Jurnal Mobile and Forensics (MF)
Vol. 2, No. 1, Maret 2020, pp. 1-10
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: http://doi.org/10.12928/mf.v2i1.1791

EKSTRAKSI LOGIS FORENSIK MOBILE PADA APLIKASI E-COMMERCE ANDROID

[1]Nuril Anwar, [2]Son Ali Akbar, [3] Ahmad Azhari, [4] Imam Suryanto
[1,3]Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[1]nuril.anwar@tif.uad.ac.id, [2]sonali@ee.uad.ac.id, [3]ahmad.azhari@tif.uad.ac.id, [4]imam.suryanto.is@gmail.com

Abstrak

Pesatnya perkembangan aplikasi android, terutama aplikasi di bidang e-commerce dan transaksi jual beli online yang populer di Indonesia, memaksa pengguna untuk memberikan izin untuk menggunakan fitur dan layanan aplikasi selama pemasangan dan pasca pemasangan. Kurangnya pemahaman pengguna akan resiko dari izin akses yang diminta oleh aplikasi sebelum atau setelah melakukan instalasi menjadikan celah pada keamanan data pengguna untuk mengakses fitur pada perangkat smartphone seperti kamera, media penyimpanan, kontak, akun dan fitur lainnya. *Logical Extraction Method* menjadi metode yang digunakan untuk mendapatkan data aplikasi dengan mengakusisi seluruh data file sistem pada smartphone menggunakan bantuan tools *MOBILedit Forensic*, TWRP (*Team Win Recovery Project*), dan Aplikasi Migrate. Akusisi data dari masing-masing aplikasi akan diambil Android Package File (APK) yang digunakan untuk proses analisis secara statis dengan menggunakan *Tools Forensic* MobSF (*Mobile Security Framework*). Berdasarkan hasil analisis yang dilakukan pada tiga aplikasi teratas e-commerce terdapat 51 izin akses dan dari tiga aplikasi *e-commerce* terpopuler di Indonesia dengan tingkat keamanan paling berbahaya dengan 49 izin akses, 7 izin akses normal dan 1 izin akses tanda tangan. Aplikasi lazada terdapat 21 izin akses berbahaya yang tidak diketahui pengguna sedangkan aplikasi Tokopedia terdapat 4 izin akses berbahaya yang tidak diketahui pengguna dan aplikasi Blibli.com terdapat 1 izin akses berbahaya yang tidak diketahui pengguna. Berdasarkan temuan celah keamanan dapat disimpulkan bahwa aplikasi e-commerce yang digunakan oleh penggunanya memungkinkan pula disisipi sebuah *malware* atau virus sejenis yang berpeluang dalam penggambilan data pribadi penggunanya.

The rapid development of android applications, especially applications in the field of e-commerce and online buying and selling transactions that are popular in Indonesia, force users to give permission to use the features and services of the application during installation and post-installation. Lack of user understanding of the risk of access permissions requested by the application before or after installation creates a gap in the user's data security to access features on smartphone devices such as cameras, storage media, contacts, accounts, and other features. Logical Extraction Method is a method used to obtain application data by acquiring all system file data on smartphones using the help of MOBILedit Forensic tools, TWRP (Team Win Recovery Project), and Migrate Applications. Data acquisition from each application will be taken by Android Package File (APK) which is used for the static analysis process using Tools Forensic MobSF (Mobile Security Framework). Based on the results of an analysis conducted on the top three e-commerce applications there are 51 access permits and of the three most popular e-commerce applications in Indonesia with the most dangerous level of security with 49 access permits, 7 normal access permits, and 1 signature access permit. The Lazada application has 21 dangerous access permits that the user does not know while the Tokopedia application has 4 dangerous access permits that the user does not know and the Blibli.com application has 1 dangerous access permit that the user does not know about. Based on the findings of a security hole, it can be concluded that the e-commerce application used by its users also allows the insertion of a malware or virus that has the opportunity to capture the user's personal data.

Kata Kunci: E-Commerce, Logical Extraction, Mobile Forensic, Permission

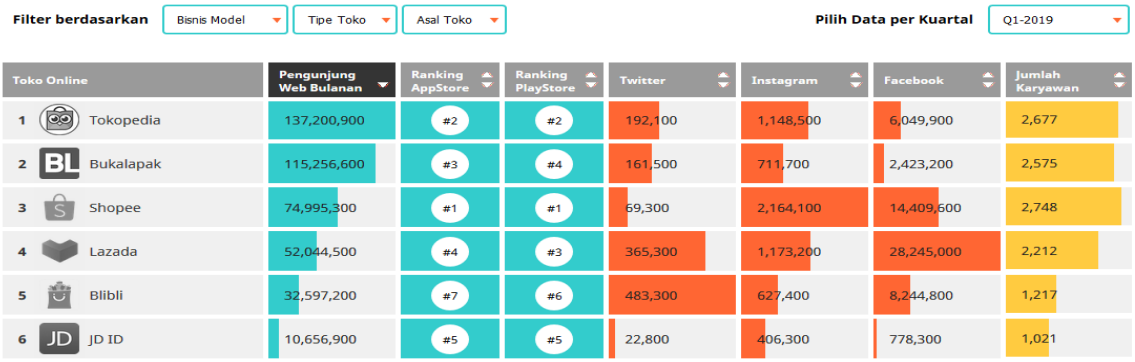
Received Februari 19, 2020; Revised Maret 26, 2020; Accepted Maret 31, 2020

PENDAHULUAN

Teknologi smartphone berbasis android banyak digunakan karena menawarkan banyak layanan, fitur dan aplikasi yang dapat mendukung produktivitas. Android saat ini merupakan platform perangkat seluler pintar yang paling banyak digunakan didunia, menempati 82,8% pangsa pasar [1].

Aplikasi android sering digunakan oleh pengguna untuk melakukan kegiatan yang berbeda, salah satu kategori aplikasi yang mendukung produktivitas sehari-hari adalah aplikasi android E-Commerce atau aplikasi belanja online. Aplikasi android E-Commerce berbasis android merupakan aplikasi yang digunakan untuk melakukan kegiatan, baik belanja maupun transaksi jual beli secara online dengan menggunakan *Smartphone*. Banyak kemudahan yang diberikan serta penggunaan yang tidak memerlukan waktu yang lama, sehingga sangat diminati dan diunduh oleh banyak pengguna. Berbagai macam aplikasi belanja online yang sudah tersedia di pasar aplikasi play store, banyak diunduh dan digunakan dengan berbagai tawaran serta fitur yang berbeda-beda [2].

Aplikasi android E-Commerce berbasis android merupakan aplikasi yang digunakan untuk melakukan kegiatan, baik belanja maupun transaksi jual beli secara online dengan menggunakan Smartphone. Berbagai macam aplikasi belanja online yang sudah tersedia di pasar aplikasi *playstore*, banyak diunduh dan digunakan dengan berbagai tawaran serta fitur yang berbeda-beda. Berdasarkan hasil dari pengamatan *www.iprice.co.id* pada kuartal pertama Tahun 2019 yaitu rata-rata pengunjung website disetiap kuartal, rangking aplikasi, pengikut media sosial dan jumlah karyawan terdapat enam aplikasi E-Commerce yang paling banyak digunakan seperti Gambar 1.



	Toko Online	Pengunjung Web Bulanan	Ranking AppStore	Ranking PlayStore	Twitter	Instagram	Facebook	Jumlah Karyawan
1	Tokopedia	137,200,900	#2	#2	192,100	1,148,500	6,049,900	2,677
2	Bukalapak	115,256,600	#3	#4	161,500	711,700	2,423,200	2,575
3	Shopee	74,995,300	#1	#1	69,300	2,164,100	14,409,600	2,748
4	Lazada	52,044,500	#4	#3	365,300	1,173,200	28,245,000	2,212
5	Blibli	32,597,200	#7	#6	483,300	627,400	8,244,800	1,217
6	JD ID	10,656,900	#5	#5	22,800	406,300	778,300	1,021

Gambar 1. Aplikasi E-Commerce Populer Indonesia

Popularitas dari aplikasi android E-commerce di Indonesia yang banyak diunduh dari *playstore* dapat dimaanfaatkan oleh pihak-pihak yang tidak bertanggung jawab, sehingga celah keamanan dari pasar aplikasi yang tidak memverifikasi keamanan aplikasi yang diterbitkan dapat memunculkan pengembangan *malware*. Aplikasi-aplikasi android E-Commerce yang diunduh dan diinstal, sering meminta izin untuk mengakses berbagai layanan yang ada di *smartphone*. Izin akses yang diberikan seperti kontak, penyimpanan file, kamera bahkan lokasi bisa menjadi ancaman berupa malware yang dapat mengambil informasi dari pengguna aplikasi tersebut.

Perangkat *smartphone* saat ini menjadi sumber penting (digital evidence) yang relevan dengan penggunaan media social dan aplikasi pendukung lain. Forensik mobile sangat diperlukan untuk mengidentifkasi ancaman *malware* dengan mengamati izin akses yang sudah diberikan oleh pengguna. Seiring dengan makin

beragamnya jenis aplikasi yang dikembangkan dan berbagai macam ancaman yang berkembang, semakin banyak pula metode dan *tools* yang bisa dimanfaatkan untuk membantu dalam melakukan forensik mobile [3]. Pengguna tidak memahami sepenuhnya resiko dan tujuan dari izin akses tertentu yang diminta oleh aplikasi sebelum melakukan instalasi maupun sesudah melakukan instalasi [4]. Mobile Phone Forensik merupakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari perangkat mobile dengan metode yang diterima secara umum serta memperhatikan aspek legal. Terlepas dari tujuan akhirnya, seluruh prosedur dan pelaksanaan mobile phone forensics harus dilandaskan metode yang umum diterima oleh ilmu digital forensics [5]. Forensik mobile sangat diperlukan untuk mengidentifkasi ancaman malware dengan mengamati izin akses yang sudah diberikan oleh pengguna. Seiring dengan makin beragamnya jenis aplikasi yang dikembangkan dan berbagai macam ancaman yang berkembang, semakin banyak pula metode dan tools yang bisa dimanfaatkan untuk membantu dalam melakukan forensik mobile. *Logical Extraction Method* adalah metode untuk perangkat mobile yang pada dasarnya mengekstak data yang tersedia dan biasanya sampai mengakses sistem file. Metode ini dapat dijalankan pada perangkat yang tidak di *root* maupun di *root* [6], Namun pada penelitian sebelumnya belum secara spesifik menunjukan kategori aplikasi yang akan diidentifkasi, seperti kategori aplikasi android E-Commerce yang saat ini banyak digunakan oleh pengguna aplikasi *mobile*. Maka akan ditawarkan identifikasi izin akses pada aplikasi android E-Commerce yang sering digunakan di Indonesia agar pengguna lebih cermat dalam memberikan izin akses suatu aplikasi. Penelitian ini akan menerapkan *Logical Extraction Method* sehingga diharapkan aplikasi android E-Commerce dapat diidentifikasi izin akses aplikasi yang diberikan serta menentukan aplikasi E-Commerce yang aman digunakan.

LANDASAN TEORI

Penelitian Terdahulu

Pada penelitian [4], Aplikasi android menjadi target utama aplikasi berbahaya seperti malware, salah satu cara dengan melalui ijin akses aplikasi untuk menjalankan fasilitas aplikasi. Ijin akses aplikasi yang diminta merupakan gambaran dari pola perilaku dari aplikasi, maka dari itu pengguna harus memahami pola dari ijin akses aplikasi. Pada penelitian tersebut mengeksplorasi resiko dari ijin akses pada tiga tingkatan secara sistematis, dengan menganalisis kategori perijinan secara kolaboratif. Dengan mengguanakan tiga metode yaitu *mutual Information, Correlation Coefficient (CorrCoef) and T-Test* untuk menentukan peringkat ijin setiap aplikasi. Kemudian menggunakan *Sequential Forward Selection* (SFS) serta *Principal Component Analysis* (PCA) untuk mengidentifkasi subsets ijin yang beresiko. Mengevaluasi penggunaan ijin yang beresiko untuk mendeteksi *malware* dengan menggunakan *Support Vector Machine* (SVM), *Decission trees* serta *Random Forrest*. Kemudian secara mendalam menganalisis hasil deteksi, kelayakan, serta keterbatasan untuk mendeteksi aplikasi berbahaya dari ijin aplikasi. Berdasarkan hasil evaluasi dengan menggunakan metode tersebut dalam skala besar, terdapat 310.926 aplikasi jinak dan 4868 aplikasi berbahaya serta dari aplikasi pihak ketiga.

Pada penelitian selanjutnya menggunakan metode yang disebut PAMD (*Permission Analysis for Android Malware Detection*), dengan cara menganalisis file manifest dari android untuk memahami tingkat perlindungan izin akses dan menyelidiki karakteristik yang berbahaya. Dalam metode penelitian ini dapat mengklasifikasi dua jenis mekanisme analisi, yaitu analisis dinamis dan analisis statis.

Dalam metode dinamis, program diuji kembali dan dievaluasi dengan menjalankan data secara langsung dengan tujuan menemukan kesalahan dalam program yang sedang berjalan untuk menghindari pemeriksaan secara berulang kali. Sedangkan dalam analisis statis, *source code* program diperiksa secara langsung sebelum dijalankan untuk mengamati file *manifest* yang berisi *malware* atau tidak. Dalam penelitian tersebut mengusulkan sebuah metode untuk menampilkan nilai dari keamanan aplikasi berdasarkan tingkat perlidungan hak akses kemudian menggunakan pohon keputusan untuk memutuskan aplikasi berisi atau aplikasi aman. Metode untuk mendeteksi malware pada aplikasi android yaitu dengan mengusulkan metode analisis statis sebagai langkah utama mengidentifkasi izin akses berbahaya yang ada pada file *manifest* android. Dari hasil analisis statis maka didapat hasil daftar malwords yang sering muncul sebagai daftar string berbahaya dengan tingkat resiko masing-masing, setelah mendapatkan daftar *malwords* kemudian menghitung skor dari izin akses dengan menggunakan persamaan yang sudah ditentukan. Data yang diperoleh akan diproses dengan menggunakan machine learning untuk menentukan aplikasi berbahaya, klasifikasi *decision tree* merupakan klasifikasi umum, intuitif dan cepat karena pada dasarnya adalah algoritma greedy. Dari penelitian tersebut telah bekerja secara efektif dengan biaya yang cukup rendah, dengan menggunakan metode machine learning diharapkan dapat menangani kasus malware lain [7].

Pada penelitian [8] perangkat android yang dalam kondisi *unroot* digunakan, metode ekstraksi logikal untuk mendapatkan data pada perangkat menggunakan beberapa teknik seperti AFLogical, SDcard Imaging, Android Backup Analysis dan aplikasi lain untuk forensik seperti Oxygen-Forensic. Pada perangkat android unroot memiliki masalah dalam memilih teknik akuisisi yang tepat untuk mendapatkan bukti digital. Pada penelitian tersebut menggunakan aplikasi *Steam* sebagai studi kasus, untuk dianalisis dan mendapatkan bukti digital dengan menggunakan beberapa teknik akuisisi. Pada teknik AFLogical hanya mendapatkan data dari perangkat sistem yang memiliki hak akses istimewa seperti perangkat dalam keadaan root, sedangkan dalam penelitian ini mencari teknik yang bias digunakan pada perangkat dalam kondisi *unroot*. Teknik SDcard Imaging mendapatkan data dari yang tersimpan pada memori eksternal namun tidak dapat mendapatkan data yang disimpan dari perangkat internal. Kemudian *Android Backup Analysis* merupakan teknik terbaik yang digunakan pada perangkat *unroot* karena menganalisis dan menggunakan data dari hasil pencadangan perangkat tanpa merusak integritas bukti itu sendiri, selain itu teknik terbaik untuk aspek kuantiitatif dan aspek kualitatif yang dapat menangkap *log* komunikasi serta informasi dari studi kasus yang diberikan.

Pada penelitian [9] mengusulkan analisis forensik secara otomatis dengan menggunakan *Fordroid*. *Fordroid* melakukan analisis antar komponen pada aplikasi android, kemudian mengidentifikasi lokasi informasi yang terdapat pada penyimpanan lokal dengan taint analysis. Selain itu *Fordroid* menganalisis struktur table dari database dengan perintah SQL yang diekstrak dari aplikasi, untuk mendapatkan log informasi dari aktifitas aplikasi. *Fordroid* menganalisis 100 aplikasi dari berbagai kategori dengan waktu sekitar 64 jam, maka dibutuhkan waktu sekitar 38 menit setiap aplikasi yang terdiri dari 2841 komponen. Sekitar 469 jalur ditemukan pada 36 aplikasi yang menulis informasi sensitif pada penyimpanan lokal,selain itu menemukan lokasi informasi yang ditulis dalam 458 jalur (98%) dan mengidentifikasi semua struktur table database (22). Lebih dari setengah sekitar 56% aplikasi membocorkan informasi sensitif dan lebih dari sepertiga sekitar 36% aplikasi menulis informasi sensitif pada penyimpanan lokal.

Penelitian [10] menunjukkan fitur aplikasi pesan instan mana yang meninggalkan jejak pembuktian yang memungkinkan data tersangka direkonstruksi sebagian, dan apakah forensik jaringan atau forensik perangkat memungkinkan dilakukannya rekonstruksi aktivitas tersebut. Peneliti menunjukkan bahwa dalam banyak kasus dapat merekonstruksi data seperti: kata sandi, *screenshot* yang diambil oleh aplikasi, gambar, video, audio yang dikirim, pesan yang dikirim, sketsa, gambar profil dan lain-lain

Forensik Digital dan Mobile Forensics

Bidang ilmu yang mempelajari tentang penyelidikan dan pemulihan data untuk mendapatkan barang bukti digital sebagai alat bukti di pengadilan yang diperoleh dari investigasi dan analisis data digital computer, telepon seluler, CDR dari operator dan SIM card [5].

Mobile Phone Forensics merupakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari perangkat *mobile* dengan metode yang diterima secara umum serta memperhatikan aspek legal. *Mobile Forensics* sendiri tidak hanya bertujuan untuk pemenuhan kebutuhan bukti digital dipengadilan(proses litigasi), namun dapat juga digunakan untuk proses non-litigasi. Terlepas dari tujuan akhirnya, seluruh prosedur dan pelaksanaan *mobile phone forensics* harus dilandaskan metode yang umum diterima oleh ilmu digital forensics (*forensically sounds*) [5].

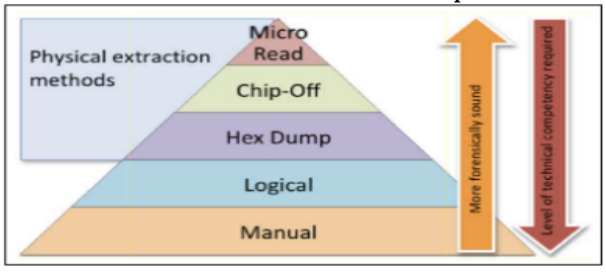
Aplikasi yang dirancang khusus untuk platform mobile seperti iOS, android, atau windows mobile. Aplikasi mobile memilki user interface dengan interaksi unik yang disediakan oleh *platform mobile*, dengan sumber daya berbasis web yang menyediakan berbagai informasi yang relevan dengan aplikasi. Selain itu memiliki kemampuan analisis dan pengumpulan informasi yang paling tepat untuk *platform mobile*, menyediakan kemampuan penyimpanan *persistent* dalam *platform* [11].

***Malicious Software* (Malware)**

Malicious Software merupakan sebuah program atau aplikasi yang dirancang dengan tujuan untuk menyusup dan merusak sebuah sistem, selain itu malware dapat mengambil informasi data melalui jaringan dan program yang sudah terinfeksi [12].

Logical Extraction Method

Logical Extraction Method adalah metode untuk perangkat *mobile* yang pada dasarnya mengekstrak data yang tersedia dan biasanya sampai mengakses file sistem. Metode ini dapat dijalankan pada perangkat yang tidak di *root* maupun di *root*. *Physical Extraction Method* merupakan metode ekstraksi untuk mendapatkan data pada *Chip Memori* perangkat dari data-data yang sudah terhapus pada perangkat yang sudah mati dan *Manual Extraction Method* adalah metode ekstraksi secara langsung pada perangkat untuk mendapatkan data pada perangkat yang sedang digunakan [6], dapat dilihat pada piramida metode ekstraski forensik pada Gambar 2.



Gambar 2. Piramida Metode Ekstraksi Forensik

Lima metode ektraksi dari perangkat mobile seperti terlihat pada Gambar 2. Piramida metode ekstraksi forensik, metode ekstraksi manual sangat sederhana dan hampir semua perangkat dapat dianalisis. Metode ekstraksi logikal adalah metode yang paling direkomendasikan untuk ekstraksi data, metode ini merupakan cara cepat untuk ekstraksi tanpa keahlian yang tinggi dengan sifat berulang untuk mengurangi kesalahan perubahan data ketika proses pengkopian di perangkat ponsel. Tiga lapisan berikutnya merupakan metode ekstraksi fisik yang membutuhkan tingkat kompetensi teknik yang lebih tinggi seperti Hex Dump melibatkan proses mengupload dan mengganti boot loader ke perangkat dan melakukan proses booting. Lapisan berikutnya adalah Chip off dan teknik melepas chip flash NAND fisik dan diperiksa secara eksternal bila perangkat dalam keadaan rusak. Lapisan terakhir mikro read yang membutuhkan keahlian paling teknis dengan menggunakan mikroskop elektron untuk melihat keadaan memori pada perangkat dan membutuhkan biaya yang besar [8].

Tahapan Penelitian

Penelitian ini mengambil objek dari pengguna aplikasi mobile E-Commerce platform android, level yang digunakan dalam penelitian ini adalah level Makro karena mencakup masyarakat sebagai pengguna dan komunitas luas. Penelitian ini dilakukan menggunakan fasilitas laboraturium Riset kampus III Universitas Ahmad Dahlan.

Pada penelitian ini terdapat tahapan serangkaian penelitan yang digunakan untuk mendapatkan data dari digital evidence dalam proses penanganan investigasi forensik Aplikasi E-Commerce, proses investigasi forensik mobile dapat mengacu susuai yang dibuat oleh National Institute of Standard and Technology (NIST) yang mempunyai beberapa tahap yaitu: Preservation, Acquisition, Examination & Analysis, dan Reporting [13], untuk selanjutnya hasil ektraksi data digital akan dilakukan identifikasi aplikasi E-Commerce yang seperti tampak pada tahapan penelitian yang terdapat pada Gambar 3.

Gambar 3. Tahapan Penelitian

Penelitian ini menggunakan *Logical Extraction Method* untuk mendapatkan data aplikasi e-commerce pada *Smartphone* yang masih digunakan. Analisis dan identifikasi serta pencarian data aplikasi e-commerce selanjutnya dilakukan analisis dengan menggunakan Tools Forensics.

HASIL DAN PEMBAHASAN

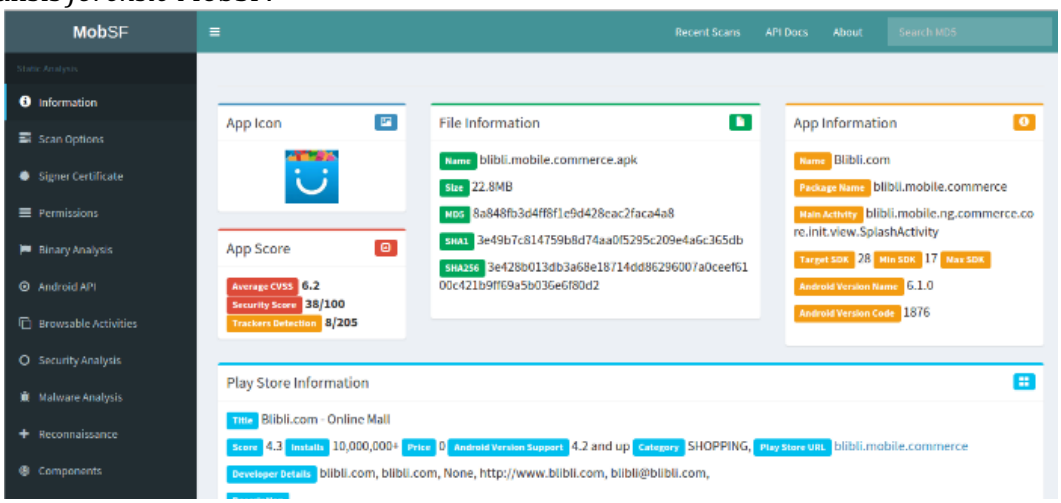
Tahap identifikasi dilakukan untuk memperoleh hasil analisis *Permission* pada aplikasi *e-commerce* yang digunakan dengan aplikasi, hasil ektraksi selanjutnya akan di analisis secara *Static* dengan menggunakan *Tools Forensic* MOBSF *(Mobile Security Framework)*. Analisis dilakukan pada kategori aplikasi android *E-Commerce* terpopuler di Indonesia berdasarkan hasil dari pengamatan www.iprice.co.id pada kuartal pertama tahun 2019 yaitu rata-rata pengunjung website di setiap kuartal, rangking aplikasi, pengikut media sosial dan jumlah karyawan terdapat enam aplikasi *E-Commerce* yang paling banyak digunakan.

Tahapan ekstraksi dilakukan dengan tiga cara ekstraksi yang berbeda dan dari tiga cara ekstraksi akan digunakan salah satu cara ekstraksi yang paling direkomendasikan untuk tahap analisis. Tabel 2 merupakan hasil ektraksi dari tiga cara ekstraksi dan hasil yang didapat setelah melakukan ekstraksi.

Tabel 2. Hasil Ekstraksi

Hasil didapat	MOBILedit Forensic	TWRP	Aplikasi Migrate
Hasil ekstraksi	blibli.mobile.commerce-WRUN2LKtnuUzm4JG... com.lazada.android-hdGlWVxVimkLj2Ky8lRxcg... com.tokopedia.tkpd-KWvBgLmSYSM6p2o70xE... id.co.elevenia-DzlYtoLSizEq81HhSRPgAQ==	data.ext4.win000 data.ext4.win000.sha2 data.ext4.win001 data.ext4.win001.sha2	Backup_2019.07.09_17.50.17 WinRAR ZIP archive 346 MB
Isi data ekstraksi	lib oat base.apk	data.ext4 data2.ext4	com.lazada.android.apk

Aplikasi dari hasil ektraksi ber-ekstensi APK (*Android Package File*) dari setiap aplikasi yang akan digunakan untuk dianalisis secara statis dengan menggunakan *Forensic MobSF* (*Mobile Security Framework*). MobSF digunakan dalam penelitian ini untuk melakukan analisis secara statis agar dapat mengamati perilaku Permission dalam sebuah aplikasi, kemudian dibandingkan dengan daftar Permission yang pengguna ketahui sebelumnya. Analisis statis dilakukan untuk mengamati sebuah aplikasi tanpa menjalankan aplikasi tersebut. Gambar 4 merupakan interface dari hasil analisis *forensic* MobSF.



Gambar 4. Interface hasil analisis MobSF

Laporan hasil analisis menunjukan dari tiga aplikasi E-Commerce terpopuler Indonesia masih terdapat izin akses yang tidak sesuai dengan yang pengguna ketahui, serta tingkat keamanan izin akses yang terdapat banyak berbahaya. Berdasarkan hasil anaisis dari tiga aplikasi E-Commerce terdapat total 51 izin akses pada masing-masing aplikasi terdapat 43 izin akses berbahaya, 7 izin akses normal dan 1 izin akses tanda tangan. Tidak berarti bahwa penyerang keamanan tidak dapat memanfaatkan hak akses normal, untuk itu pengguna diharapkan lebih cermat dalam menggunakan izin akses aplikasi serta meningkatkan kesadaran keamanan dari penggunaan aplikasi android. Gambar 5 merupakan hasil analisis aplikasi e-commerce.

Lazada	BlibBli.com	Tokopedia
Izin akses	Izin akses	Izin akses
-ACCESS_COARSE_LOCATION	-ACCESS_COARSE_LOCATION	-ACCESS_COARSE_LOCATION
-ACCESS_FINE_LOCATION	-ACCESS_FINE_LOCATION	-ACCESS_FINE_LOCATION
-ACCESS_LOCATION_EXTRA_COMMANDS	-ACCESS_WIFI_STATE	-ACCESS_WIFI_STATE
-ACCESS_WIFI_STATE	-BLUETOOTH	-CALL_PHONE
-BLUETOOTH	-BLUETOOTH_ADMIN	-CAMERA
-BLUETOOTH_ADMIN	-CALL_PHONE	-CHANGE_WIFI_STATE
-CAMERA	-CAMERA	-GET_ACCOUNTS
-CHANGE_WIFI_STATE	-CHANGE_WIFI_STATE	-INTERNET
-GET_TASKS	-FOREGROUND_SERVICE	-READ_CONTACTS
-INTERNET	-GET_ACCOUNTS	-READ_EXTERNAL_STORAGE
-READ_CALENDAR	-INTERNET	-READ_PHONE_STATE
-READ_CONTACTS	-READ_CONTACTS	-RECORD_AUDIO
-READ_APP_BADGE	-READ_EXTERNAL_STORAGE	-USE_FINGERPRINT
-READ_EXTERNAL_STORAGE	-READ_PHONE_STATE	-SYSTEM_ALERT_WINDOW
-READ_PHONE_STATE	-RECEIVE_BOOT_COMPLETED	-VIBRATE
-RECEIVE_BOOT_COMPLETED	-RECORD_AUDIO	-NFC
-RECORD_AUDIO	-USE_FINGERPRINT	-WAKE_LOCK
-SYSTEM_ALERT_WINDOW	-VIBRATE	-WRITE_EXTERNAL_STORAGE
-VIBRATE	-WAKE_LOCK	-USE_CREDENTIALS
-READ_SETTINGS	-WRITE_EXTERNAL_STORAGE	-c2dm.permission.RECEIVE
-FLASHLIGHT	-c2dm.permission.RECEIVE	-finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
-WAKE_LOCK	-finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	-providers.gsf.permission.READ_GSERVICES
-WRITE_EXTERNAL_STORAGE	blibli.mobile.commerce.permission.C2D_MESSAGE	-tokopedia.tkpd.permission.C2D_MESSAGE
-WRITE_CALENDAR		
-WRITE_SETTINGS		
-WRITE_MEDIA_STORAGE		
-c2dm.permission.RECEIVE		
-htc.launcher.permission.READ_SETTINGS		
-htc.launcher.permission.UPDATE_SHORTCUT		
-sonyericsson.home.permission.BROADCAST_BADGE		
-huawei.android.launcher.permission.CHANGE_BADGE		
-huawei.android.launcher.permission.READ_SETTINGS		
-huawei.android.launcher.permission.WRITE_SETTINGS		
-oppo.launcher.permission.READ_SETTINGS		
-oppo.launcher.permission.WRITE_SETTINGS		
-finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE		
-lazada.-C2D_MESSAGE		
-anddoes.launcher.permission.UPDATE_COUNT		
-sec.android.provider.badge.permission.READ		
-sec.android.provider.badge.permission.WRITE		
-sonymobile.home.permission.PROVIDER_INSERT_BADGE		
-majeur.launcher.permission.UPDATE_BADGE		
-lazada.-MIPUSH_RECEIVE		

Gambar 5. Hasil analisis tiga *e-commerce*

Pada Gambar 5, hasil analisis terdapat izin akses dari hasil analisis masing-masing APK, menunjukan bahwa izin akses yang terdapat pada masing-masing aplikasi. Izin akses hasil analisis dbandingkan dengan izin akses yang terdapat pada aplikasi sesuai dengan yang pengguna ketahui sebelumnya. Gambar 6 merupakan hasil perbandingan serta tingkat keamanan dari masing-masing izin akses.

Lazada		BlibBli.com		Tokopedia	
Izin akses	Tingkat keamanan	Izin akses	Tingkat keamanan	Izin akses	Tingkat keamanan
anddoes.launcher.permission.UPDATE_COUNT	Berbahaya	blibli.mobile.commerce.permission.C2D_MESSAG	Tanda tangan	USE_CREDENTIALS	Berbahaya
c2dm.permission.RECEIVE	Berbahaya	c2dm.permission.RECEIVE	Berbahaya	SYSTEM_ALERT_WINDOW	Berbahaya
FLASHLIGHT	Normal	FOREGROUND_SERVICE	Normal	com.tokopedia.tkpd.permission.C2D_MESSAG	Tanda tangan
htc.launcher.permission.READ_SETTINGS	Berbahaya			c2dm.permission.RECEIVE	Berbahaya
htc.launcher.permission.UPDATE_SHORTCUT	Berbahaya			providers.gsf.permission.READ_GSERVICES	Berbahaya
huawei.android.launcher.permission.CHANGE_BADGE	Berbahaya				
huawei.android.launcher.permission.READ_SETTINGS	Berbahaya				
huawei.android.launcher.permission.WRITE_SETTINGS	Berbahaya				
lazada.C2D_MESSAGE	Tanda tangan				
lazada.MIPUSH_RECEIVE	Berbahaya				
majeur.launcher.permission.UPDATE_BADGE	Berbahaya				
oppo.launcher.permission.READ_SETTINGS	Berbahaya				
oppo.launcher.permission.WRITE_SETTINGS	Berbahaya				
READ_SETTINGS	Berbahaya				
sec.android.provider.badge.permission.READ	Berbahaya				
sec.android.provider.badge.permission.WRITE	Berbahaya				
sonyericsson.home.permission.BROADCAST_BADGE	Berbahaya				
sonymobile.home.permission.PROVIDER_INSERT_BADG	Berbahaya				
SYSTEM_ALERT_WINDOW	Berbahaya				
WRITE_MEDIA_STORAGE	Berbahaya				
WRITE_SETTINGS	Berbahaya				

Gambar 6. Hasil Perbandingan Izin Akses

Pada Gambar 6, Hasil perbandingan izin akses dapat dilihat beberapa izin akses yang tidak sesuai dengan pengguna ketahui sebelumnya, izin akses tersebut memiliki tingkat keamanan masing-masing seperti berbahaya, normal dan signature.

Dari hasil analisis tiga aplikasi terdapat jumlah tingkat keamanan izin akses yang tidak diketahui pengguna seperti pada Tabel 3 [14].

Tabel 3. Jumlah Tingkat Keamanan Izin Akses

Tingkat Perlindungan	Lazada	BliBli.com	Tokopedia
Normal	1 izin akses	1 izin akses	-
Berbahaya	19 izin akses	1 izin akses	4 izin akses
Tanda tangan	1 izin akses	1 izin akses	1 izin akses

Pada Tabel 3. Jumlah tingkat keamanan izin akses terdapat hasil analisis izin akses yang tidak diketahui pengguna dari 3 aplikasi populer Indonesia yaitu aplikasi Lazada memiliki tingkat resiko izin akses yang tidak diketahui pengguna paling

berbahaya sebanyak 19 izin akses, kemudian aplikasi Tokopedia terdapat 4 izin akses berbahaya yang tidak diketahui pengguna dan aplikasi BliBli.com terdapat 1 izin akses berbahaya yang tidak diketahui oleh pengguna. Pengguna diharapkan dapat menggunakan izin akses yang terdapat pada aplikasi sesuai kebutuhan fitur yang sedang digunakan, agar izin akses tidak selalu terbuka untuk menghindari aplikasi mengakses perangkat Smartphone.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dapat diperoleh kesimpulan Ada 51 izin akses dari hasil analisis 3 aplikasi E-Commerce, beberapa izin akses hasil analisis berbeda dengan izin akses dari pengguna ketahui dengan tingkat perlindungan izin akses terdapat 43 izin akses berbahaya, 7 izin akses normal dan 1 izin akses tanda tangan. Dari 3 aplikasi E-Commerce populer Indonesia, aplikasi Lazada terdapat 21 izin akses berbahaya yang tidak diketahui pengguna sedangkan aplikasi Tokopedia terdapat 4 izin akses berbahaya yang tidak diketahui pengguna dan aplikasi BliBli.com terdapat 1 izin akses berbahaya yang tidak diketahui pengguna. Berdasarkan temuan celah keamanan dapat disimpulkan bahwa aplikasi e-commerce yang digunakan oleh penggunanya memungkinkan pula disisipi sebuah malware atau virus sejenis yang berpeluang dalam penggambilan data pribadi penggunanya

UCAPAN TERIMA KASIH

Ucapan terimakasih kepada pihak yang terlibat dalam penelitian ini; Lembaga Pengabdian dan Penelitian Universitas Ahmad Dahlan LPPM UAD yang telah membiayai penelitian ini Penelitian ini, Laboratorium Riset Kampus III Universitas Ahmad Dahlan serta semua pihak yang membantu terselesaikannya penelitian ini.

DAFTAR PUSTAKA

[1] N. Viet Duc, P. Thanh Giang, and P. Minh Vi, “Permission Analysis for Android Malware,” no. February 2012, pp. 207–216, 2017.

[2] H. Dong, N. Q. He, G. Hu, Q. Li, and M. Zhang, “Malware detection method of android application based on simplification instructions,” *J. China Univ. Posts Telecommun.*, vol. 21, no. SUPPL. 1, pp. 94–100, 2014.

[3] S. H. Mohtasebi and A. Dehghantanha, “Towards a Unified Forensic Investigation Framework of Smartphones,” *Int. J. Comput. Theory Eng.*, vol. 5, no. 2, pp. 351–355, 2013.

[4] W. Wang, X. Wang, D. Feng, J. Liu, Z. Han, and X. Zhang, “Exploring Permission-Induced Risk in Android Applications for Malicious Application Detection,” vol. 9, no. 11, pp. 1869–1882, 2014.

[5] A. P. Heriyanto, *Mobile Phone Forensics: Theory: Mobile Phone Forensics dan Security Series*. Yogyakarta: Perpustakaan Nasional, 2016.

[6] R. Tammaics and D. Tindall, “Learning Android Forensics,” 2015.

[7] N. V. Duc, P. T. Giang, and P. M. Vi, “Permission Analysis for Android Malware,” *Proc. 7th VAST - AIST Work. “RESEARCH Collab. Rev. Perspect.*, no. November 2015, pp. 207–216, 2016.

[8] N. Y. P. Lukito, F. A. Yulianto, and E. Jadied, “Comparison of data acquisition technique using logical extraction method on Unrooted Android Device,” *2016 4th Int. Conf. Inf. Commun. Technol. ICoICT 2016*, vol. 4, no. c, 2016.

[9] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, “Automated forensic analysis of

mobile applications on android devices," *Proc. Digit. Forensic Res. Conf. DFRWS 2018 USA*, vol. 26, pp. S59–S66, 2018.

[10] D. Walnycky *et al.*, "Network and device forensic analysis of Android social-messaging applications," 2015.

[11] C. L. Liu, N. T. Hua, and A. B. Tucker, *Software Engineering A Practitioner's Approach*. .

[12] M. Howard, A. Pfeffer, M. Dalai, and M. Reposa, "Predicting signatures of future malware variants," *Proc. 2017 12th Int. Conf. Malicious Unwanted Software, MALWARE 2017*, vol. 2018-January, pp. 126–132, 2018.

[13] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.

[14] "<permission> | Android Developers." [Online]. Available: https://developer.android.com/guide/topics/manifest/permission-element. [Accessed: 22-Apr-2020].