EasyChair Preprint

№ 3937

Security Analysis of First and Third Party Applications Using File Backup

Aldito Rama Dana, Rhendy Oentoko and Nurhalis Jusman

July 23, 2020

Analisis Keamanan Aplikasi Pihak Pertama dan Ketiga Menggunakan File Backup

Aldito Rama Dana[1], Nurhalis Jusman[2], Rhendy Oentoko[3]

[1] Fakultas Ilmu Komputer, Teknik Komputer, Universitas Amikom Yogyakarta

e-mail: [1] aldito.1999@students.amikom.ac.id, [2] nurhalis.jusman@students.amikom.ac.id, [3] rhendy.0102@students.amikom.ac.id

Abstrak

Forensik pada perangkat seluler bukanlah hal baru. Banyak akademisi atau badan hukum telah melakukan forensik pada perangkat seluler dengan tujuan tertentu. Aplikasi pihak pertama dan ketiga didukung pada perangkat seluler, karena aplikasi pihak ketiga memiliki banyak dan beragam fungsi dan dapat diinstal pada perangkat seluler. Aplikasi pihak ketiga dapat ditemukan di toko-toko penyedia aplikasi pihak ketiga, misalnya, Appstore dan Play Store yang paling terkenal. Sedangkan untuk aplikasi pihak pertama sudah otomatis terinstal pada perangkat seluler sesuai dengan produsennya. Aplikasi pihak pertama dan ketiga dapat dilakukan untuk analisis forensik karena aplikasi menyimpan informasi tentang perangkat seluler yang digunakan. termasuk informasi tentang pengguna yang berguna untuk penyelidikan. tujuan utama analisis forensik perangkat seluler adalah untuk mengetahui apakah penggunaan aplikasi pihak ketiga meninggalkan data dalam penyimpanan internal perangkat seluler. Pada paper ini menganalisis aplikasi pihak ketiga yang terinstal dalam perangkat seluler dengan memanfaatkan file backup dari perangkat seluler melalui aplikasi iTunes dan 3uTools untuk melakukan analisis informasi atau data yang tersimpan.

Kata Kunci: Aplikasi pihak pertama, Aplikasi Pihak Ketiga, Forensik, perangkat seluler, forensik digital

Abstract

Forensics on mobile devices is not new. Many academics or legal entities have conducted forensics on mobile devices with specific objectives. First and third party applications are supported on mobile devices, because third party applications have many and varied functions and can be installed on mobile devices. Third-party applications can be found in stores that provide third-party applications, for example, the most famous Appstore and Play Store. Whereas the first party application is automatically installed on the mobile device according to the manufacturer. First and third party applications can be done for forensic analysis because the application stores information about the mobile device used. including information about users useful for investigations. the main purpose of a mobile device forensic analysis is to find out whether third-party application usage leaves data in the internal storage of a mobile device. This paper analyzes third-party applications installed on mobile devices by utilizing backup files from mobile devices through the iTunes and 3uTools applications to analyze the information or data stored.

Keywords: First party applications, Third Party Applications, Forensics, mobile devices, digital forensics

1. PENDAHULUAN

Pada masa sekarang ini, perangkat seluler semakin dikenal dan semakin familier di kalangan masyarakat. Dan perangkat seluler memiliki peran penting dalam berbagai bidang antara lain seperti jejaring sosial, hiburan, email, dan *e-commerce*. Ini tidak lepas dari peran toko aplikasi seperti contohnya *App Store* dan *Play Store* yang membawakan atau menyediakan aplikasi pihak ketiga untuk perangkat seluler yang menjadikan perangkat seluler lebih memiliki fungsi yang luas dengan aplikasi pihak ketiga.Toko aplikasi juga menyediakan mekanisme bagi pengembang untuk mengiklankan, menjual dan mendistribusikan aplikasi dari pengembang[1].

Forensik digital khususnya pada perangkat seluler pada zaman ini semakin mendapat sorotan di seluruh kalangan, karena mengingat jumal pengguna perangkat seluler sekarang ini sudah melebihi pengguna *personal computer* untuk mempermudah kegiatan sehari-hari. *platform* seluler lebih banyak digunakan kerana memiliki tingkat ke efektifitas yang baik, aplikasi pihak ketiga juga semakin banyak berkembang dan beraneka ragam sesuai dengan fungsinya. Sebenarnya belum ada alat yang di jual bebas atau komersial untuk menganalisis secara forensik digital pada perangkat seluler khususnya pada aplikasi pihak ketiga[1]

Dasarnya, aplikasi pihak pertama menyediakan fitur yang dasar dari setiap perangkat seluler atau bisa disebut juga dengan fitur wajib dan basic untuk perangkat seluler maka dari itu dengan adanya aplikasi pihak ketiga atau *Third-Party Application* semakin banyak juga fungsi dari perangkat seluler. *Market* atau tempat untuk mengunduh aplikasi tersebut atau penyedia aplikasi pihak ketiga kemungkinan membuat untung bagi pengembang aplikasi maupun konsumen pengguna aplikasi. Pengembang mendapatkan keuntungan dari pemasangan aplikasi, iklan dan pembelian dari aplikasi sedangkan konsumen dapat menikmati fasilitas atau fungsi dari aplikasi pihak ketiga tersebut[2][3]. Namun, pendistribusian tersebut juga memberikan kemudahan untuk pengembang aplikasi pihak ketiga yang mempunyai niat jahat untuk mendistribusikan malware.

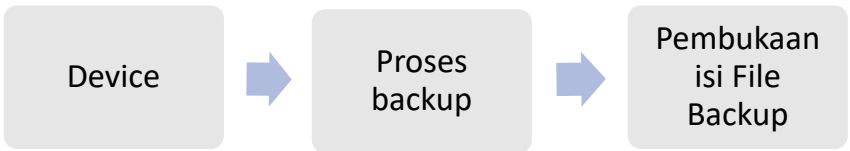
Aplikasi pihak pertama atau biasa disebut dengan aplikasi bawaan perangkat seluler, juga menyimpan informasi pribadi dan informasi lainnya yang bersifat pribadi maupun tidak dari pengguna perangkat tersebut. Secara tidak sadar dan secara terus menerus aplikasi pihak pertama dan pihak ketiga membutuhkan informasi dari pengguna perangkat seluler tersebut untuk menggunakan atau menjalankan salah satu fitur dari aplikasi tersebut[4][5]. Maka dari itu, informasi atau data-data tersebut tersimpan pada perangkat seluler dan bisa dijadikan atau bisa di analisis guna untuk kebutuhan forensik digital[6]. Dengan memanfaatkan file backup sebuah perangkat seluler, karena pada file backup tersebut menyimpan informasi dan data-data dari aplikasi pihak pertama maupun aplikasi pihak ketiga.

Akan tetapi setiap aplikasi pihak pertama maupun aplikasi pihak ketiga untuk menyimpan atau menempatkan informasi dan data-data tentang aplikasi tersebut maupun informasi data pengguna pribadi tergantung pada pengembang pembuat aplikasi tersebut. Akan tetapi jika suatu perangkat seluler hanya menggunakan aplikasi pihak ketiga, maka untuk analisis forensik sederhana dengan tujuan untuk menyelesaikan kejahatan siber akan kurang maksimal[7][8]. Pada artikel ini kita menggunakan file *back up* dari perangkat ponsel untuk mengetahui isi dari data-data dari aplikasi pihak pertama dan pihak ketiga guna membantu proses forensik digital.

Pada *paper* ini kita menunjukkan bahwa file backup dari perangkat seluler, terdapat jejak informasi dan data-data dari aplikasi khususnya pihak pertama yang terdapat pada file tersebut. Tanpa terenkripsinya file backup tersebut, dapat dilihat data dan informasi yang ada dengan memanfaatkan aplikasi iTunes untuk mem-backup dan 3uTools untuk melihat informasi dan data-data yang ada untuk membantu dalam proses forensik digital[9][10].

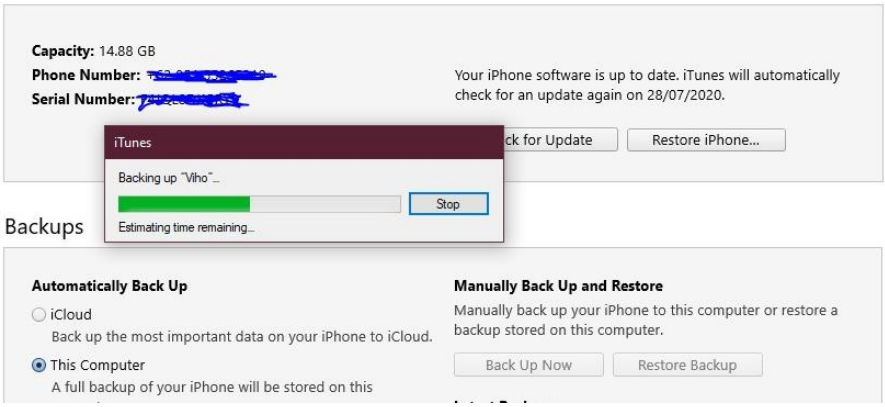
2. METODE PENELITIAN

2.1. Akuisisi data dan eksperimental



Gambar 1. Alur penelitian

Pada penelitian ini menggunakan metodologi menggunakan file back up dari sebuah perangkat seluler, pada kali ini menggunakan perangkat seluler yang menggunakan sistem operasi *iOs* untuk menjadi targetnya. Perangkat tersebut digunakan untuk kegiatan sehari-hari atau bisa disebut dengan *daily device*, maka dari itu banyak tersimpan data dan informasi dari pengguna yang telah tersimpan pada perangkat seluler tersebut. Untuk mem-backup perangkat tersebut, kita menggunakan aplikasi iTunes yang di install pada windows.



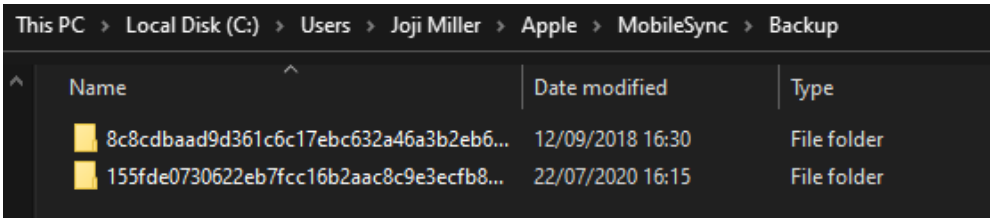
Gambar 2. Proses backup menggunakan aplikasi iTunes

Tabel 1. Perangkat keras dan luna yang digunakan

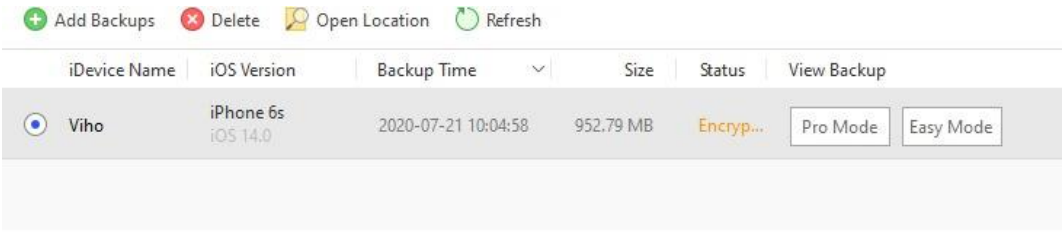
Nama	Keterangan
iPhone 6s (iOS 14)	Target device
Windows 10	Sistem operasi pc
iTunes	Perangkat lunak
3uTools	Perangkat lunak

2.2. Analisis data

Setelah proses backup, file tersebut akan tersimpan komputer yang digunakan dalam bentuk 2 file folder. File tersebut dibuka menggunakan software 3uTools untuk mengetahui isi dan data-data yang terdapat dalam file backup tersebut.



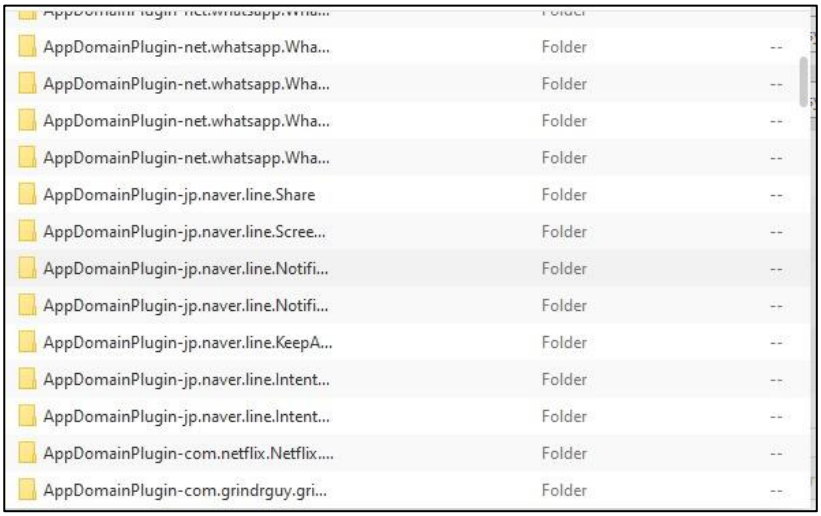
Gambar 3. Keterangan tempat file backup device tersimpan



Gambar 4. Keterangan Device yang telah di Backup dan siap di buka dengan aplikasi 3uTools

3. HASIL DAN PEMBAHASAN

Kebanyakan Tools biasanya fokus pada integrasi aplikasi bawaan Media seperti itu sebagai musik, film, dan podcast disinkronkan ke perangkat melalui iTunes disimpan di / iTunes Control direktori. Tempat direktori yang ini menyediakan alat dengan kemampuan untuk menemukan jenis data yang sama di tempat yang sama di seluruh beberapa perangkat seluler Apple, terlepas dari bagaimana caranya pengguna mengonfigurasi perangkat. Gambar yang diambil oleh iPhone (dan video pada model yang kompatibel) termasuk Tag data EXIF.



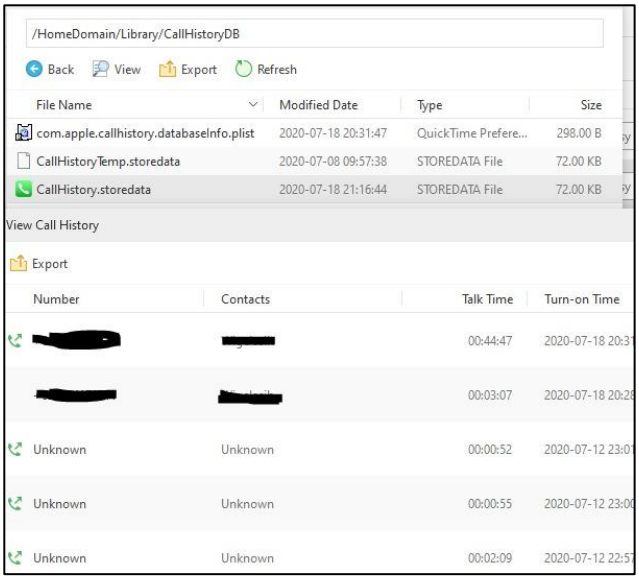
Gambar 5. Keterangan hasil dari aplikasi pihak ketiga yang terdapat di file backup

Data ini disimpan di ponsel di dalam direktori / Media / 100APPLE / dan mungkin disertakan saat salinan gambar ditransfer ke media atau lokasi lain. Setelah diekstraksi, EXIF data dapat diperiksa menggunakan alat seperti *View* di Mac OS X untuk menemukan tempat dimana tersimpan pada saat gambar diambil. Gambar dapat ditemukan di lokasi yang sama untuk setiap perangkat seluler Apple dengan kamera yang kompatibel. Data yang didapat seperti waktu dan lokasi perangkat itu digunakan untuk mengambil gambar.

Informasi pada Wi-Fi juga dapat digunakan untuk menghubungkan tanggal, waktu dan lokasi geografis. History pada wifi disimpan dalam file plist. Di bersama dengan DHCP atau

data lain, ini dapat digunakan untuk menempatkan perangkat pada waktu tertentu lokasi serta untuk menautkan lalu lintas (email, web, atau jika tidak) ke alamat IP atau Titik Akses yang diberikan. Perangkat seluler Apple tetap menyimpan data ini untuk membuat daftar Wi-Fi yang dikenal atau history Wi-Fi pada jaringan yang terkait dengan perangkat. Ini memungkinkan perangkat untuk menyambungkan secara otomatis dengan akses jaringan yang sebelumnya telah terhubung.

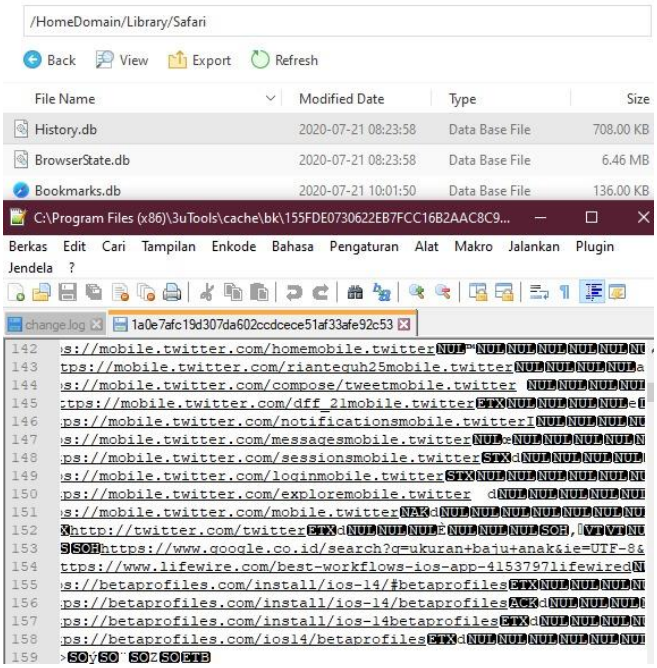
Meskipun bermanfaat untuk pemilik perangkat, data Wi-Fi mudah dan dapat diakses untuk seorang analis forensik. Semua yang pernah pengguna buka pada browser yang digunakan termasuk safari tersimpan pada cache dan dapat dibuka kembali. Kontak yang ada di dalam "buku telepon" di dalam telepon. Tidak semua aplikasi menyimpan kontak informasi dengan cara atau tempat yang sama, tetapi kenyataannya bahwa data yang ada dapat memungkinkan pemeriksa mengaksesnya.



Gambar 6. Keterangan hasil dari nomor kontak pada handphone

Aplikasi lain juga menyimpan informasi tentang aktivitas pengguna. Browser pada perangkat seluler Apple, Safari, menyimpan riwayat web dan penanda di telepon. Safari di Apple sepenuhnya mendukung standar web baru, Hypertext Markup Language versi 5 (HTML5). HTML5 memberikan standar yang digunakan pengembang web dapat membuat basis data informasi dan menyimpannya secara lokal di perangkat.

Situs web seperti Google Mail memasukkan ini ke dalam versi untuk Apple perangkat seluler untuk memberi pengguna offline fungsionalitas situs web. Bookmark, riwayat, dan bahkan basis data lokal HTML5 dapat diakses melalui pencarian file di dalam direktori / Library. Aplikasi catatan juga tersedia untuk dilihat dalam hal ini direktori dan berisi cap waktu untuk catatan yang disimpan. Banyak artefak hadir di dalam aplikasi bawaan data menarik bagi analis forensik. Jumlah data yang dapat diperoleh dari ini bisa berharga untuk investigasi.



Gambar 7. Keterangan history browser

4. KESIMPULAN

Dari analisis keamanan pihak pertama dan ketiga dengan memanfaatkan iTunes sebagai media file backup dapat disimpulkan bahwa :

1. Proses Analisa kali ini menggunakan perangkat seluler yang menggunakan sistem iOs dengan aplikasi backup iTunes dan membuka file backup tersebut dengan aplikasi 3utools yang akan menghasilkan data dan informasi yang terdapat pada device tersebut dengan tujuan untuk membantu proses penyelidikan dalam forensik digital
2. File backup iTunes yang dibreakdown dibuat tidak terenskripsi sehingga dapat dibuka dengan aplikasi 3uTools untuk mengetahui isinya
3. Didapat banyak informasi dan data seperti sms, kontak, history browser, document aplikasi pihak ketiga pada device tersebut yang berguna untuk keperluan forensic digital.
4. Direkomendasikan jika ingin membackup perangkat seluler sebaiknya file backup tersebut di enskripisi karena masih menyimpan data dan informasi yang bersifat pribadi

Referensi:

[1] A. Levinson, B. Stackpole, and D. Johnson, “Third party application forensics on Apple mobile devices,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–9, 2011.

[2] W. Yang, X. Xiao, R. Pandita, W. Enck, and T. Xie, “Improving mobile application security via bridging user expectations and application behaviors,” *ACM Int. Conf. Proceeding Ser.*, no. March,

2014.

[3] S. Azam, R. S. Sumra, B. Shanmugam, K. C. Yeo, M. Jonokman, and G. N. Samy, “Security source code analysis of applications in Android OS,” *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 30–34, 2018.

[4] J. F. Garc, J. Alonso, and C. Garc, “Security Assessment Methodology for Mobile Applications,” no. May 2018, p. 2015, 2015.

[5] I. Journal and C. Science, “FRAPPE - For Identifying Third Party Application on Facebook,” vol. 3, no. 3, pp. 80–83, 2016.

[6] P. Manisha, B. Sudhamayi, and M. Kiranmai, “Verification of Security for Untrusted Third Party Ip Cores,” *Int. Res. J. Eng. Technol.*, vol. 4, no. 9, pp. 634–641, 2017.

[7] L. Desmet, W. Joosen, F. Massacci, and K. Naliuka, “A Flexible Security Architecture to Support Third-party,” *Security*, pp. 19–28.

[8] R. W. Proctor, M.-C. Lien, G. Salvendy, and E. E. Schultz, “A Task Analysis of Usability in Third-Party Authentication,” *Inf. Secur. Bull.*, no. April, pp. 49–56, 2000.

[9] I. A. Levinson, B. Stackpole, and I. D. Johnson, “Forensik Aplikasi Pihak Ketiga pada Perangkat Seluler Apple Abstrak,” pp. 1–9, 2011.

[10] A. HAYRAN, M. İĞDELİ, A. YILMAZ, and C. GEMCİ, “Security Evaluation of IOS and Android,” *Int. J. Appl. Math. Electron. Comput.*, no. February, pp. 258–258, 2016.