

**ANALISIS STATIK KEAMANAN MENGGUNAKAN MOBILE  
SECURTY FRAMEWORK (MOBSF) PADA APLIKASI  
MODIFIKASI (MOD) BERBASIS ANDROID**

**SKRIPSI**

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



disusun oleh

**ARDIANSYAH**

**20.83.0505**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2025**

**ANALISIS STATIK KEAMANAN MENGGUNAKAN MOBILE SECURITY  
FRAMEWORK (MOBSF) PADA APLIKASI MODIFIKASI (MOD)  
BERBASIS ANDROID**

**SKRIPSI**

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



disusun oleh  
**ARDIANSYAH**  
**20,83.0505**

Kepada

**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS AMIKOM YOGYAKARTA**  
**YOGYAKARTA**  
**2025**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS STATIK KEAMANAN MENGGUNAKAN MOBILE SECURITY  
FRAMEWORK (MOBSF) PADA APLIKASI MODIFIKASI (MOD)  
BERBASIS ANDROID**

yang disusun dan diajukan oleh

**Ardiansyah**

**20.83.0505**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 17 September 2025

**Dosen Pembimbing,**



**Joko Dwi Santoso, M.Kom.**  
**NIK. 190302181**

**HALAMAN PENGESAHAN**  
**SKRIPSI**  
**ANALISIS STATIK KEAMANAN MENGGUNAKAN MOBILE SECURITY**  
**FRAMEWORK (MOBSF) PADA APLIKASI MODIFIKASI (MOD)**  
**BERBASIS ANDROID**

yang disusun dan diajukan oleh

**ARDIANSYAH**

**20.83.0505**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 17 September 2025

**Susunan Dewan Penguji**

**Nama Penguji**

Seni Destya, S.T., M.KOM.  
NIK. 190302312

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

Dr. Dony Ariyus, S.S., M.Kom.  
NIK. 190302128

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 17 September 2025

**DEKAN FAKULTAS ILMU KOMPUTER**



**Prof. Dr. Kusrini, M.Kom**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ardiansyah  
NIM : 20.83.0505

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS STATIS KEAMANAN MENGGUNAKAN MOBILE SECURITY  
FRAMEWORK (MOBSF) PADA APLIKASI MODIFIKASI (MOD)  
BERBASIS ANDROID**

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, 17 September 2025

Yang Menyatakan,



Ardiansyah

## HALAMAN PERSEMBAHAN

Penulis mengucapkan terimakasih yang sebesar-besarnya kepada semua pihak yang terlibat yang telah memberikan dukungan, bimbingan, dan motivasi selama penulisan karya akademik ini. Pada kesempatan kali ini penulis menyampaikan terimakasih setulus-tulusnya kepada:

1. Allah Swt. yang telah melimpahkan rahmat dan karunia dalam bentuk apapun, sehingga dilancarkan dan diberikan kemudahan dalam segala urusan yang penulis hadapi, terutama dalam proses penyampaian skripsi ini.
2. Kedua orang tua saya dan kakak-kakak saya yang mendoakan, melimpahkan rasa kasih sayang, selalu memberikan nasehat, motivasi, bimbingan dan dukungan kepada saya tanpa berhenti, karena tanpa mereka saya bukanlah apa-apa.
3. Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang telah memberikan arahan, bimbingan, kritik dan saran selama proses penyusunan hingga penyelesaian naskah skripsi ini.
4. Seluruh teman dan sahabat yang telah memberikan dukungan kepada saya.
5. Diri saya sendiri yang telah berusaha dengan baik untuk mengerjakan skripsi ini hingga selesai.



## KATA PENGANTAR

Alhamdulillah, Puji dan Syukur kita panjatkan kepada Allah Subhanahu Wata'ala. Allhamdulillah atas segala pertolong, Rahmat, dan kasi sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Statis Keamanan Menggunakan Mobile Security Framework (MOBSF) Pada Aplikasi Modifikasi (MOD) Berbasis Android” Segala puji hanya bagi Allah SWT yang telah memberikan penulis kesempatan, kesehatan, dan kemudahan dalam menyelesaikan studi di perguruan tinggi ini.

Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan, dan nasehat dari berbagai pihak selama penyusunan skripsi ini. Pada kesempatan kali ini penulis menyampaikan terimakasih setulus-tulusnya kepada:

1. Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang telah memberikan arahan, bimbingan, kritik dan saran selama proses penyusunan hingga penyelesaian naskah skripsi ini..
2. Kedua orang tua saya dan kakak-kakak saya yang mendoakan, melimpahkan rasa kasih sayang, selalu memberikan nasehat, motivasi, bimbingan dan dukungan kepada saya tanpa berhenti, karena tanpa mereka saya bukanlah apa-apa.
3. Seluruh teman dan sahabat yang telah memberikan dukungan kepada saya. Seluruh teman dan sahabat yang telah memberikan dukungan kepada saya.
4. Pihak lain yang membantu, baik langsung maupun tidak langsung, dalam proses penyusunan skripsi ini.

Akhir kata penulis menyadari bahwa tidak ada yang sempurna, penulis masih melakukan kesalahan dalam penyusunan skripsi ini. Oleh karena itu, penulis meminta maaf yang sedalam-dalamnya atas kesalahan yang dilakukan penulis.

Peneliti berharap semoga skripsi ini dapat bermanfaat bagi pembaca dan dijadikan refensi demi pengembangan ke arah lebih baik. Kebernaran datangnyadari Allah SWT dan kelesahan dating dari diri penulis. Semoha Allah SWT senantiasa melimpahkan Rahmat dan Ridho-Nya kepada kita semua

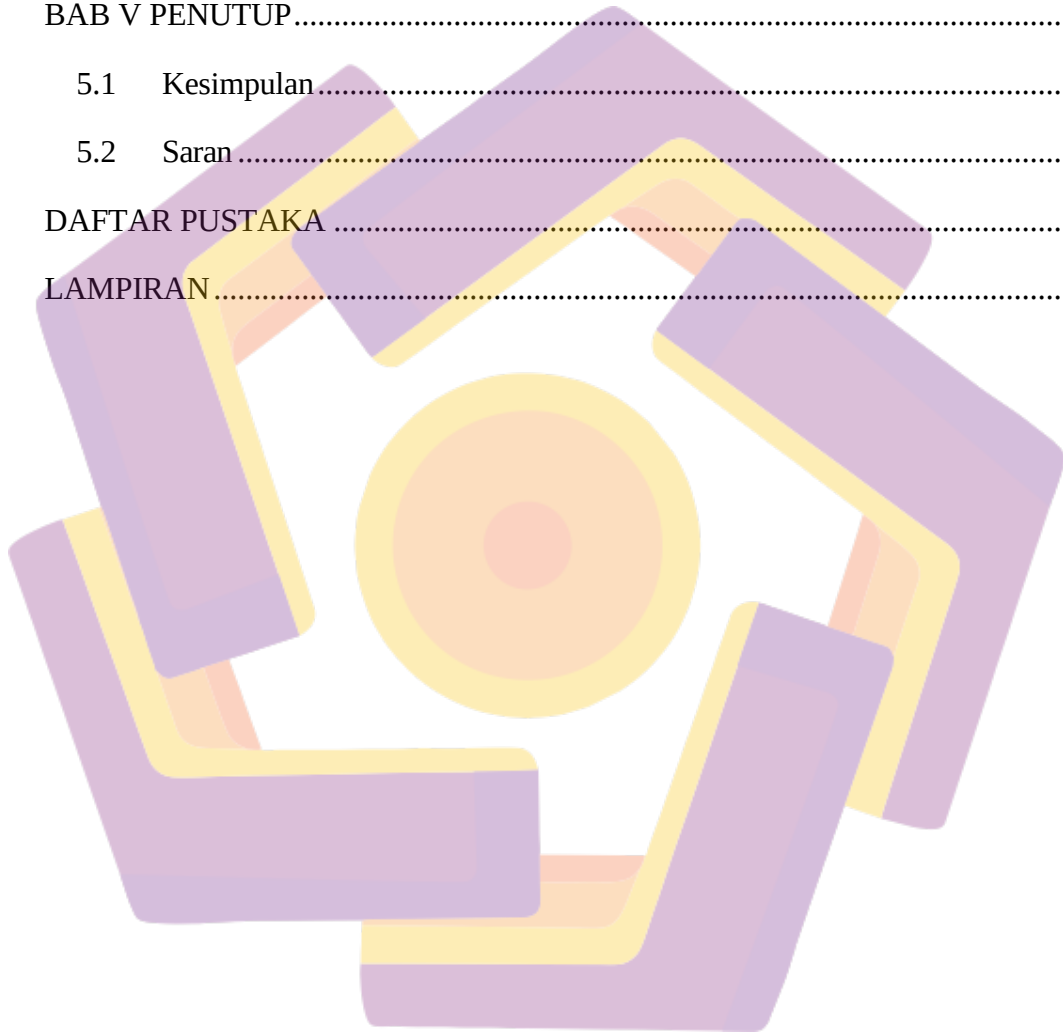
## DAFTAR ISI

|                                   |      |
|-----------------------------------|------|
| HALAMAN JUDUL .....               | i    |
| HALAMAN PERSETUJUAN.....          | ii   |
| HALAMAN PERSEMBAHAN .....         | v    |
| KATA PENGANTAR .....              | vi   |
| DAFTAR ISI.....                   | vii  |
| DAFTAR TABEL.....                 | x    |
| DAFTAR GAMBAR.....                | xi   |
| DAFTAR LAMPIRAN.....              | xiii |
| DAFTAR LAMBANG DAN SINGKATAN..... | xiv  |
| DAFTAR ISTILAH .....              | xv   |
| INTISARI.....                     | xvi  |
| ABSTRACT.....                     | xvii |
| BAB I PENDAHULUAN .....           | 1    |
| 1.1 Latar Belakang.....           | 1    |
| 1.2 Rumusan Masalah .....         | 3    |
| 1.3 Batasan Masalah.....          | 3    |
| 1.4 Tujuan Penelitian.....        | 3    |
| 1.5 Manfaat Penelitian .....      | 3    |
| 1.6 Sistematika Penulisan .....   | 3    |
| BAB II TINJAUAN PUSTAKA.....      | 5    |
| 2.1 Studi Literatur.....          | 5    |
| 2.2 Digital Forensik .....        | 11   |
| 2.3 Mobile Forensik.....          | 11   |
| 2.4 Android.....                  | 11   |



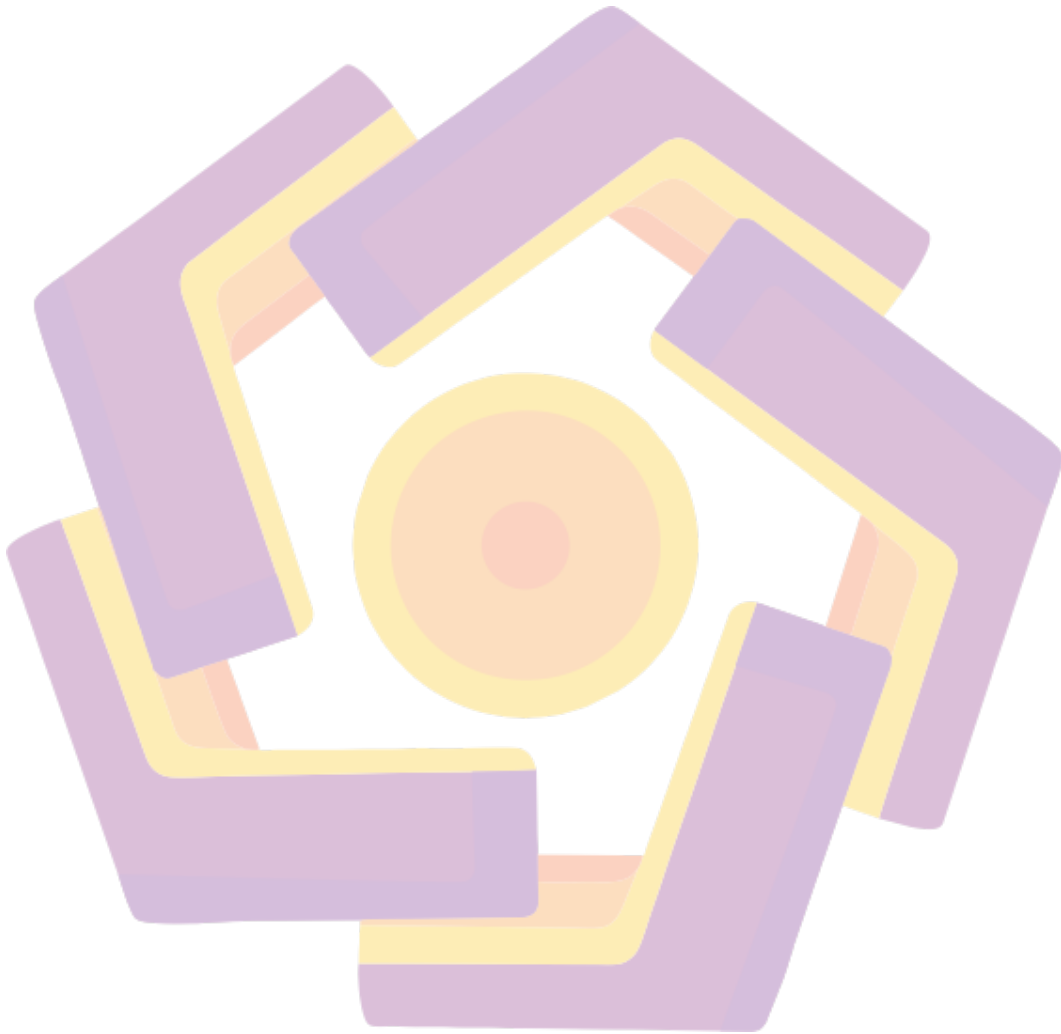
|                                |                                                                    |    |
|--------------------------------|--------------------------------------------------------------------|----|
| 2.5                            | Aplikasi Modifikasi .....                                          | 11 |
| 2.6                            | Mobile Security Framework (MobSF) .....                            | 12 |
| 2.7                            | Analisis Statik.....                                               | 14 |
| 2.8                            | Dangerous Permission .....                                         | 14 |
| 2.9                            | Weak Crypto.....                                                   | 14 |
| 2.10                           | SLL bypass .....                                                   | 15 |
| 2.11                           | Root Detection.....                                                | 15 |
| 2.12                           | Domain Malware Check.....                                          | 15 |
| BAB III METODE PENELITIAN..... |                                                                    | 16 |
| 3.1                            | Objek Penelitian .....                                             | 16 |
| 3.2                            | Alur Penelitian.....                                               | 16 |
| 3.2.1                          | Rumusan masalah.....                                               | 18 |
| 3.2.2                          | Studi Literatur .....                                              | 18 |
| 3.2.3                          | Persiapan .....                                                    | 18 |
| 3.2.4                          | Pengujian.....                                                     | 18 |
| 3.2.5                          | Pembahasan.....                                                    | 19 |
| 3.2.6                          | Kesimpulan .....                                                   | 19 |
| 3.3                            | Kebutuhan Hardware.....                                            | 19 |
| 3.4                            | Kebutuhan Software .....                                           | 20 |
| BAB IV .....                   |                                                                    | 21 |
| 4.1                            | Persiapan.....                                                     | 21 |
| 4.1.1                          | Persiapan Sampel Aplikasi Modifikasi (MOD) .....                   | 21 |
| 4.1.2                          | Persiapan Konfirmasi <i>Mobile Security Framework</i> (MOBSF)..... | 21 |
| 4.2                            | Pengujian .....                                                    | 23 |
| 4.2.1                          | Pengujian Sampel Aplikasi Menggunakan MobSF .....                  | 23 |
| 4.2.2                          | Dangerous Permission.....                                          | 25 |

|                      |                            |    |
|----------------------|----------------------------|----|
| 4.2.3                | Weak Crypo .....           | 41 |
| 4.2.4                | SLL Bypass.....            | 51 |
| 4.2.5                | Root Detection .....       | 52 |
| 4.2.6                | Domain Malware Check ..... | 53 |
| 4.3                  | Hasil pengujian .....      | 56 |
| BAB V PENUTUP.....   |                            | 59 |
| 5.1                  | Kesimpulan.....            | 59 |
| 5.2                  | Saran .....                | 59 |
| DAFTAR PUSTAKA ..... |                            | 60 |
| LAMPIRAN.....        |                            | 63 |



## DAFTAR TABEL

|                                                            |    |
|------------------------------------------------------------|----|
| Tabel 3. 1 kebutuhan <i>Hardware</i> .....                 | 19 |
| Tabel 3. 2 kebutuhan <i>Software</i> .....                 | 20 |
| Tabel 4. 1 Informasi Sampel aplikasi Modifikasi (MOD)..... | 21 |
| Tabel 4. 2 Hasil Analisis Statik Menggunakan Mobsf .....   | 56 |



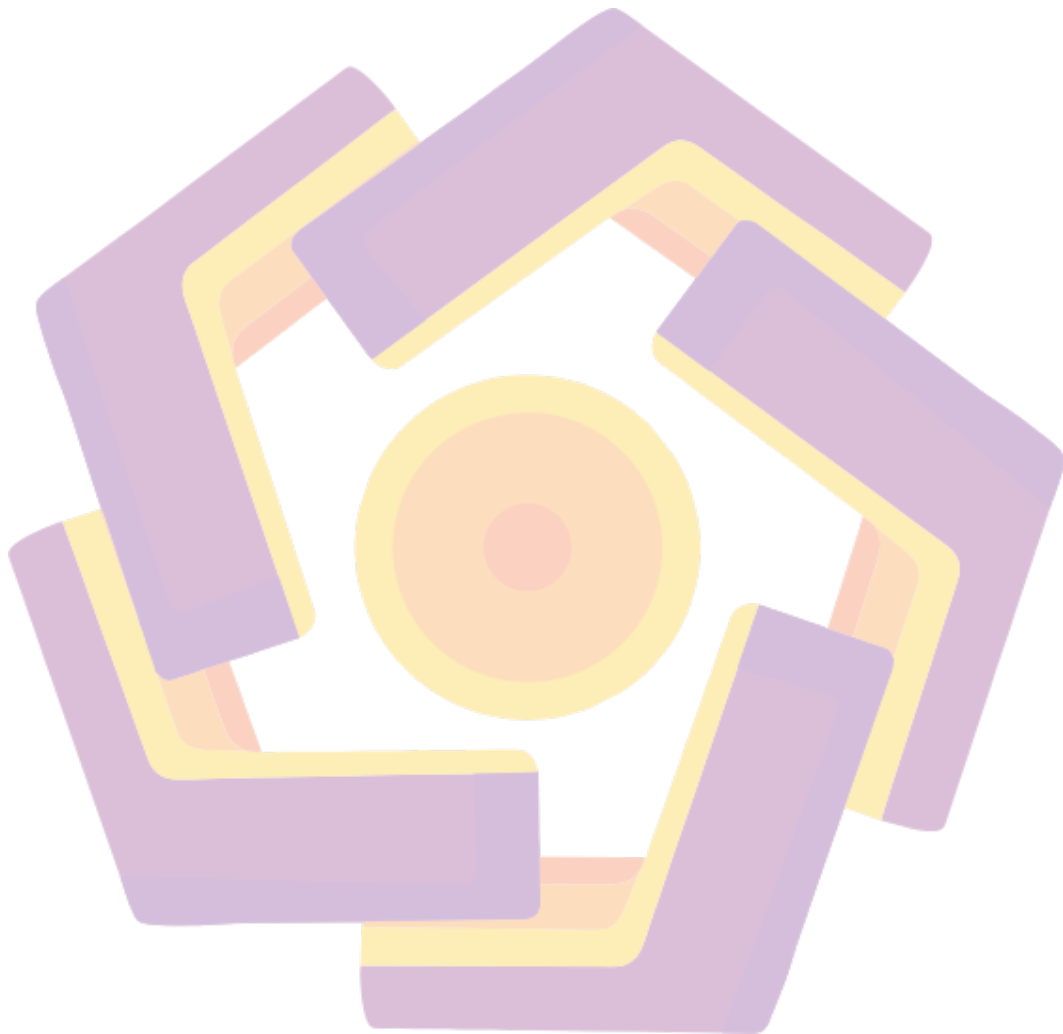
## DAFTAR GAMBAR

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Gambar 3.1 Alur Penelitian                                                    | 17 |
| Gambar 3. 2 Alur Diagram Dari MobSF                                           | 19 |
| Gambar 4.1 Sampel aplikasi modifikasi                                         | 21 |
| Gambar 4.2 Berhasil menginstall docker.io                                     | 22 |
| Gambar 4.3 Berhasil melakukan Pull image Dicker MobSF                         | 22 |
| Gambar 4.4 Berhasil menjalan MobSf                                            | 23 |
| Gambar 4.5 Tampilan aplikasi MobSf yang berhasil dijalankan                   | 23 |
| Gambar 4.6 Hasil Pengujian MobSF Pada Aplikasi whastapp Modifikasi            | 24 |
| Gambar 4.7 Hasil Pengujian MobSF Pada Aplikasi Spotify Modifikasi             | 24 |
| Gambar 4.8 Hasil Pengujian Mobsf Pada Aplikasi Subway Surfers Modifikasi      | 25 |
| Gambar 4. 9 Analisis WhastApp Modifikasi Bagian Application Permissions       | 26 |
| Gambar 4.10 Analisis WhastApp Modifikasi Bagian Application Permissions       | 27 |
| Gambar 4.11 Analisis WhastApp Modifikasi Bagian Application Permissions       | 28 |
| Gambar 4.12 Analisis WhastApp Modifikasi Bagian Application Permissions       | 28 |
| Gambar 4.13 Analisis WhastApp Modifikasi Bagian Application Permissions       | 29 |
| Gambar 4.14 Analisis WhastApp Modifikasi Bagian Application Permissions       | 29 |
| Gambar 4.15 Analisis WhastApp Bagian Modifikasi Application Permissions       | 30 |
| Gambar 4.16 Analisis WhastApp Modifikasi Bagian Application Permissions       | 30 |
| Gambar 4.17 Analisis WhastApp Modifikasi Bagian Application Permissions       | 31 |
| Gambar 4.18 Analisis WhastApp Bagian Modifikasi Application Permissions       | 31 |
| Gambar 4.19 Analisis Spotify Modifikasi Bagian Application Permissions        | 35 |
| Gambar 4 20 Analisis Spotify Modifikasi Bagian Application Permissions        | 36 |
| Gambar 4.21 Analisis Spotify Modifikasi Bagian Application Permissions        | 37 |
| Gambar 4.22 Analisis Spotify Modifikasi Bagian Application Permissions        | 38 |
| Gambar 4.23 Analisis Spotify Modifikasi Bagian Application Permissions        | 38 |
| Gambar 4.24 Analisis Subway Surfers Modifikasi Bagian Application Permissions | 40 |
| Gambar 4 25 Analisis Subway Surfers Modifikasi Bagian Application Permissions | 41 |

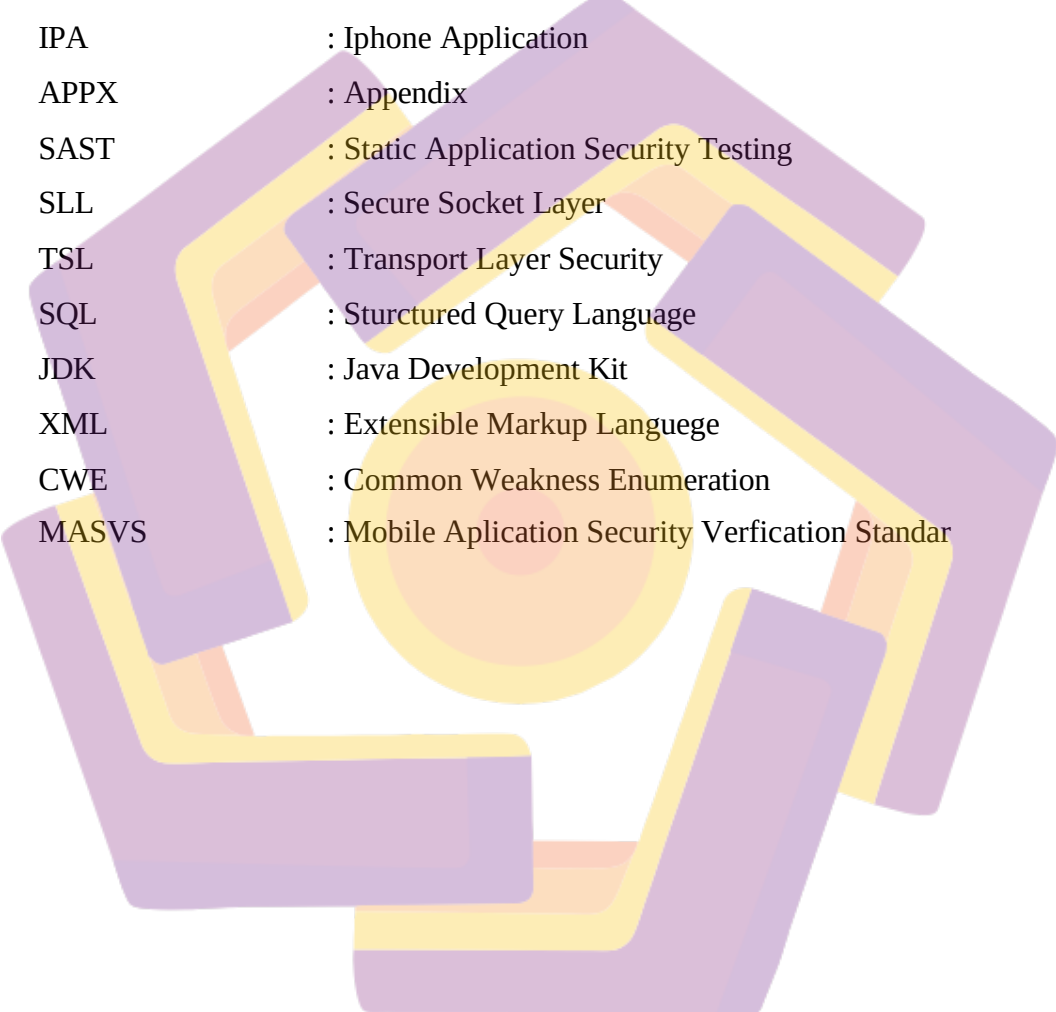
|                                                                      |    |
|----------------------------------------------------------------------|----|
| Gambar 4.26 Analisis whastapp Modifikasi Bagian Code Analysis        | 42 |
| Gambar 4. 27 Analisis WhastApp Modifikasi Bagian Code Analysis       | 42 |
| Gambar 4.28 Analisis Spotify Modifikasi Bagian Code Analysis         | 45 |
| Gambar 4.29 Analisis Spotify modifikasi Bagian Code Analysis         | 45 |
| Gambar 4. 30 Analisis Subway Surfers Modifikasi Bagian Code Analysis | 47 |
| Gambar 4. 31 Analisis Subway Surfers Modifikasi Bagian Code Analysis | 48 |
| Gambar 4.32 Analisis WhastApp Modifikasi Bagian Url                  | 51 |
| Gambar 4.33 Analisis Spotify Modifikasi Bagian Url                   | 51 |
| Gambar 4.34 Analisis Subway Surfers Modifikasi Bagian Url            | 52 |
| Gambar 4.35 Analisis WhastApp Modifikasi Bagian Root Detection       | 52 |
| Gambar 4.36 Analisis Subway Surfers Modifikasi Bagian Root Detection | 53 |
| Gambar 4.37 Analisis Subway Surfers Modifikasi Bagian Root Detection | 53 |
| Gambar 4.38 Analisis WhastApp Modifikasi Bagian Root Detection       | 54 |
| Gambar 4.39 Analisis Spotify Modifikasi Bagian Root Detection        | 55 |
| Gambar 4.40 Analisis Subway Surfers Modifikasi Bagian Root Detection | 56 |

## DAFTAR LAMPIRAN

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Lampiran 1 Hasil pengujian ketiga aplikasi modifikasi menggunakan Mobsf | 63 |
| Lampiran 2 semua hasil data ketiga aplikasi modifikasi:                 | 63 |



## DAFTAR LAMBANG DAN SINGKATAN

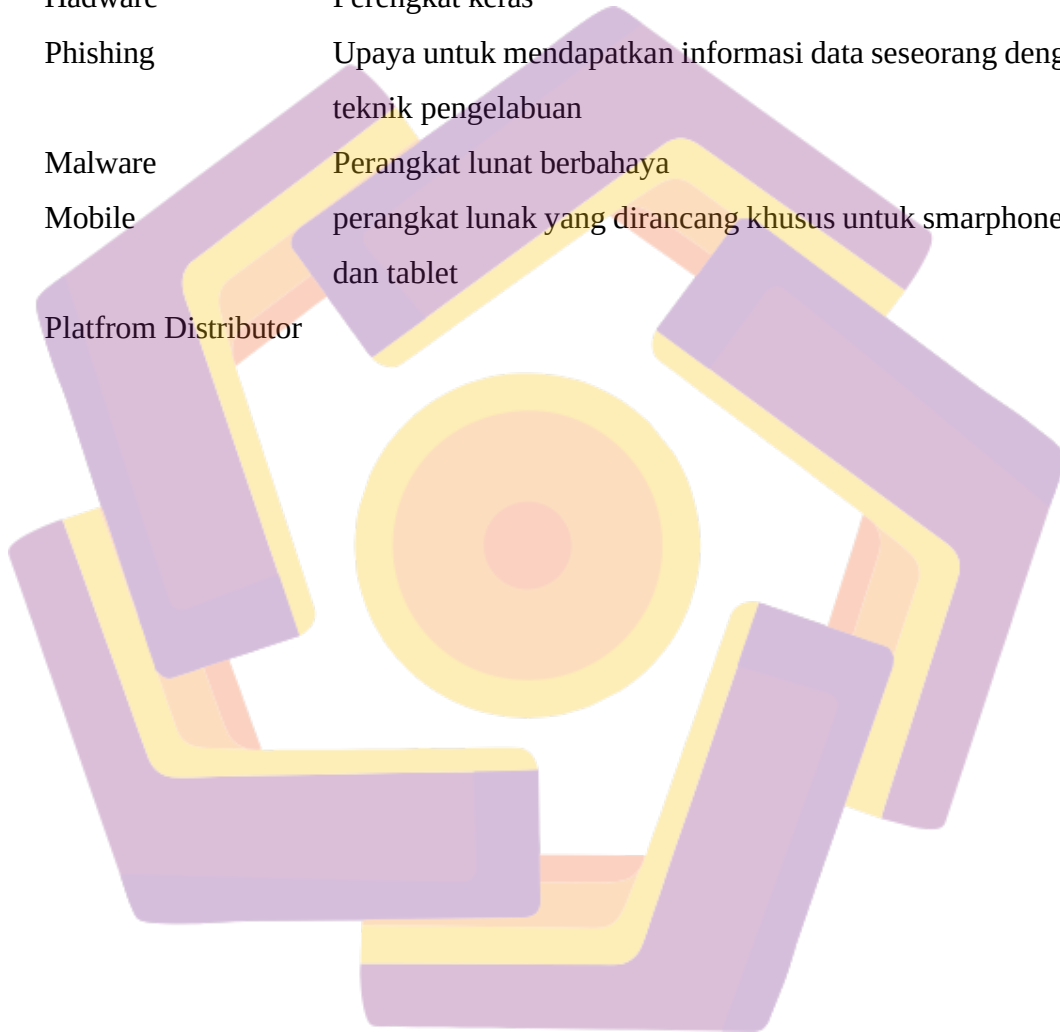


|         |                                                  |
|---------|--------------------------------------------------|
| (MOBSF) | : Mobile Sccurity framework                      |
| MOD     | : Modifikasi                                     |
| GPS     | : Global Positioning Sytem                       |
| APK     | : Android Package Kit                            |
| IPA     | : Iphone Application                             |
| APPX    | : Appendix                                       |
| SAST    | : Static Application Security Testing            |
| SLL     | : Secure Socket Layer                            |
| TSL     | : Transport Layer Security                       |
| SQL     | : Sturctured Query Language                      |
| JDK     | : Java Development Kit                           |
| XML     | : Extensible Markup Languagee                    |
| CWE     | : Common Weakness Enumeration                    |
| MASVS   | : Mobile Aplication Security Verfication Standar |



## DAFTAR ISTILAH

|                      |                                                                            |
|----------------------|----------------------------------------------------------------------------|
| Open-soucer          | Jenis perangkat lunak yang kode sumbernya terbuka untuk dipelajari.        |
| Software             | Peangkat lunak                                                             |
| Hadware              | Perangkat keras                                                            |
| Phishing             | Upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan |
| Malware              | Perangkat lunat berbahaya                                                  |
| Mobile               | perangkat lunak yang dirancang khusus untuk smarphone dan tablet           |
| Platfrom Distributor |                                                                            |



## INTISARI

Dalam era digital yang semakin berkembang pesat, penggunaan perangkat *mobile* dan aplikasi berbasis *android* telah menjadi bagian tidak terpisahkan dari kehidupan masyarakat. Dalam beberapa tahun terakhir, penggunaan aplikasi *mobile* meningkat dalam berbagai bidang kehidupan masyarakat.

Hal tersebut menyebabkan munculnya banyak masalah dan ancaman privasi dan mendorong para peretas untuk melakukan kejahatan siber. Salah satunya pada aplikasi modifikasi (MOD) yang menyediakan fitur tambahan atau menghilangkan batasan dari aplikasi asli. Aplikasi ini sering kali disusupi malware atau virus, yang dapat menggancam keamanan data pengguna. Aplikasi modifikasi (MOD) yang sering diunduh dan digunakan untuk mendapatkan fitur tambahan secara gratis. Aplikasi mod tersebut memiliki resiko yang tinggi terhadap keamanan karena tidak melalui proses pemeriksaan yang ketat seperti aplikasi di *Google play store*.

Penelitian bertujuan untuk melakukan analisis statik keamanan menggunakan *mobile security famework* (MOBSF) pada aplikasi modifikasi dengan parameter analisis yang digunakan yaitu *dangerous permissions*, *weak crypto*, *root detection*, *SSI bypass*. Pengujian dilakukan pada ketiga aplikasi modifikasi yaitu *whatsapp modifikasi*, *spotify modifikasi*, dan *subway surfers modifikasi* untuk mengetahui tingkat keamanan dan kerentangan pada aplikasi modifikasi. Hasil dari pengujian tersebut mendapat keamanan yang relatif sama. Pada aplikasi *whatsapp modifikasi* memiliki skor keamanan 49, aplikasi *spotify modifikasi* memiliki skor keamanan 50, aplikasi *subway surfers modifikasi* memiliki skor keamanan 40. Pada ketiga aplikasi terdapat celah keamanan karena memiliki *dangerous permissions*, *weak crypto*, *root detection*

**Kata kunci:** Analisis Statik, keamanan aplikasi, android, aplikasi MOD.

## **ABSTRACT**

*In the rapidly growing digital era, the use of mobile devices and android-based applications has become an integral part of people's lives. In recent years, the use of mobile applications has increased in various areas of people's lives.*

*This has led to the emergence of many privacy issues and threats and encouraged hackers to commit cyber crimes. One of them is modified apps (MODs) that provide additional features or remove limitations from the original app. These apps are often infiltrated with malware or viruses, which can threaten the security of user data. Modified apps are often downloaded and used to get additional features for free. The mod application has a high risk of security because it does not go through a rigorous inspection process like the application in the Google play store.*

*The research aims to perform static security analysis using the mobile security framework (MOBSF) on modified applications with the analysis parameters used, namely dangerous permissions, weak crypto, root detection, SSI bypass. Tests were carried out on three modified applications, namely modified whastapp, modified spotify, and modified subway surfers to determine the level of security and vulnerability in modified applications. The results of the test got relatively the same security. The modified whastapp application has a security score of 49, the modified sporify application has a security score of 50, the modified subway surfers application has a security score of 40. In all three applications there are security gaps because they have dangerous permissions, weak crypto, and root detection.*

**Keyword:** Static analysis, application security, android, MOD application