

**ANALISIS MALWARE ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS MALWARE ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS MALWARE ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING**

yang disusun dan diajukan oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Februari 2023

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.

NIK. 190302181

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS MALWARE ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING

yang disusun dan diajukan oleh

FRENVOL DE SANTONARIO MAGNO MOISES
17.83.0039

Telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Februari 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.Kom
NIK. 190302181

M. Rudyanto Arief, S.T, M.T
NIK. 190302098

Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105

*Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Februari 2023.*

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : FRENVOL DE SANTONARIO MAGNO MOISES
NIM : 17.83.0039

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS MALWARE ANDROID MENGGUNAKAN METODE
REVERSE ENGINEERING**

Dosen Pembimbing : Joko Dwi Santoso, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 27 Februari 2023

Yang Menyatakan,



Frenvol De Santonario Magno Moises

HALAMAN PERSEMBAHAN

Segala puji bagi Tuhan Yang Maha Esa atas limpahan rahmat dan hidayah serta karunia-Nya sehingga *skripsi* ini selesai dengan sebaik-baiknya. *Skripsi* ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Geraldo Moises dan Ibu Durvalina Belo Magno yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Joko Dwi Santoso, M.kom. Selaku dosen pembimbing yang telah membantu dalam penyusunan *skripsi* ini.
3. Kepada kakak serta adik saya yang selalu memberikan semangat dan dukungan.
4. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.
5. Seseorang yang sangat berharga dan memberikan banyak arti dalam hidup saya, Lidia Kristiani Sihalohe. Terima kasih atas cinta, dukungan, kebaikan, perhatian, dan kebijaksanaan serta telah mengajarkan arti kedewasaan.

Terimakasih yang sebesar-besarnya untuk Kalian semua, akhir kata saya persembahkan *skripsi* ini untuk Kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup saya. Semoga *skripsi* ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis *Malware* Android Menggunakan Metode *Reverse engineering*”.

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer (S.Kom) Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Tuhan Yang Maha Esa karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Joko Dwi Santoso, M.Kom. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 4 Oktober 2022

FRENVOL DE SANTONARIO MAGNO MOISES



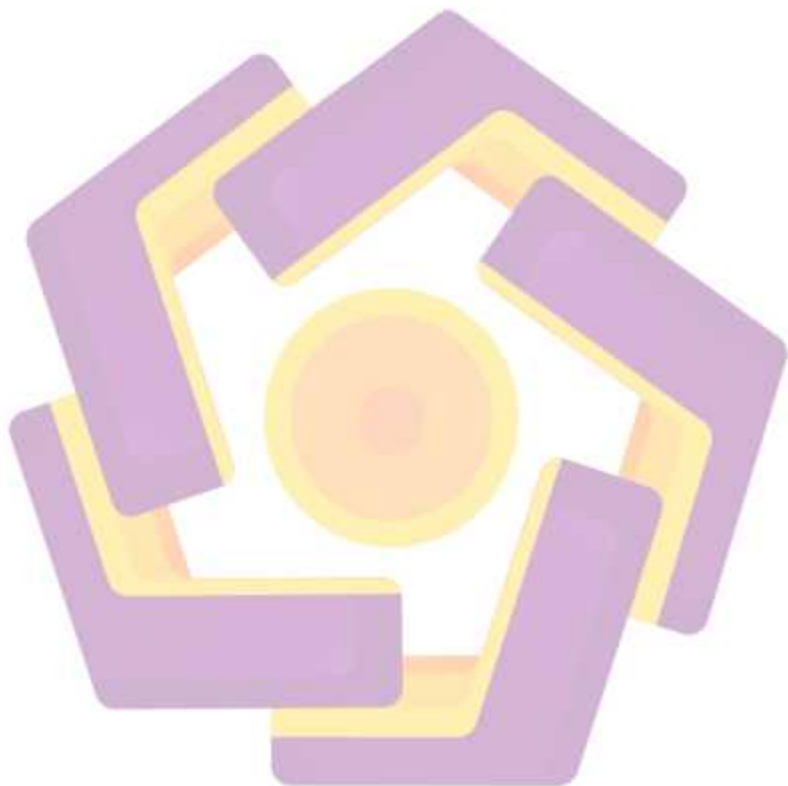
DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN <i>SKRIPSI</i>	
Error! Bookmark not defined.	
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penelitian	4
1.4 Batasan Masalah	4
1.5 Tujuan Penelitian	5
1.6 <i>Sistematika</i> Penulisan.....	5
BAB II <i>LANDASAN TEORI</i>	7
2.1 Tinjauan Pustaka.....	7
2.2 <i>Malware</i>	10
2.2.1 <i>Virus</i>	11
2.2.2 <i>Worm</i>	11
2.2.3 <i>Spyware</i>	11
2.2.4 <i>Trojan</i>	11
2.2.5 <i>Adware</i>	12

2.2.6	<i>Keylogger</i>	12
2.2.7	<i>Ransomware</i>	12
2.2.8	<i>Malicious</i>	12
2.2.9	<i>Rootkit</i>	12
2.2.10	<i>Backdoor</i>	13
2.3	<i>Anti-Malware</i>	13
2.3.1	<i>Anomaly-based Detection</i>	13
2.3.2	<i>Specification-based Detection</i>	13
2.3.3	<i>Signature-based detection</i>	13
2.4	<i>Android</i>	14
2.5	<i>Reverse engineering</i>	16
2.5.1	<i>Assembly</i>	17
2.5.2	<i>Disassembly</i>	17
2.5.3	<i>Debugging</i>	17
2.5.4	<i>X86 Arsitektur</i>	17
2.5.5	<i>Instruction</i>	17
2.5.6	<i>Hashing</i>	17
2.5.7	<i>String Analysis</i>	18
2.5.8	<i>Malware Analysis Environment and Requirement (MAER)</i>	18
2.5.9	<i>Repository Malware</i>	18
2.5.10	<i>Decompile</i>	18
2.6	<i>Apktool</i>	19
2.7	<i>Java Development Kit</i>	19
2.8	<i>Virtual Machine</i>	19
2.9	<i>Kali linux</i>	19
2.10	<i>APK (Application Packet File)</i>	20
2.11	<i>Smali</i>	20
2.12	<i>Mobile Security Framework (MobSF)</i>	20
2.13	<i>Genymotion</i>	21
2.14	<i>JD-GUI</i>	21
BAB III METODOLOGI PENELITIAN		22

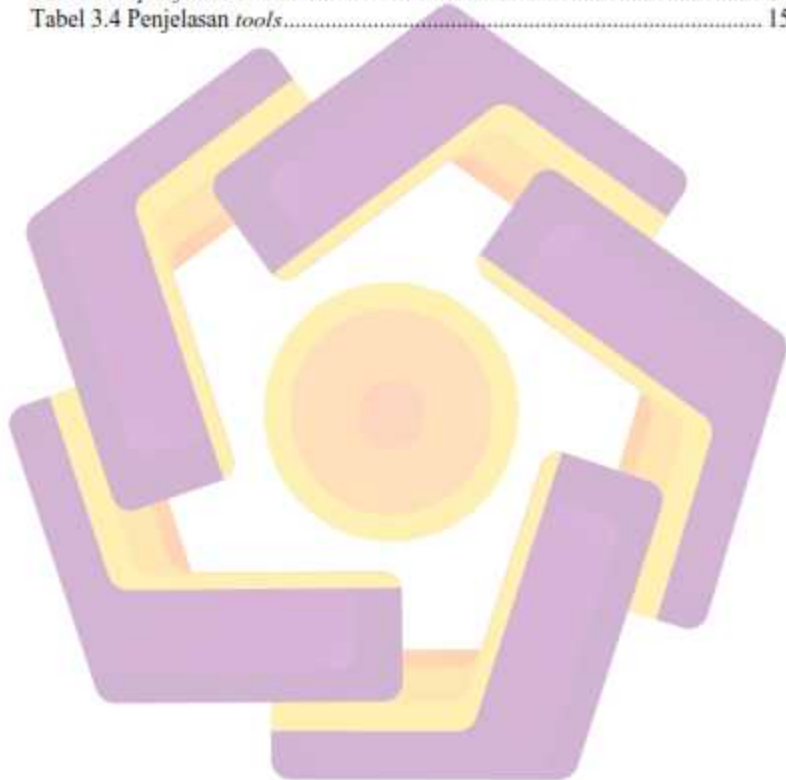
3.1	Gambaran Umum Penelitian.....	22
3.2	Malware dan Aplikasi yang dianalisis.....	22
3.3	Solusi yang diusulkan.....	22
3.4	Alat dan Bahan Penelitian.....	22
3.4.1	Perangkat Keras (<i>Hardware</i>).....	23
3.4.2	Perangkat Lunak (<i>Software</i>).....	23
3.5	Metode penelitian.....	24
3.5.1	Pre-Experimental Design.....	24
3.5.2	One Group <i>Pretest Posttest</i> Design.....	24
3.5.3	Pengumpul <i>AN</i> Data.....	25
3.5.4	Perancangan dan Simulasi.....	25
3.5.5	Dokumentasi.....	25
3.5.6	<i>Flowchart</i> Penelitian.....	25
BAB IV HASIL DAN PEMBAHASAN.....		27
4.1	Rancangan Sistem.....	27
4.1.1	Instalasi <i>Virtual Machine Enviroment</i>	27
4.1.2	Setting <i>Network</i>	28
4.1.3	Instalasi <i>Tools</i>	30
4.1.3.1	<i>Apktool</i> 30	
4.1.3.2	<i>JD-GUI</i>	
	Err
	or! Bookmark not defined.	
4.1.3.3	<i>DEX2jar</i>	31
4.2.2	Malware testing: <i>Checksum</i> Sample <i>Malware</i>	31
4.2	<i>Decompil</i> e <i>t</i> Aplikasi.....	33
4.3	<i>Permission analysis</i>	34
4.4	Analisis Souce Code.....	38
4.5	Pengujian Sistem.....	40
4.5.1	Demonstrasi Add <i>Virtual Devices</i> pada <i>Genymotion</i>	40
4.5.2	Demostrasi Setting <i>Network</i> pada <i>Device Genymotion</i>	45
4.6	Pengujian Sistem.....	49

4.6.1 Demonstrasi	49
BAB V PENUTUP	51
5.1 Kesimpulan.....	51
5.2 Saran.....	51



DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	1
Tabel 4. 1 Penjabaran <i>Application Permission syssecApp.apk</i>	2
Tabel 3.1 Daftar Solus	13
Tabel 3.2 <i>Spesifikasi Perangkat Keras (Hardware)</i>	14
Tabel 3.3 <i>Spesifikasi Virtual Environment Kali Linux</i>	14
Tabel 3.4 Penjelasan <i>tools</i>	15



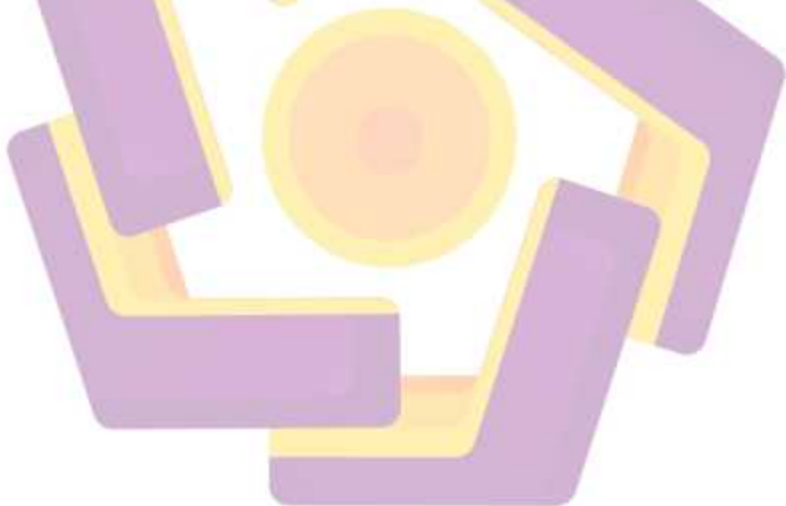
DAFTAR GAMBAR

Gambar 1. 1	Data pengguna ponsel cerdas di dunia	1
Gambar 1. 2	Data serangan <i>mobile</i> aplikasi Q3 2020.....	2
Gambar 1. 3	Data Serangan <i>Trojan Downloader</i> pada Q3 2020	3
Gambar 2.1	Android <i>architecture</i>	15
Gambar 3. 1	Rumus One Group <i>Pretest-Posttest</i> Design.....	25
Gambar 3. 2	<i>Flowchart</i> Penelitian	26
Gambar 4. 1	<i>Import File OVA Kali-linux-2020.1-vbox-amd64</i>	27
Gambar 4. 2	Proses <i>Impor File OVA</i> di <i>VirtualBox</i>	28
Gambar 4. 3	<i>Bridged Adapter Virtual enviroment Kali Linux</i>	28
Gambar 4. 4	Konfigurasi <i>Network Kali linux</i>	29
Gambar 4. 5	Konfigurasi <i>Name Resolver</i>	29
Gambar 4.4	<i>File Apktool</i>	30
Gambar 4.5	Memberi hak akses.....	30
Gambar 4.6	Inisiasi perintah <i>Git Clone</i> pada <i>tools JD-GUI</i>	30
Gambar 4.7	<i>Instalasi JD-GUI</i>	31
Gambar 4.8	<i>Instalasi DEX2jar</i>	31
Gambar 4.9	Hasil scan menggunakan <i>VirusTotal</i>	32
Gambar 4.10	<i>Checksum</i> aplikasi <i>syssecApp.apk</i>	32
Gambar 4.11	Proses <i>Decompile</i> <i>syssecApp.apk</i>	33
Gambar 4.12	Hasil <i>Decompile</i> <i>syssecApp.apk</i>	33
Gambar 4.13	<i>Application Permission syssecApp.apk</i>	34
Gambar 4.14	<i>Decompile file Java</i> menggunakan <i>JD-GUI</i>	38
Gambar 4.15	<i>class</i> yang pertama di <i>JAM</i> kan oleh sebuah aplikasi	39
Gambar 4.16	<i>Class</i> yang di panggil dari <i>OnAlarmReceiver</i>	39
Gambar 4.17	<i>class</i> yang berfungsi sebagai <i>host</i>	40
Gambar 4.18	fungsi <i>class</i> data yang diambil	40
Gambar 4.19	<i>Add Virtual Devices</i>	41
Gambar 4.20	<i>Devices Samsung Galaxy S10</i>	41
Gambar 4.21	Pengaturan <i>Name, Display, dan System</i> pada <i>Devices</i>	42
Gambar 4.22	Pengaturan <i>Android System options</i> dan <i>Network mode</i>	42
Gambar 4.23	Prose <i>Instalasi Devices</i>	43
Gambar 4.24	<i>Start Device</i>	43
Gambar 4.25	<i>Starting virtual device</i>	43
Gambar 4.26	<i>Homepage Device</i>	44
Gambar 4.27	<i>Icon WiFi</i>	45
Gambar 4.28	Pengaturan <i>SSID AndroidWiFi</i>	46
Gambar 4.29	<i>Network Details AndroidWiFi</i>	47
Gambar 4.30	<i>IP Setting Device</i>	48
Gamabr 4.31	Runing aplikasi <i>syssecApp.apk</i> di <i>emulator</i>	49

INTISARI

Kemajuan pesat telah dicapai dalam pengembangan teknologi smartphone berbasis Android. Komunikasi, belanja, dan transaksi keuangan hanyalah beberapa dari tugas sehari-hari yang dilakukan orang dengan smartphone mereka. Android, di sisi lain, adalah sistem operasi open-source yang memudahkan siapa saja untuk membuat aplikasi Android yang dapat diakses melalui smartphone. Menghitung aplikasi yang disematkan malware oleh application, salah satunya adalah malware. Analisis dilakukan dengan sample *malware Trojan* pada aplikasi *syssecApp.apk* dengan menggunakan metode *reverse engineering*, dalam melakukan *reverse engineering malware Trojan* menggunakan tools *APKTOOL*, *JD-GUI*. Penelitian ini akan melakukan analisa terhadap sebuah aplikasi *syssecApp.apk* yang terinfeksi *malware Trojan* dengan menggunakan metode *reverse engineering*. Hasil dari analisis pada aplikasi *syssecApp.apk* ditemukan adanya ip host penerima yang terdapat pada source code didalam *syssecApp.apk*

Kata kunci: Android, APK, Malware, Reverse engineering



ABSTRACT

Rapid progress has been made in the development of Android-based smartphone technology. Communication, shopping and financial transactions are just a few of the daily tasks that people perform with their smartphones. Android, on the other hand, is an open-source operating system that makes it easy for anyone to create Android apps that can be accessed via a smartphone. Counting applications embedded with malware by application, one of which is malware. The analysis was carried out with samples of Trojan malware in the `syssecApp.apk` application using the reverse engineering method, in doing Trojan malware reverse engineering using APKTOOL tools, JD-GUI. This research will analyze the `syssecApp.apk` application that infects Trojan malware using the reverse engineering method. The results of the analysis on the `syssecApp.apk` application found that there is an ip host receiver contained in the source code in `syssecApp.apk`.

Keywords: Android, APK, Malware, Reverse engineering

