android:host="stage.pdl.id" android:pathPrefix="/c"/>
```

Gambar 5. Host Peduli Lindungi

Alamat *URL* host yang diberikan adalah **pdl.id, dev.pdl.id dan stage.pdl.id**. Jika diakses, halaman tersebut hanyalah menyediakan service dari perintah yang dikirim. Sehingga merupakan layanan *Application Programming Interface* (*API*).

4.2. Virustotal

Virustotal merupakan salah satu *tools* yang dapat digunakan untuk menganalisa file apakah berpotensi mengandung *malicious* atau tidak. Hasil analisa berdasarkan beberapa referensi Antivirus terkenal. Hasil analisis dengan *Virustotal* tampak pada Gambar 6.

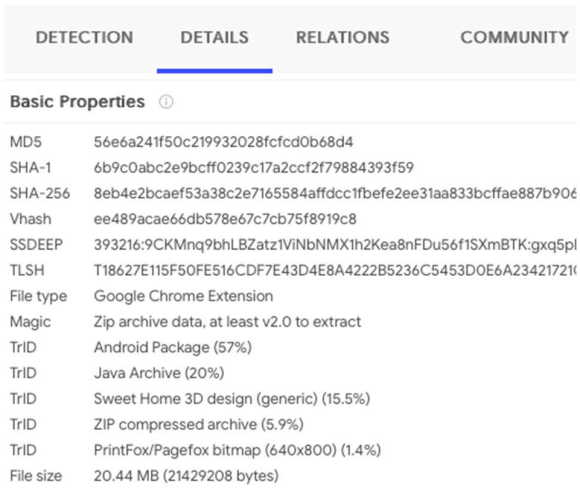


Gambar 6. *Detection of Malicious*

Dari Gambar 6 diperoleh hasil bahwa dari total 61 antivirus yang ada di *Virustotal* tidak satupun antivirus yang mendeteksi adanya potensi *malicious*. Sehingga dipastikan aplikasi Peduli Lindungi tidak berpotensi berisi kode program atau proses-proses berbahaya.

Selain memberikan informasi berupa deteksi keberadaan malicious, *Virustotal* juga memberikan informasi details terkait nilai *hashing, file type, magic extraction, TrID* dan *file size* seperti tampak pada Gambar 7. Nilai-nilai yang tertera menunjukkan karakter, sifat dari *apk* Peduli Lindungi.

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

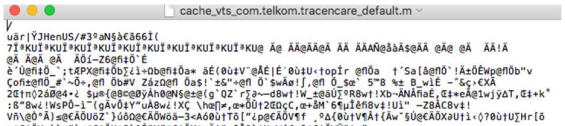


Gambar 7. Details Peduli Lindungi

4.3. Intezer

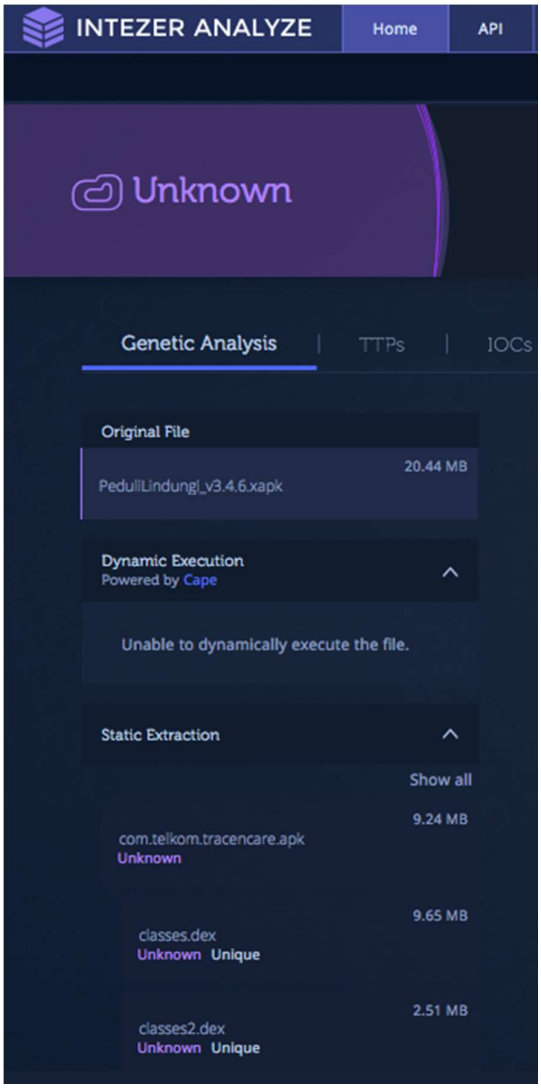
Intezer merupakan salah satu *platform* analisis *file* dari bahaya *malware* yang dapat melakukan analisis secara statis berupa ekstraksi aplikasi dan analisis dinamis berupa menjalankan aplikasi di ruang virtual (*sanbox*). Selain itu juga memiliki fasilitas *sanboxing*, *unpacking*, *malicious tracking*, *runtime protection* dan *memory analysis*.

Pada analisis secara dynamic / live, aplikasi Peduli Lindungi terinstall di dalam **android/data/com.telkom.tracencare**. Dimana didalamnya terdapat cache dari pengoperasian aplikasi Peduli Lindungi. Masing-masing cache memiliki data informasi yang terenkripsi dan tidak memberikan informasi atau data yang jelas. Isi dari *cache* jika dibuka akan tampak pada Gambar 8. Didalam folder **com.telkom.tracencare** tidak ditemukan file database yang tersimpan. Sehingga memang aplikasi Peduli Lindungi didesain hanya untuk menerima informasi dari server.



Gambar 8 *Cache* Peduli Lindungi di android

Untuk analisis *intezer* dilakukan dengan mengupload *XAPK* aplikasi Peduli Lindungi ke **https://analyze.intezer.com** kemudian dilakukan proses analisis. Hasil proses analisis ditunjukkan pada Gambar 9.



Gambar 9. Analisis Statis dan Dinamis dengan *Intezer*

Dari Gambar 9 menunjukkan hasil analisis intezer dengan status *Unknown*. Bahwa file **PeduliLindungi_v.3.4.6.xapk** merupakan kode unik dimana berisi sejumlah besar kode-kode yang belum terdaftar di perangkat lunak berbahaya. Sehingga dapat dikatakan bahwa seluruh isi dari kode program dan aktifitas aplikasi Peduli Lindungi tidak berpotensi mengandung kode dan aktifitas berbahaya.

4.4. Hasil Analisis

Dari hasil analisis yang telah dilakukan secara statis dan dinamis, maka diperoleh hasil seperti Tabel 3 berikut.

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

Tabel 3. Hasil

Kriteria	Keterangan
Izin Aplikasi	Ada dan Legal. Dapat di *download* di *Android Play Store* dan dikeluarkan resmi oleh Kementrian Kominfo
Permission	Terdapat *permission* dan dapat dikonfigurasi oleh pengguna. Diantaranya *permission* untuk akses *Camera, Location, Notification, start service* dan *Storage*
Malicious Software	Tidak Ditemukan baik dalam analisis statis maupun dinamis
Enkripsi Data	Program aplikasi berbasis service sehingga komunikasi jaringan dan data terenkripsi
Data dan *Database*	Seluruh data informasi tidak tersimpan utuh di memori *Smartphone*. Tidak terdapat database yang tersimpan di *Smartphone*. Kecuali pengguna mendownload file (Sertifikat Vaksin)

Jika dilihat dari aktifitas secara langsung oleh pengguna atau diamati pada saat aplikasi dijalankan, terdapat beberapa hasil yaitu :

a) Aplikasi tidak otomatis Keluar/*Logout* jika aplikasi Peduli Lindungi ditutup dari layar. Apabila aplikasi kembali dibuka, akan langsung masuk ke beranda pengguna. Sehingga untuk benar-benar menonaktifkan pengguna, maka harus mengklik menu Keluar/*Logout*
b) Data Pribadi tetap dapat dilihat orang lain apabila pengguna menunjukkan langsung aplikasi Peduli Lindungi atau *Smartphone* jatuh ke orang lain dan aplikasi belum di Keluarkan/*Logout* serta *Smartphone* tanpa kunci pengaman. Selain itu pengunduhan sertifikat vaksin dalam bentuk *file* akan memungkinkan *file* sertifikat jatuh ke orang yang tidak berwenang. Seperti halnya kebiasaan pengguna yang mengupload sertifikat vaksin ke media sosial.
c) Muncul notifikasi **"Selamat! Anda sedang ikut berpartisipasi!"** karena aplikasi Peduli Lindungi memonitoring keberadaan perangkat. Apabila perangkat berpindah lokasi, maka akan muncul notifikasi tersebut.

V. PENUTUP

Dari hasil analisis forensik dengan teknik statis dan dinamis, aplikasi Peduli Lindung tidak berpotensi terjadi kebocoran Data Pribadi. Dibuktikan dengan tidak ditemukannya *malware* dan *database* yang tersimpan. Adanya konfigurasi *permission* secara manual. Aplikasi dikeluarkan oleh lembaga resmi pemerintahan dan aplikasi yang bersifat *service platform*. Kebocoran data pribadi lebih ke pengguna aplikasi itu sendiri. Seperti contohnya meng*upload* sertifikat vaksinasi ke media sosial, menyebarkan Nomor Induk Kependudukan (NIK), menyebarkan fotocopy Kartu Tanda Penduduk (KTP) dan nomor telepon. Minimnya pengetahuan tentang pentingnya melindungi data pribadi dan mudahnya perangkat *Smartphone* diakses oleh orang lain, menjadikan pengguna *Smartphone* kurang waspada terhadap pencurian data. Terlebih aplikasi Peduli Lindungi tidak langsung *Logout*/Keluar ketika aplikasi di tutup.

Identifikasi dan analisis komunikasi jaringan antara aplikasi ke *server* atau sebaliknya dapat dikaji untuk penelitian selanjutnya. Selain itu, analisis *Electronis Health Alert Card (e-HAC)* juga perlu dilakukan analisis, karena aplikasi Peduli Lindungi akan diintegrasikan dengan beberapa layanan umum.

DAFTAR PUSTAKA

[1] H. Wijayanto and I. A. Prabowo, "Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic," *J. SISFOKOM (Sist. Inf. dan Komputer)*, vol. 09, no. November, pp. 395–399, 2020.
[2] C. Indonesia, "NIK Jokowi Bocor, 3 Lembaga Negara Langsung Gerak Cepat," *https://www.cnnindonesia.com/nasional/20210904073135-20-689613/nik-jokowi-bocor-3-lembaga-negara-langsung-gerak-cepat*, 2021. .
[3] G. Gogolin, *Digital forensics explained*. CRC Press, 2021.
[4] H. Wijayanto, A. H. Muhammad, and D. Hariyadi, "Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid," *J. Ilm. SINUS*, vol. 18, no. 1, pp. 1–10, 2020.
[5] Kementerian Komunikasi dan Informatika, "Kebijakan Kerahasiaan PeduliLindungi," *pedulilindungi.id*, 2021. .
[6] M. N. Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.
[7] J. Sachowski, *Implementing Digital*

ISSN Cetak : 2338-4018
ISSN Online : 2620-7532

Forensic Readiness. United State: Elsevier, 2016.

[8] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Sp 800-86. guide to integrating forensic techniques into incident response." National Institute of Standards & Technology, United State of America, 2006.

[9] J. Sachowski, *Digital Forensics and Investigations: People, Processes, and Technologies to Defend the Enterprise*. United State: CRC Press, 2018.

[10] D. Hariyadi *et al.*, "Analisis Barang Bukti Digital Aplikasi Paziim Pada Ponsel Paziim Digital Evidence Analysis Application on Android," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 2, pp. 52–56, 2019.