JURNAL TEKNOLOGI TERPADU. 8 VOL. 2 OKTOBER 2020 ISSN : 2338 - 66649

Received : April 2020	Accepted: Agustus 2020	Published : Oktober 2020

Pengujian dan Analisa Reverse Engineering Pada Platform Android (Studi Kasus: Tebak_Gambar.apk)

I Putu Agus Eka Pratama[1*], Rasendriya Revo Daniswara[2]
[1,2] Prodi Teknologi Informasi, Fakultas Teknik, Universitas Udayana*

[*]eka.pratama@unud.ac.id

Abstract

Not all of software (applications) provide the source code directly to the users. Applications with closed source code only provide ready-made binaries to be installed or run directly, making it difficult for users to learn the structure of the application along with the source code and components in it. For this reason, reverse engineering needs to be done on the application. In this research, reverse engineering is carried out on an application on the Android platform called Tebak_Gambar.apk based on Java. The concept of reverse engineering work in the Tebak_Gambar.apk file is to decompile the .apk file to get the .jar file, then decompile the .jar file to obtain the components of the Tebak_Gambar.apk application. The final result of reverse engineering of the Tebak_Gambar.apk application is the production of the components making up the application, so that it gives more value to help the user to understand the application structure along with the source code .java, activity scheme .xml, and additional components (images, audio, fonts). The drawback is that it cannot find the names of variables, methods, and classes, so it is necessary to rename according to the understanding of the logic flow of the application concerned.

Keywords : application, Tebak_Gambar.apk, reverse engineering, Java, decompilation

Abstrak

Tidak semua perangkat lunak (aplikasi) menyediakan langsung sumber kodenya kepada para pengguna. Aplikasi dengan sumber kode tertutup hanya menyediakan binary siap pakai untuk diinstal atau dijalankan langsung, sehingga menyulitkan pengguna untuk mempelajari struktur aplikasi beserta sumber kode dan komponen di dalamnya. Untuk itu, perlu dilakukan reverse engineering pada aplikasi. Pada penelitian ini, dilakukan reverse engineering pada aplikasi platform Android bernama Tebak_Gambar.apk berbasis Java. Konsep kerja reverse engineering pada file Tebak_Gambar.apk adalah melakukan dekompilasi file .apk untuk memperoleh file .jar, kemudian melakukan dekompilasi file .jar untuk memperoleh komponen-komponen penyusun aplikasi Tebak_Gambar.apk. Hasil akhir dari reverse engineering aplikasi Tebak_Gambar.apk adalah dihasilkannya komponen-komponen penyusun aplikasi, sehingga memberi nilai lebih yaitu membantu pengembang memahami struktur aplikasi beserta dengan source code .java, activity scheme .xml, dan komponen tambahan (gambar, audio, font). Adapun kekurangannya adalah tidak dapat menemukan nama dari variabel, method, dan class, sehingga perlu melakukan penamaan ulang sesuai dengan pemahaman terhadap alur logika dari aplikasi bersangkutan.

Kata kunci : aplikasi, Tebak_Gambar.apk, reverse engineering, Java, dekompilasi

1. Pendahuluan

1.1. Latar Belakang

Di tengah perkembangan teknologi yang semakin pesat seperti saat ini, para pengembang perangkat lunak komputer (aplikasi) dituntut untuk bisa mengembangkan aplikasi yang dapat memenuhi kebutuhan para pengguna yang makin kompleks.

Mereka harus dapat mengembangkan aplikasi yang inovatif. Untuk dapat mengembangkan aplikasi yang inovatif, pengembang dapat mempelajarinya melalui aplikasi lain yang telah ada. Namun hal ini akan sulit untuk dilakukan apabila pengembang tidak dapat mengetahui cara kerja dari aplikasi tersebut, struktur di dalamnya, serta metode dan algoritma apa yang digunakan. Solusi untuk hal ini adalah dengan melakukan reverse engineering terhadap aplikasi.

Melalui proses reverse engineering, pengembang dapat mengetahui source code dari sebuah binary file (executable) pada sebuah aplikasi. Proses kompilasi dari sebuah source code menjadi executable file disebut sebagai proses forward engineering, sedangkan reverse engineering merupakan proses mengembalikan sebuah executable file menjadi sebuah source code [1]. Source code yang didapatkan dari proses reverse engineering ini bisa menjadi modal untuk mempelajari logika dari program tersebut, untuk menciptakan sebuah inovasi yang dapat menjawab kebutuhan masyarakat yang terus bertambah. reverse enginering dapat dilakukan pada hampir semua platform dan bahasa pemrograman, salah satunya pada platform Android dan Java.

Android merupakan sistem operasi yang berbasis kernel linux [2]. Perkembangan android sekarang diaplikasikan ke dalam ponsel atau sejenisnya. Di dalam platform Android, berbagai jenis perangkat lunak dalam bentuk permainan, social media, layanan, dan lainnya dikembangkan. Perangkat lunak pada platform Android pada dasarnya terdiri atas file java, resources, dan manifest[3]. Khusus untuk pengembangan aplikasi game pada platform Android, digunakan Game Development Life Cycle (GDLC). GDLC terdiri dari 5 proses utama, yang meliputi: pitch, pre production, production, testing, dan mastering[4].

Dengan memahami teknik reverse engineering, akan memudahkan pengembang di dalam menjalankan GDLC, terutama pada tahap testing. Aplikasi Tebak_Gambar.apk dipilih sebagai contoh aplikasi untuk pengujian reverse engineering, karena aplikasi ini berbasis Java pada platform Android, namun disediakan dalam bentuk binari (.apk), sehingga perlu dilakukan proses reverse engineering untuk memperoleh source code dan komponen-komponen pendukung, sehingga dapat dipelajari lebih lanjut.

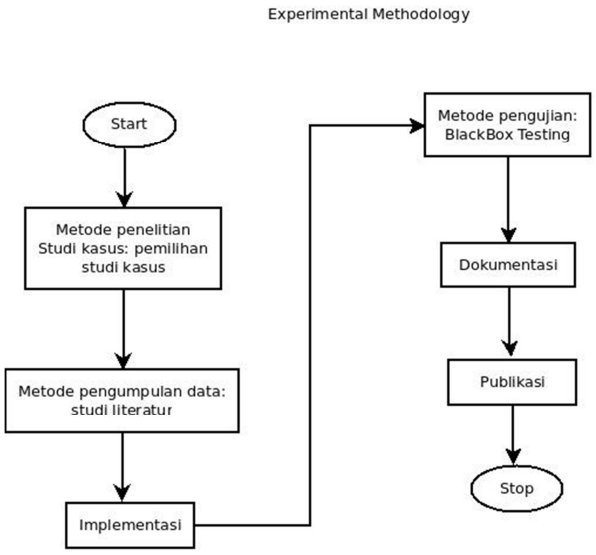
Terdapat empat buah penelitian mengenai reverse engineering yang telah dilakukan oleh sejumlah peneliti sebelumnya. Rahmadani di dalam penelitiannya mengungkapkan bahwa reverse engineering dapat digunakan untuk penentuan pola interaksi pada Sequence Diagram, sehingga memudahkan di dalam proses desain UML, dengan sampel pada aplikasi di platform Android [7]. Aldya menyebutkan membuktikan bahwa reverse engineering dapat membantu mengetahui dan menjelaskan alur di dalam identifikasi malware RAT, beserta dengan tool-tool yang digunakan [8]. Redo menyajikan penelitian tentang reverse engineering untuk menemukan prinsip-prinsip teknologi suatu produk dengan cara menganalisa struktur, fungsi dan cara pada produk tersebut, sehingga dapat dilakukan patching ke dalam perangkat lunak tersebut untuk meningkatkan kualitas dari perangkat lunak itu sendiri [9]. Terakhir, Waliulu dan Alam telah membuktikan bahwa reverse engineering dapat diujikan untuk analisa statis forensic malware Web C2-Div, yang meliputi scanning, suspected packet di dalam jaringan, serta analisa malware behavior dan disassembler body malware [10].

Berdasarkan kepada keempat penelitian sebelumnya ini, maka pada penelitian ini difokuskan kepada reverse engineering untuk memperoleh sumber kode dari binari aplikasi Tebak_Gambar.apk, sehingga dari sumber kode dan komponen hasil reverse engineering

yang diperoleh, dapat dipelajari secara lebih mendalam. Reverse Engineering terhadap file binari aplikasi Tebak_Gambar.apk, menggunakan JD-GUI dan ApkTool pada sistem operasi Linux Ubuntu.

2. Metode Penelitian

Metode-metode penelitian yang digunakan di dalam penelitian ini, yaitu: metode penelitian kualitatif berupa studi kasus, metode pengumpulan data berupa studi literatur, dan metode pengujian berupa BlackBox Testing. Metode-metode penelitian ini berdasarkan kepada metodologi penelitian Experimental Methodology, yang di dalamnya meliputi: pemilihan studi kasus, studi literatur, implementasi, pengujian, dokumentasi, dan publikasi [5]. Bagan diagram alir dari Experimental Methodology, ditunjukkan pada Gambar 1 di bawah ini:



Gambar 1. Bagan alir Experimental Methodology

2.1. Pemilihan Studi Kasus

Metode penelitian kualitatif berupa studi kasus yang digunakan di dalam penelitian ini,

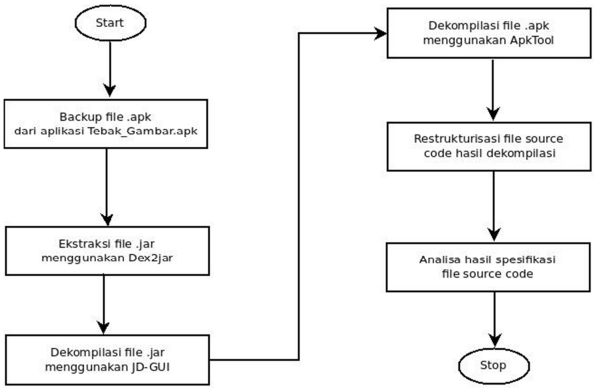
memerlukan adanya pemilihan studi kasus. Studi kasus yang dipilih adalah reverse engineering pada aplikasi Tebak_Gambar.apk yang berjalan pada platform android, dengan pertimbangan bahwa aplikasi Tebak_Gambar.apk berbasis Java yang disediakan dalam bentuk file binari (.apk), sehingga perlu dilakukan reverse engineering untuk memperoleh source code dan komponen-komponen pendukung, sehingga dapat dipelajari lebih lanjut.

Aplikasi Tebak_Gambar.apk merupakan aplikasi permainan kuis yang dikembangkan oleh Lukis Cindera dan Irwanto Widyatri pada tahun 2013, di mana pemain diberikan sebuah gambar untuk diinputkan jawaban pada kolam jawaban yang disediakan [6].Tujuan reverse engineering pada aplikasi Tebak_Gambar.apk adalah untuk memperoleh source code aplikasi, sehingga dapat diketahui struktur dan komponen-komponennya, agar dapat dipelajari lebih lanjut.

3. Hasil Penelitian

3.1. Implementasi dan Pengujian

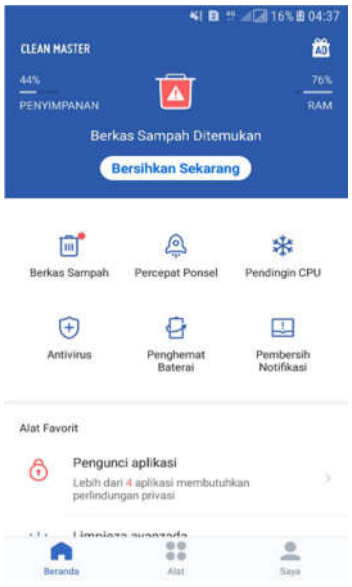
Urutan langkah implementasi dan pengujian, meliputi: backup file .apk dari aplikasi Tebak_Gambar.apk, ekstraksi file .jar menggunakan Dex2jar untuk memperoleh file Tebak_Gambar-dex2jar.jar, dekompilasi file Tebak_Gambar-dex2jar.jar menggunakan JD-GUI untuk melihat isi file Tebak_Gambar-dex2jar.jar, dekompilasi file Tebak_Gambar.apk menggunakan aplikasi ApkTool untuk memperoleh file lainnya di luar file Java, restrukturisasi file source code hasil dekompilasi, dan analisa hasil spesifikasi file *source code*. Bagan diagram alir dari urutan langkah sebagaimana penjelasan di atas, disajikan pada Gambar 2 di bawah ini:



Gambar 2. Bagan alir urutan langkah pada implementasi dan pengujian

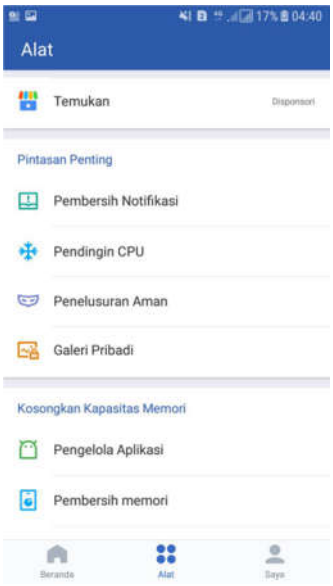
3.2. Backup Tebak_Gambar.apk

Backup aplikasi Tebak_Gambar.apk dilakukan melalui proses dekompilasi file .apk menjadi source code, menggunakan Clean Master di Android. Urutan langkahnya yaitu: mengunduh Clean Master, menginstal, menjalankan di Android, ditunjukkan pada Gambar 3:



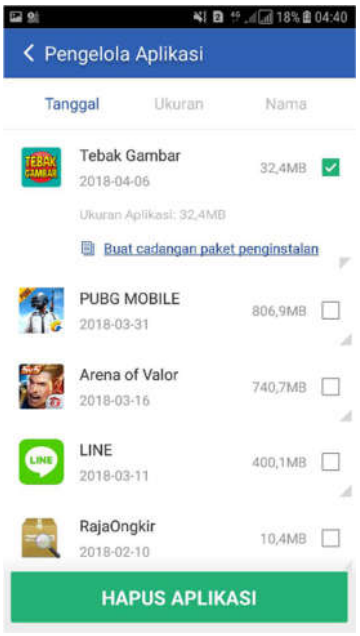
Gambar 3. Tampilan awal Clean Master

• Kemudian memilih menu Alat dan sub menu menu Pengelola Aplikasi, ditunjukkan pada Gambar 4:



Gambar 4. Tampilan menu Alat pada *Clean Master*

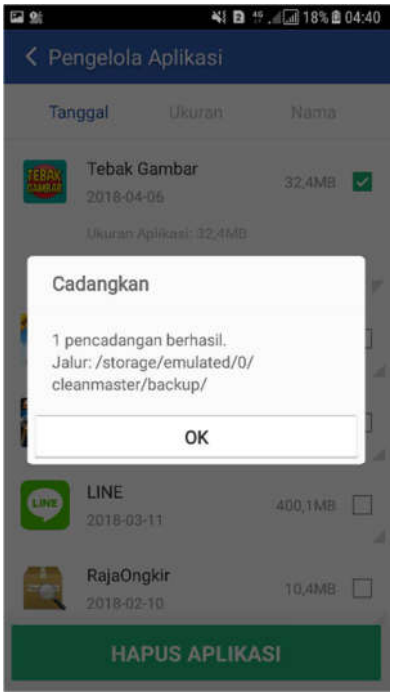
•Selanjutnya memilih aplikasi Tebak_Gambar, memilih opsi Buat Cadangan Paket Penginstalan, sebagaimana ditunjukkan pada Gambar 5:



Gambar 5. Menu Pengelola Aplikasi pada *Clean Master*

•Setelah proses backup selesai dilakukan, kemudian akan muncul notifikasi sebagaimana

ditunjukkan pada Gambar 6, kemudian membuka direktori file dan memindahkannya ke folder /home.



Gambar 6. Notifikasi proses backup berhasil dilakukan

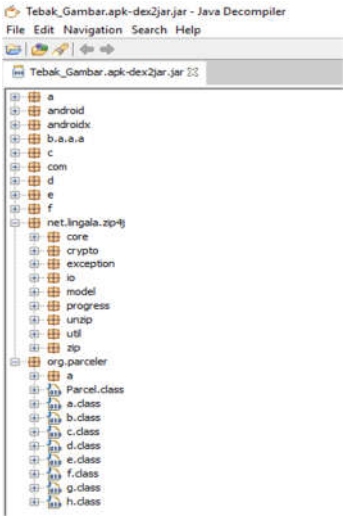
3.3. Ekstraksi File .jar Menggunakan Dex2jar

Setelah mendapatkan file package dari aplikasi Tebak_Gambar.apk, langkah selanjutnya adalah melakukan ekstraksi file .jar menggunakan aplikasi Dex2jar. Urutan langkah yang dilakukan yaitu: menjalankan Terminal di Linux Ubuntu, pindah ke directory file dex2jar, menjalankan perintah sh d2j-dex2jar.sh Tebak_Gambar.apk melalui Terminal di Linux Ubuntu. Luaran yang dihasilkan berupa file Tebak_Gambar-dex2jar.jar, ditunjukkan pada Gambar 7:

Gambar 7. Ekstrak file .jar dari Tebak_Gambar.apk

3.4. Dekompilasi Menggunakan JD-GUI

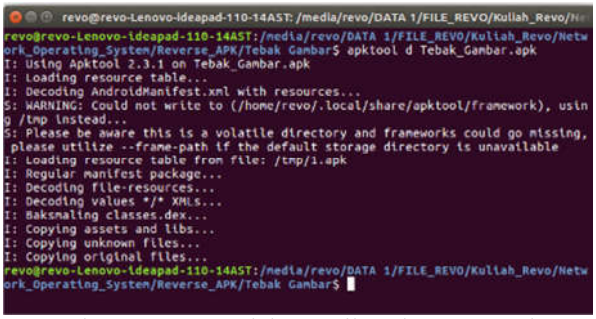
Langkah selanjutnya adalah dekompilasi menggunakan JD-GUI untuk dapat melihat isi dari file Tebak_Gambar-dex2jar.jar. Urutan langkah yaitu: menjalankan aplikasi JD-GUI, memilih menu File, memilih opsi Open File, memilih file Tebak_Gambar-dex2.jar, dan memulai proses dekompilasi. Hasil dekompilasi adalah sejumlah komponen class dan kelengkapan file Java lainnya, ditampilkan pada Gambar 8:



Gambar 8. Hasil dekompilasi Tebak_Gambar-dex2.jar

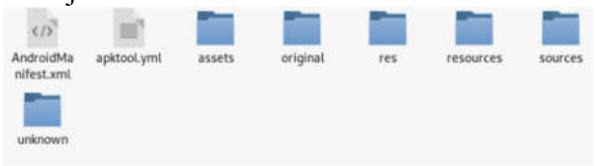
3.5. Dekompilasi Menggunakan ApkTool

Tahap pengujian selanjutnya adalah melakukan dekompilasi file Tebak_Gambar.apk menggunakan aplikasi Apktool, untuk memperoleh file lainnya di luar file Java, sehingga dapat melengkapi proses reverse engineering. Urutan langkah yaitu: membuka Terminal di Linux Ubuntu, pindah ke direktori file Tebak_Gambar.apk, menjalankan perintah apktool.jar d Tebak_Gambar.apk di Terminal Linux (opsi d menyatakan direktori tempat file berada), ditunjukkan pada Gambar 9:



Gambar 9. Command decompile apk menggunakan ApkTool.

• Setelah muncul direktori Tebak_Gambar, kemudian dilakukan dekompilasi, sehingga setelah dekompilasi selesai, di dalam direktori Tebak_Gambar akan terdapat sejumlah subdirektori di luar Java, yaitu: original, res, resources, sources, apktool.yml, sebagaimana ditunjukkan Gambar 10:



Gambar 10.Hasil decompile file Tebak_Gambar.apk menggunakan apktool

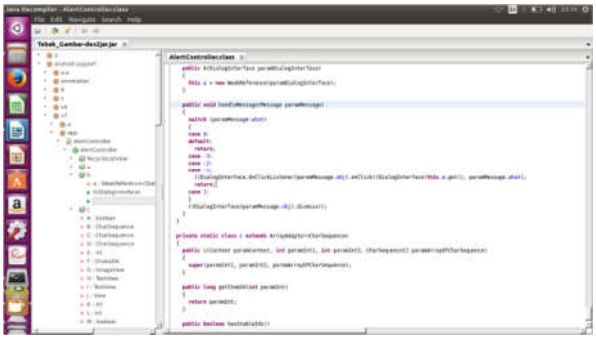
3.6. Restrukturisasi File Source Code

Berdasarkan kepada langkah - langkah pengujian reverse engineering yang telah dilakukan, maka diperoleh hasil yaitu :

1.Hasil dekompilasi menggunakan tools dex2jar dan jdgui.

2.Hasil dekompilasi menggunakan Apktool.

Dari pengujian dekompilasi file Tebak_Gambar-dex2.jar menggunakan JD-GUI, dapat diperoleh hasil dekompilasi berupa source code yang baik dan terstruktur. Namun hasil dekompilasi menggunakan JD-GUI ini memiliki satu kekurangan, yaitu pengguna tidak dapat menemukan nama dari variabel, method, maupun class. Solusi untuk hal ini adalah melakukan penamaan ulang (rename) untuk setiap variabel, method, atau class sesuai dengan pemahaman terhadap alur logika dari aplikasi bersangkutan, dalam hal ini Tebak_Gambar.apk (Gambar 9).



Gambar 9.Source code hasil dekompilasi menggunakan aplikasi JD-GUI

Terkait hasil dari proses dekompilasi untuk memperoleh file selain Java, (misal: file .xml), hasil yang diperoleh serupa dengan hasil dari menggunakan aplikasi JD-GUI, yaitu source code yang terstruktur rapi pada direktorinya masing - masing. Salah satunya adalah *source code* .xml dari layout yang terdapat pada sub direktori /Tebak_Gambar/res/layout. Kelebihan lain yang diperoleh dari hasil pengujian dekompilasi untuk memperoleh file selain file Java ini adalah penamaan file xml yang tidak lagi berupa variabel acak, serta isi dari file xml cukup terstruktur. Salah satunya adalah file activity_main.xml pada direktori layout (Gambar 10).

Gambar 10.File activity_main.xml

3.7. Analisa Spesifikasi File Source Code

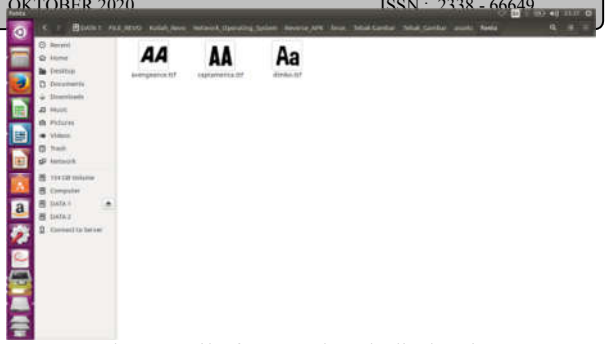
Dari langkah - langkah pengujian yang telah dilakukan dan pengamatan terhadap hasil - hasil yang diperoleh, dapat dilakukan analisis terhadap spesifikasi file source code hasil reverse engineering aplikasi Tebak_Gambar.apk. Proses dekompilasi

menggunakan JD-GUI dan dex2jar, bertujuan untuk memperoleh file .class (Java) yang ada pada file Tebak_Gambar.apk. Hasil dekompilasi yang diperoleh tidak akurat, terlihat dari penamaan variabel, method, dan class yang masih memiliki penamaan otomatis oleh JD-GUI. Hasil lainnya adalah source code tertata dengan struktur yang rapi.

Sedangkan proses dekompilasi menggunakan Apktool, bertujuan untuk mendapatkan resource lainnya dari file Tebak_Gambar.apk (misal: file .xml). Hasil yang diperoleh dari proses dekompilasi menggunakan Apktool ini adalah penamaan variabel dan method yang akurat, serta source code dari file xml yang terstruktur. Hasil lainnya yang diperoleh adalah file icon yang digunakan pada aplikasi Tebak_Gambar.apk. Sebagai contoh: file drawable-xhdpi-v4 yang berfungsi untuk menyimpan sejumlah icon dari aplikasi Tebak_Gambar.apk (Gambar 11).

Gambar 11.File drawable-xhdpi-v4

Pada sub direktori Asset juga diperoleh sejumlah font dan library fungsi yang ada pada aplikasi Tebak_Gambar.apk (Gambar 12).



Gambar 12.File fonts pada sub direktori Asset

4. Kesimpulan

Teknik reverse engineering yang dilakukan terhadap file aplikasi Tebak_Gambar.apk di Linux Ubuntu pada penelitian ini, membantu pengembang di dalam memahami struktur dan algoritma dari aplikasi. Aplikasi Apktool berfungsi untuk membantu proses reverse engineering melalui kemampuannya di dalam menampilkan struktur file .xml dari aplikasi Tebak_Gambar.apk, sedangkan aplikasi JD-GUI dan dex2jar berfungsi untuk memperoleh file .class (Java) dari aplikasi Tebak_Gambar.apk, sehingga pengembang dapat mempelajari algoritma dari aplikasi tersebut.

Teknik reverse engineering di platform Android dapat dilakukan oleh siapapun, dengan mengikuti tahapan - tahapan pengujian yang telah dijabarkan di dalam penelitian ini. Namun untuk memahami struktur dan algoritma dari aplikasi yang diujikan beserta dengan hasil yang diperoleh, diperlukan pemahaman yang baik mengenai pemrograman di platform Android.

5. Saran

Penelitian yang dilakukan, mampu menunjukkan peran dari reverse engineering di dalam membantu pengembang untuk mengetahui struktur dan algoritma yang ada di dalam aplikasi berbentuk file binary, melalui source code yang ditampilkan. Ke depannya perlu dilakukan pengujian reverse engineering pada aplikasi di luar basis Java (misal: C, C#,

Python) yang penggunaannya cukup banyak dewasa ini di dunia teknologi informasi.

6. Daftar Pustaka

[1] Eldad Eilam, Reversing : The Secret of Reverse engineering, Crosspoint Boulevard Indianapolis, Wiley Publishing, Inc, 2005.

[2] Y. Kusuma, Membedah Kehebatan Android, Jakarta, DKI: Grasindo, 2011.

[3] Android Studio, Mengenal Android Studio (Indonesia).https://developer.android.com/studio/intro/index.html?hl=id. 9 april 2018 20.15.

[4] Dendy Triadi, Bedah Tuntas Fitur Android, Yogyakarta, Jogja Great! Publisher, 2013

[5] Lukis Cindera, Irwanto Widyatri. Tebak Gambar. Google Play Store. 2013. https://play.google.com/store/apps/details?id=com.tebakgambar&hl=in.

[6] V.S. Rahmadani, dkk, "Penerapan Reverse Engineering Dalam Penentuan Pola Interaksi Sequence Diagram Pada Sampel Aplikasi Android," Journal of Information Systems Engineering and Business Intelligence, Vol. 1, No. 1, April 2015.

[7] A.P. Aldya, dkk, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," JEPIN (Jurnal Edukasi dan Penelitian Informatika) Vol. 5 No. 1 April 2019

[8] M.R. Redo, "Pendekatan Reverse Engineering Untuk Pengujian Keamanan Guna Meningkatkan Kualitas Perangkat Lunak," Jurnal Informatika, Vol. 16, No. 1, Juni 2016.

[9] R.F. Waliulu, T.H.I. Alam, "Reverse Engineering Analysis Statis Forensic Malware Webc2-Div," Insect (Informatic and Security) Jurnal Teknik Informatika Universitas <Muhammadiyah Sorong, Vol 4, No 1, 2018.