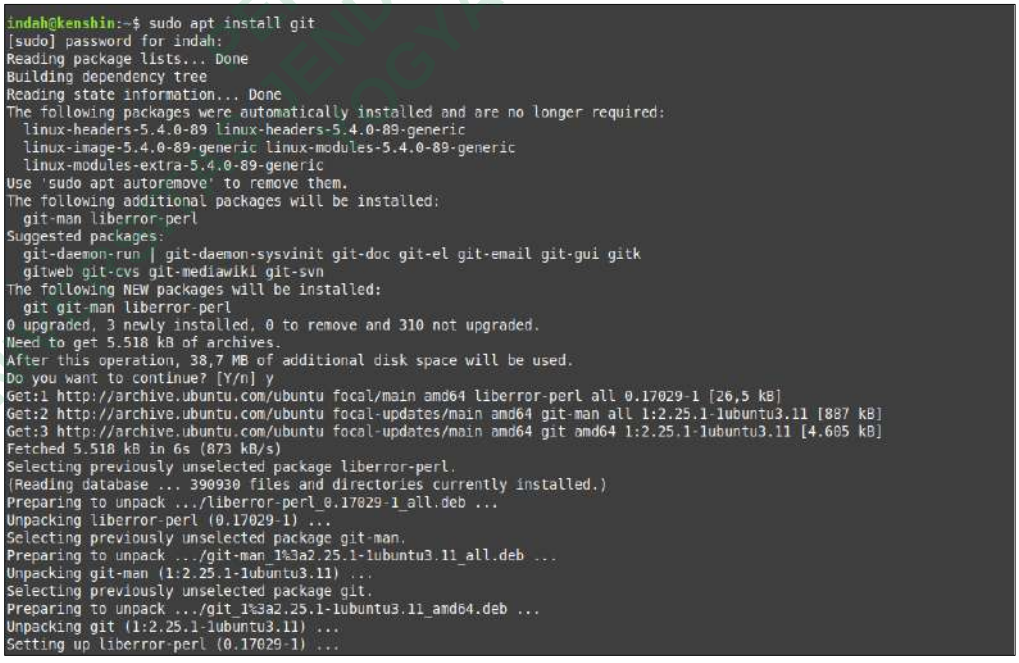
BAB 4
HASIL PENELITIAN

4.1 INSTALASI MOBILE SECURITY FRAMEWORK

Proses pertama yang dilakukan pada penelitian yaitu menginstal *Mobile Security Framework* pada laptop sebagai tempat pengujian aplikasi. *Mobile Security Framework* dapat diunduh melalui https://github.com/MobSF/Mobile-Security-Framework-MobSF. Berikut ini adalah langkah-langkah menginstal *Mobile Security Framework* di Linux Mint.

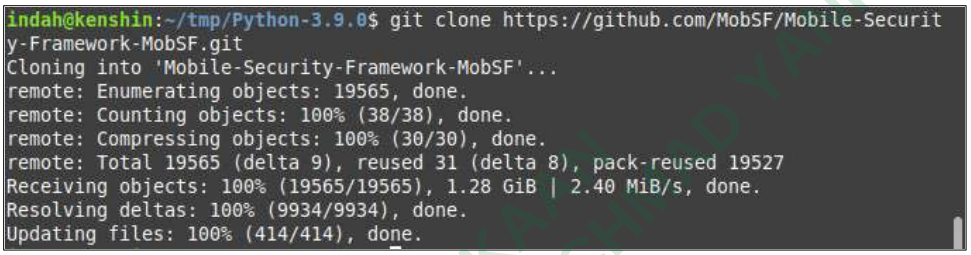
1. Langkah pertama membuka aplikasi Terminal kemudian menjalankan perintah sudo apt install git seperti pada Gambar 4.1. GIT adalah singkatan dari *Group Inclusive Tour*, merupakan kontrol versi yang sering digunakan oleh para pengembang perangkat lunak untuk bekerja sama dalam pembuatan dan pengembangan aplikasi.



Gambar 4.1 Menjalankan Perintah Instal Git

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

2. Langkah kedua menjalankan perintah git clone https://github.com/MobSF/Mobile-Security-Framework MobSF.git seperti pada Gambar 4.2. Istilah "clone" pada konteks ini mengacu pada tindakan menduplikat suatu repositori. Proses clone umumnya dimanfaatkan oleh para pengembang untuk berkolaborasi dalam suatu proyek, sehingga proyek tersebut dapat dikerjakan oleh lebih dari satu orang dan disimpan dalam satu repositori tunggal.



Gambar 4.2 Menduplikat File Respositori MobSF

3. Langkah ketiga mengubah direktori dengan menggunakan perintah cd, kemudian menjalankannya. Perintah cd *(change directory)* digunakan untuk mengubah atau membuka direktori tertentu. Seperti terlihat pada Gambar 4.3. Berikut ini adalah perintah untuk menjalankannya.

   cd Mobile-Security-Framework-MobsF

   ./setup.sh

Gambar 4.3 Membuka Direktori MobSF

4. Langkah keempat memperbarui python ke python3.9 dengan menjalankan perintah sudo apt-get update. *Apt-get update* berperan dalam mengambil "daftar" komponen terkini berdasarkan konfigurasi komponen yang ada pada terminal, seperti pada Gambar 4.4.

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

```
indah@kenshin:~/Mobile-Security-Framework-MobSF$ sudo apt-get update
[sudo] password for indah:
Hit:1 http://packages.microsoft.com/repos/code stable InRelease
Hit:2 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:3 https://desktop-download.mendeley.com/download/apt stable InRelease
Hit:4 http://archive.canonical.com/ubuntu focal InRelease
Hit:5 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:6 http://security.ubuntu.com/ubuntu focal-security InRelease
Ign:7 http://packages.linuxmint.com una InRelease
Hit:8 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:9 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:10 http://packages.linuxmint.com una Release
Get:11 http://ddebs.ubuntu.com focal InRelease [41,3 kB]
Hit:12 http://ddebs.ubuntu.com focal-updates InRelease
Fetched 41,3 kB in 3s (13,1 kB/s)
Reading package lists... Done
```

Gambar 4.4 Mengupdate Sistem

5. Langkah kelima menjalankan perintah mkdir *(make directory)* yang berfungsi untuk membuat folder atau direktori baru. Seperti terlihat pada Gambar 4.5. Berikut ini adalah perintah untuk menjalankannya.

   mkdir -/tmp

   cd -/tmp

   wget https://www.python.org/ftp/python/3.9.0/Python-3.9.0.tgz

   tar -xvzf Python-3.9.0.tgz

```
indah@kenshin:~/Mobile-Security-Framework-MobSF$ mkdir ~/tmp
indah@kenshin:~/Mobile-Security-Framework-MobSF$ cd ~/tmp
indah@kenshin:~/tmp$ wget https://www.python.org/ftp/python/3.9.0/Python-3.9.0.tgz
--2023-11-01 21:16:52--  https://www.python.org/ftp/python/3.9.0/Python-3.9.0.tgz
Resolving www.python.org (www.python.org)... 199.232.44.223, 2a04:4e42:48::223
Connecting to www.python.org (www.python.org)|199.232.44.223|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 26724009 (25M) [application/octet-stream]
Saving to: 'Python-3.9.0.tgz'

Python-3.9.0.tgz     100%[===================>]  25,49M  2,51MB/s    in 10s

2023-11-01 21:17:02 (2,48 MB/s) - 'Python-3.9.0.tgz' saved [26724009/26724009]

indah@kenshin:~/tmp$ tar -xvzf Python-3.9.0.tgz
Python-3.9.0/
Python-3.9.0/CODE_OF_CONDUCT.md
Python-3.9.0/README.rst
Python-3.9.0/Doc/
Python-3.9.0/Doc/howto/
Python-3.9.0/Doc/howto/pyporting.rst
```

Gambar 4.5 Membuat Direktori Baru

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

6. Langkah keenam menjalankan perintah konfigurasi, instalasi kemudian mengaksesnya pada web browser. *Configure / ifconfig* merupakan perintah untuk mengkonfigurasi jaringan pada server atau untuk memeriksa informasi jaringan yang sedang aktif. Seperti terlihat pada Gambar 4.6. Berikut ini adalah perintah untuk menjalankannya.

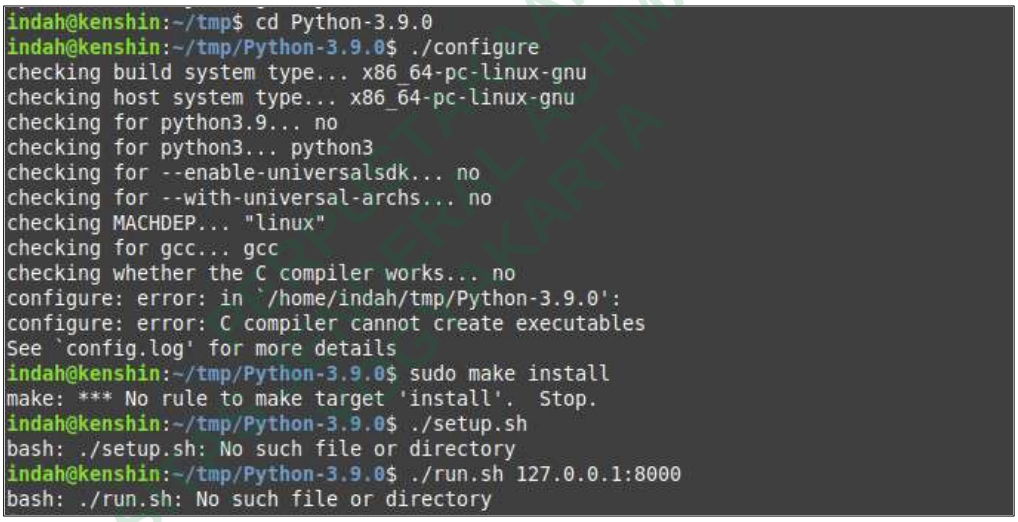
   cd Python-3.9.0

   ./configure

   sudo make install

   ./setup.sh

   ./run.sh 127.0.0.1:8000



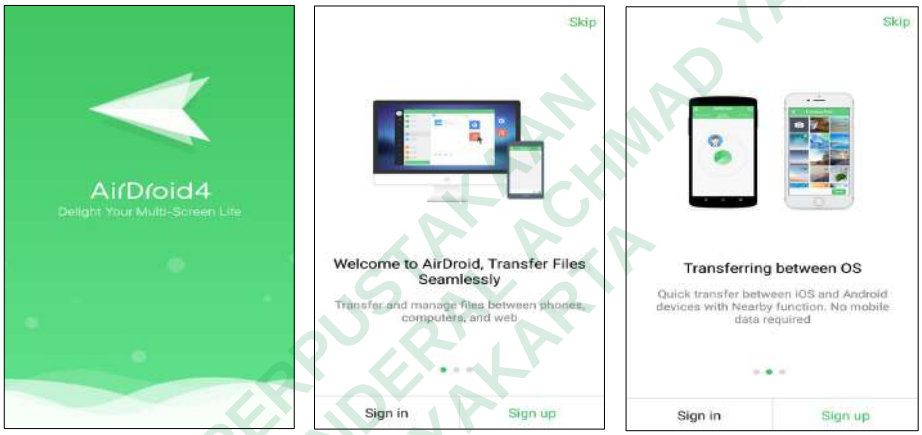
Gambar 4.6 Menjalankan Perintah Konfigurasi

UNIVERSITAS ... AHMAD YANI YOGYAKARTA

4.2 MENGEKSTRAK APLIKASI GAME BOOSTER MENGGUNAKAN AIRDROID

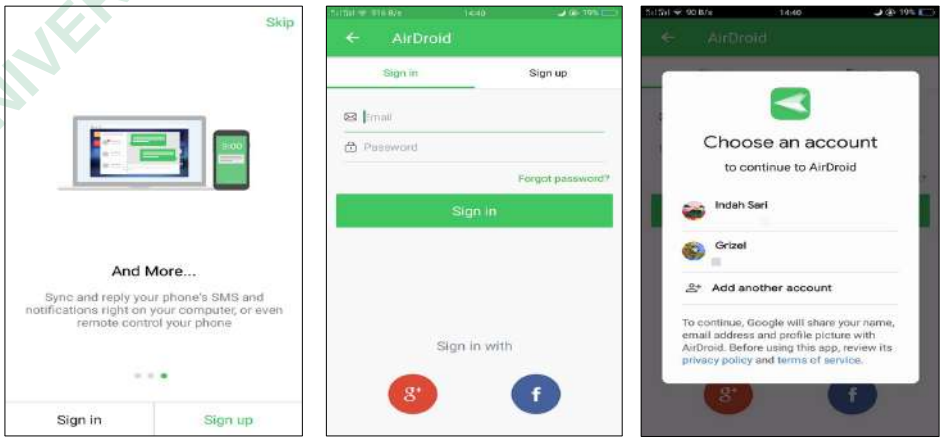
Proses kedua yang dilakukan pada penelitian yaitu mengekstrak file aplikasi *Game Booster* di laptop. Aplikasi *Airdroid* dapat diunduh melalui https://play.google.com/store/apps/details?id=com.sand.airdroid&hl=id
Berikut ini adalah langkah-langkahnya.

1. Instal aplikasi *Game Booster* pada perangkat Android.
2. Instal aplikasi *AirDroid* pada perangkat Android, lalu buka aplikasi kemudian ikuti proses menggunakannya, seperti terlihat pada Gambar 4.7



Gambar 4.7 Tampilan Awal Beranda Aplikasi

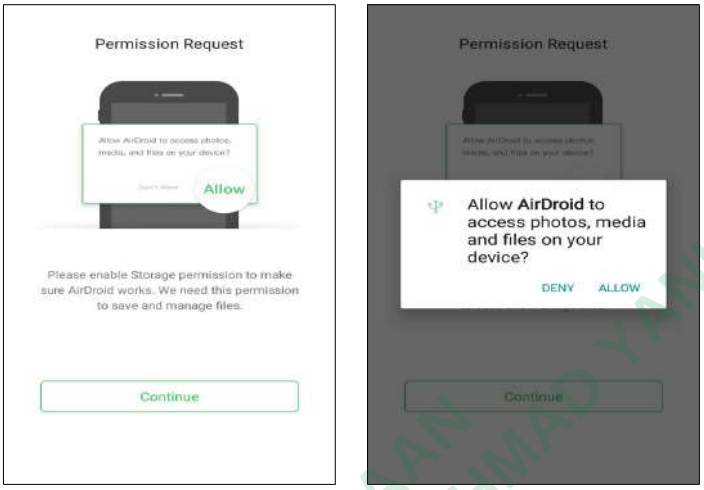
3. Klik tombol *Sign in* di kolom kiri bawah, kemudian *login* menggunakan akun *Google*. Seperti terlihat pada Gambar 4.8



Gambar 4.8 Proses Login ke Aplikasi *AirDroid*

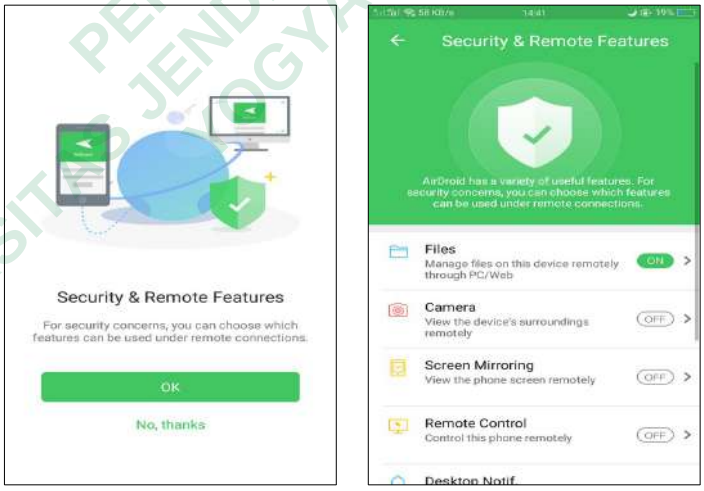
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

4. Klik tombol *Allow* untuk mengizinkan aplikasi *AirDroid* mengakses foto, media dan file pada *device*. Seperti terlihat pada Gambar 4.9



Gambar 4.9 Permintaan Izin Aplikasi *AirDroid*

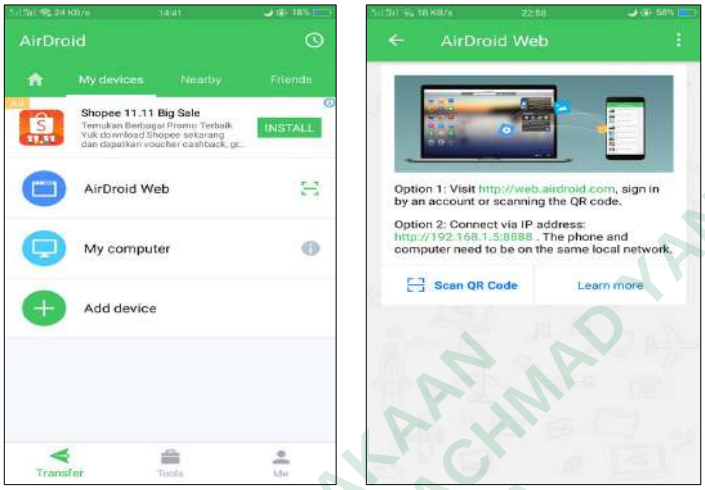
5. Klik tombol Ok untuk mengizinkan aplikasi *AirDroid* mengakses fitur keamanan dan jarak jauh. Seperti terlihat pada Gambar 4.10



Gambar 4.10 Fitur Keamanan dan Jarak Jauh

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

6. Pada halaman beranda klik ikon *AirDroid Web*, kemudian hubungkan aplikasi *AirDroid* dengan laptop melalui akses internet. Dengan mengunjungi http://web.airdroid.com. Seperti terlihat pada Gambar 4.11



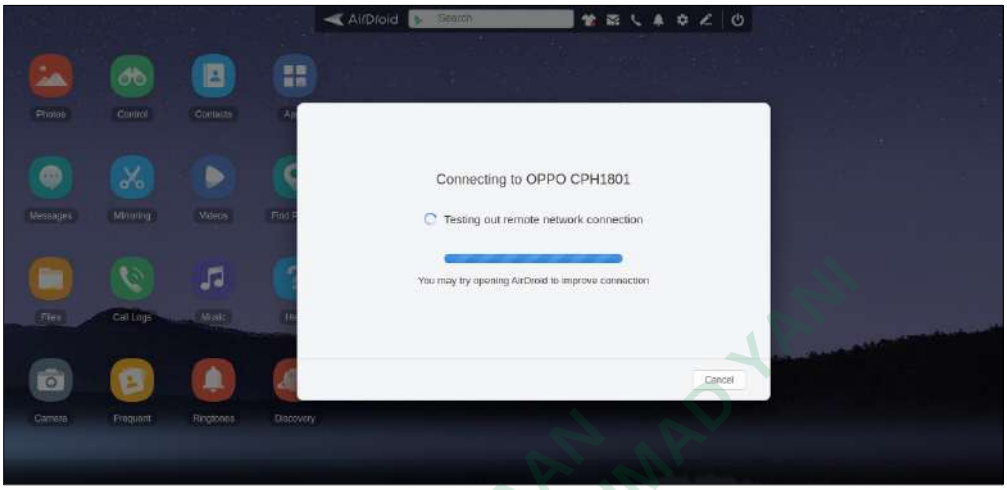
Gambar 4.11 Menghubungkan Aplikasi *AirDroid* ke Laptop

7. Setelah website terbuka masukan *email* dan juga *password* kemudian klik *sign in* atau bisa langsung menggunakan *Scan QR Code.* Seperti terlihat pada Gambar 4.12

Gambar 4.12 Tampilan Login *Airdroid Web*

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

8. Pada tahap ini menunggu proses *loading* hingga selesai. Seperti terlihat pada gambar 4.13



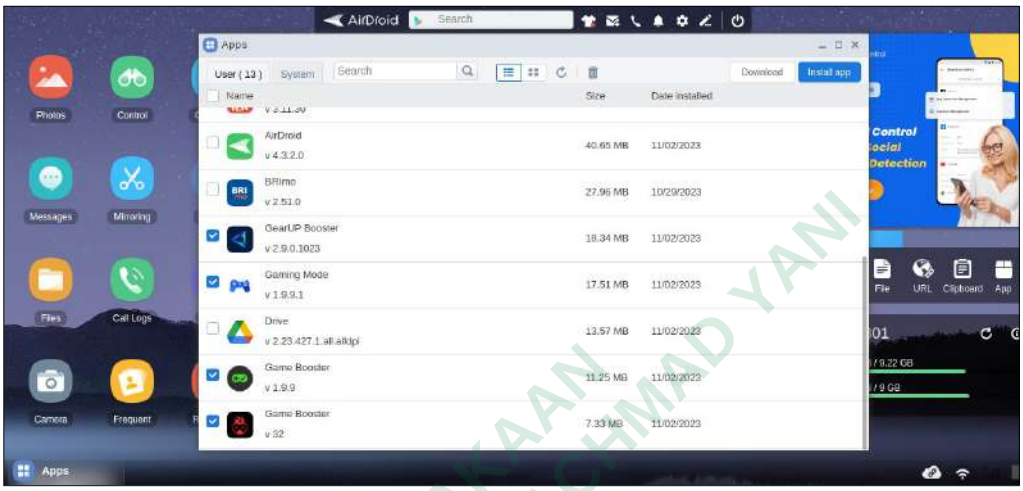
Gambar 4.13 Proses loading *AirDroid Web*

9. Setelah halaman berhasil terbuka klik ikon *Apps.* Seperti terlihat pada Gambar 4.14

Gambar 4.14 Tampilan Beranda *AirDroid Web*

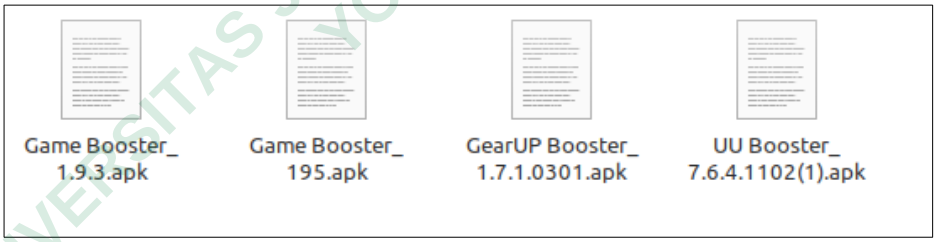
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

10. Kemudian cari aplikasi *Game Booster*, lalu centang pada kolom yang disediakan. Klik tombol *download*, tunggu hingga proses selesai. Seperti terlihat pada Gambar 4.15



Gambar 4.15 Proses Mendownload Aplikasi *Game Booster*

11. Berikut ini adalah file APK *Game Booster* yang berhasil di *download* dan siap di uji coba pada *Mobile Security Framework.* Seperti terlihat pada Gambar 4.16



Gambar 4.16 File APK *Game Booster*

4.2.1 Hasil Extraksi Aplikasi Game Booster

Berikut ini merupakan hasil ekstraksi aplikasi *Game Booster* yang terdokumentasi pada Tabel 4.1. Didapatkan hasil berupa nama aplikasi, nama file, nama paket, nama/kode versi aplikasi, ukuran file, serta target/minimum SDK. Nama paket merupakan ruang nama Java yang digunakan untuk kode dalam modul tersebut. Ruang nama dimasukkan sebagai atribut paket dalam file *manifest*

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

modul Android. Sistem Android menggunakan nilai *version code* untuk mencegah penggunaan APK dengan *version code* lebih rendah daripada versi yang sedang terpasang di perangkat, sehingga menghindari terjadinya *downgrade.*

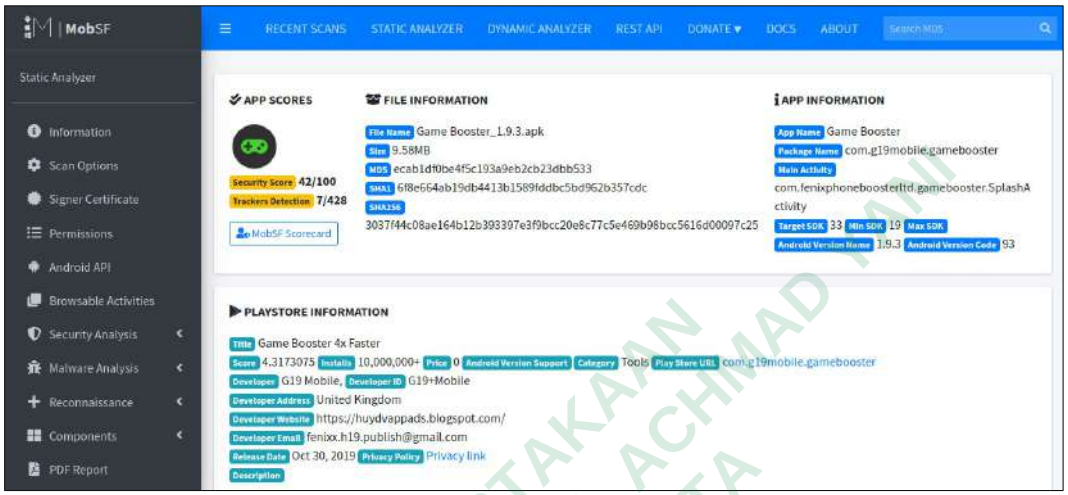
Tabel 4.1 Hasil Extraksi Aplikasi *Game Booster*

No	App	File Name	Package Name	Version Name/Code	File Size	Target/ Minimum SDK
1	Game Booster 4x Faster	Game Booster_1.9.3.apk	com.g19mobile.gamebooster	1.9.3/93	9.58 MB	33/19
2	Game Booster Fire GFX-Lag Fix	Game Booster_195.apk	com.booster.gameboostermega	195/195	7.02 MB	33/19
3	GearUp Game Booster: Lower Lag	GearUP Booster_1.7.1.0301.apk	com.gearup.booster	1.7.1.0301/38	10.9 MB	33/21
4	UU Game Booster-Lower Lag	UU Booster_7.6.4.1102(1).apk	com.netease.uu	7.6.4.1102/661	12.13 MB	33/21

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

4.3 HASIL PENGUJIAN

Analisis dilakukan dengan cara mengunggah file APK *Game Booster* ke *Mobile Security Framework*, tunggu hingga proses analisis selesai. Pada Gambar 4.17 memperlihatkan hasil analisis aplikasi *Game Booster 4x Faster.*



Gambar 4.17 Hasil Analisis Aplikasi *Game Booster 4x Faster*

Pada bagian Skor Aplikasi berisi:

1. Skor Keamanan diberi peringkat 42/100 yang berarti memiliki resiko sedang.
2. Deteksi Pelacak diberi peringkat 7/428 yang berarti memiliki 7 pelacak.

Pada Informasi File, nama filenya adalah Game Booster_1.9.3.apk dengan ukuran file sebesar 9.58 MB. Informasi yang diidentifikasi dalam aplikasi:

1 Nama aplikasinya adalah *Game Booster* dengan nama paketnya adalah com.g19mobile.gamebooster.

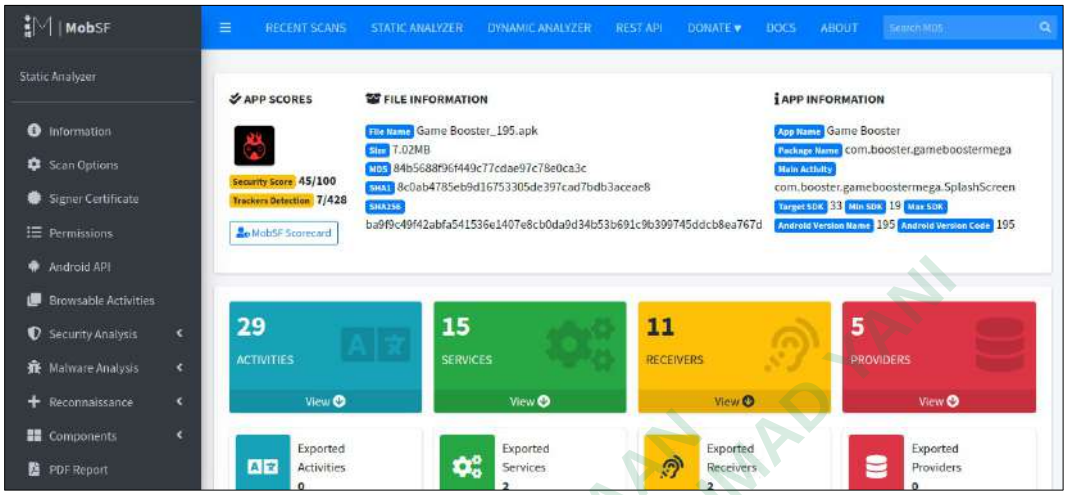
2 Aktivitas utama di com.fenixphoneboosterltd.gamebooster.SplashActivity

3 *Software Development Kit* (SDK) merupakan rangkaian alat perangkat lunak yang terinstal dalam satu paket. SDK target merujuk pada versi yang dirancang agar bisa menjalankan aplikasi, yaitu 33. SDK minimum merupakan versi terendah yang di jalankan oleh aplikasi, yaitu 19 dan tidak memiliki batasan maksimum untuk SDK.

4 Nama/Kode versi Android adalah 1.9.3/93.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Pada Gambar 4.18 memperlihatkan hasil analisis dari aplikasi *Game Booster Fire GFX-Lag Fix* di *Mobile Security Framework (MobSF).*



Gambar 4.18 Hasil Analisis Apikasi *Game Booster Fire GFX-Lag Fix*

Pada bagian Skor Aplikasi berisi:

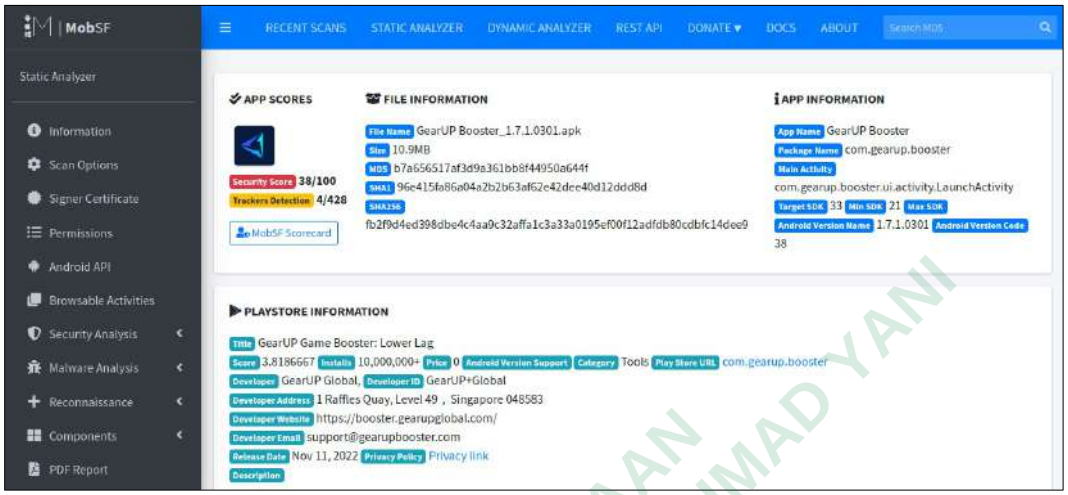
1. Skor Keamanan diberi peringkat 45/100 yang berarti memiliki resiko sedang.
2. Deteksi Pelacak diberi peringkat 7/428 yang berarti memiliki 2 pelacak.

Pada Informasi File, nama filenya adalah Game Booster_195.apk dengan ukuran file sebesar 7.02 MB. Informasi yang diidentifikasi dalam aplikasi:

1. Nama aplikasinya adalah *Game Booster* dan nama paketnya adalah com.booster.gameboostermega.
2. Aktifitas utama di com.booster.gameboostermega.SplashScreen.
3. SDK target yaitu 33, SDK minimum 19 dan tidak memiliki SDK max.
4. Nama/Kode versi Android adalah 195/195.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Pada Gambar 4.19 memperlihatkan hasil analisis dari aplikasi *GearUp Game Booster: Lower Lag* di *Mobile Security Framework (MobSF).*



Gambar 4.19 Hasil Analisis Aplikasi *GearUp Game Booster: Lower Lag*

Pada bagian Skor Aplikasi berisi:

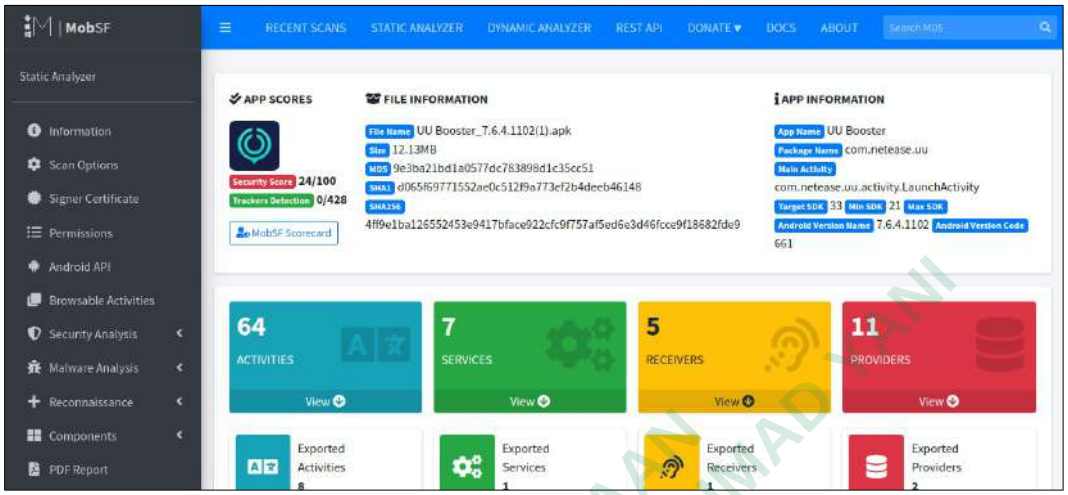
1. Skor Keamanan diberi peringkat 38/100 yang berarti memiliki resiko sedang.
2. Deteksi Pelacak diberi peringkat 4/428 yang berarti memiliki 4 pelacak.

Pada Informasi File, nama filenya adalah GearUP Booster_1.7.1.0301.apk dengan ukuran file sebesar 10.9 MB. Informasi yang diidentifikasi dalam aplikasi:

1. Nama aplikasinya adalah *GearUP Booster* dengan nama paketnya com.gearup.booster.
2. Aktivitas utama di com.gearup.booster.ui.activity.LaunchActivity.
3. SDK target yaitu 33, SDK minimum 21 dan tidak memiliki SDK max.
4. Nama/Kode versi Android adalah 1.7.1.0301/38.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Pada Gambar 4.20 memperlihatkan hasil analisis dari aplikasi *UU Game Booster-Lower Lag* di *Mobile Security Framework (MobSF).*



Gambar 4.20 Hasil Analisis Aplikasi *UU Game Booster-Lower Lag*

Pada bagian Skor Aplikasi berisi:

1. Skor Keamanan diberi peringkat 24/100 yang berarti memiliki resiko sedang.
2. Deteksi Pelacak diberi peringkat 0/428 yang berarti tidak memiliki pelacak.

Pada Informasi File, nama filenya adalah UU Booster_7.6.4.1102(1).apk dengan ukuran file sebesar 12.13 MB. Informasi yang diidentifikasi dalam aplikasi:

1. Nama aplikasinya adalah *UU Booster* dan nama paketnya adalah com.netease.uu.
2. Aktifitas utama di com.netease.uu.activity.LaunchActivity.
3. SDK target yaitu 33, SDK minimum 21 dan tidak memiliki SDK max.
4. Nama/Kode versi Android adalah 7.6.4.1102/661.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

4.3.1 Weak Crypto

Pada Tabel 4.2 merupakan hasil analisis dari keempat aplikasi *Game Booster* yang telah diuji menggunakan *Mobile Security Framework. Weak Crypto* dapat ditemukan pada bagian *Code Analysis.*

Tabel 4.2 Analisis pada *Weak Crypto*

No	Issue	Severity	Standards	Files
1	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	High	**CWE:** CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-3	e/a/b/a/e/a.java
2	The App uses an insecure Random Number Generator.	Warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	com/applovin/ exoplayer2/h/z.java
3	MD5 is a weak hash known to	Warning	**CWE:** CWE-327: Use of a Broken or	com/bykv/vk/ openvk/component/

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

	have hash collisions.		Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	video/api/f/b.java com/bytedance/sdk/component/utils/e.java com/safedk/android/analytics/a.java
4	SHA-1 is a weak hash known to have hash collisions.	Warning	**CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	com/applovin/impl/sdk/utils/StringUtils.java com/applovin/impl/sdk/utils/n.java com/revenuecat/purchases/common/UtilsKt.java

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Berikut ini merupakan penjelasan dari tabel diatas, hasil diperoleh melalui pengujian yang telah dilaksanakan.

1. High Severity: Aplikasi menggunakan mode enkripsi CBC dengan padding PKCS5/PKCS7 yang rentan terhadap serangan *padding oracle. Mode Cipher Block Chaining* (CBC) adalah metode di mana setiap blok data terkait satu sama lain, dan proses enkripsi dan dekripsi melibatkan *ciphertext* (hasil enkripsi) blok sebelumnya. *Public Key Cryptographic Standard* (PKCS) adalah penambahan data sebelum proses enkripsi pada awal, tengah, atau akhir, dengan menambahkan sejumlah bit tertentu. Pada PKCS5, ini hanya berlaku untuk penyandian blok berukuran 64 bit, sementara PKCS7 dijelaskan dalam RFC 5652. Serangan *padding oracle* digunakan oleh penyerang untuk melakukan enkripsi dan dekripsi tanpa memerlukan kunci. Menurut standar:

- *Common Weakness Enumeration (CWE)* adalah daftar yang menampilkan keberadaan *bug* pada software atau hardware yang berbahaya, terdeteksi CWE-649: Ketergantungan pada kebingungan atau enkripsi input yang relavan dengan keamanan tanpa pemeriksaan Integritas.
- *Open Web Application Security Project (OWASP)* Top 10 adalah panduaan bagi pengembang dan tim keamanan terhadap kerentanan aplikasi web yang dapat dengan mudah diserang dan harus segera diatasi, terdeteksi M5: Kriptografi tidak memadai.
- *OWASP The Mobile Application Security Verification Standard (MASVS)* adalah standar keamanan untuk aplikasi seluler, terdeteksi MSTG-CRYPTO-3 artinya aplikasi menggunakan primitif kriptografi yang sesuai untuk kasus penggunaan tertentu, dikonfigurasi dengan parameter yang mematuhi praktik terbaik industri.

2. Warning Severity
    1. Aplikasi menggunakan Generator Nomor Acak yang tidak aman. *Random Number Generator* (RNG) menghasilkan rangkaian angka atau simbol yang urutannya sulit diprediksi sehingga tampak acak. Menurut standar:
        - *Common Weakness Enumeration (CWE)* terdeteksi CWE-330: Penggunaan nilai acak yang tidak mencukupi.
        - *Open Web Application Security Project (OWASP)* Top 10 terdeteksi M5: Kriptografi yang tidak memadai.
        - *The Mobile Application Security Verification Standard (MASVS)* terdeteksi MSTG-CRYTO-6 artinya semua nilai acak dihasilkan menggunakan generator nomor acak yang cukup aman.

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

2. MD5 adalah hash lemah yang diketahui memiliki tabrakan hash. Tabrakan hash berarti setidaknya dua teks memberikan nilai hash yang sama. *Message Digest Algorithm 5 (MD5)* merupakan fungsi hash kriptografi yang sering digunakan dengan panjang nilai hash sebesar 128-bit. MD5 digunakan untuk memverifikasi login sistem dan menyembunyikan kata sandi yang disimpan dalam database, agar menambah nilai secure yang aman pada sistem. Menurut standar:
   - *Common Weakness Enumeration (CWE)* terdeteksi CWE-327: Penggunaan algoritma kriptografi yang rusak atau berisiko.
   - *Open Web Application Security Project (OWASP)* Top 10 terdeteksi M5: Kriptografi tidak memadai.
   - *The Mobile Application Security Verification Standard* terdeteksi MSTG-CRYPTO-4 artinya aplikasi tidak menggunakan protokol atau algoritma kriptografi yang secara luas dianggap tidak digunakan lagi untuk tujuan keamanan.

3. *Secure Hashing Algorithm* (SHA) adalah fungsi enkripsi yang dirancang khusus oleh lembaga keamanan internet untuk menjaga keamanan data. Pada SHA-1 menghasilkan fungsi hash 160 bit yang panjangnya kurang dari 2^{64} bit, merupakan standar keamanan yang masih rendah. Menurut standar:
   - *Common Weakness Enumeration* (CWE) terdeteksi CWE-327: Penggunaan algoritma kriptografi yang rusak atau beresiko.
   - *Open Web Application Security Project* (OWASP) Top 10 terdeteksi M5: Kriptografi tidak memadai.
   - *The Mobile Application Security Verification Standard* terdeteksi MSTG-CRYPTO-4 artinya aplikasi tidak menggunakan protokol atau algoritma kriptografi yang secara luas dianggap tidak digunakan lagi untuk tujuan keamanan.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

4.3.2 SSL Bypass

Pada Tabel 4.3 merupakan hasil analisis dari keempat aplikasi *Game Booster* yang telah diuji menggunakan *Mobile Security Framework. SSL Bypass* dapat ditemukan pada bagian URLs.

Tabel 4.3 Analisis pada *SSL Bypass*

No	App	URL	File
1	Game Booster 4x Faster	http://play.google.com/store/apps/details?id=	com/fenixphoneboosterltd/gamebooster/c/h.java
2	Game Booster Fire GFX-Lag Fix	https://game-booster-free-fire.firebaseio.com	Android String Resource
3	GearUp Game Booster: Lower Lag	http://www.toponad.com	com/anythink/core/common/k/h.java
4	UU Game Booster-Lower Lag	https://twitter.com/%1$s/status/%2$s https://wap.cmpassport.com/resources/html/contract.html https://e.189.cn/sdk/agreement/content.do?type=main&appkey=&hidetop=true https://ms.zzx9.cn/html/oauth/protocol2.html	Android String Resource

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Pada ke-empat aplikasi *Game Booster* yang telah diuji menggunakan *Mobile Security Framework.* Terdapat URL yang menggunakan protokol jaringan *Hypertext Transfer Protocol (HTTP)* dan *Hypertext Transfer Protocol Secure*

(HTTPS). Pada jaringan HTTPS lebih aman dibandingkan HTTP karena diauntentifikasi oleh teknologi keamanan Internet standar seperti *Secure Socket Layer (SSL). SSL* adalah cara situs web membuat koneksi aman (terenkripsi) antara server web (situs web) dan klien (browser). Pada HTTPS terdapat dua kunci kriptografi yaitu *Private Key* dan *Public Key*. Pada *private key* kunci dikontrol dan disimpan oleh pemilik situs web yang bersifat pribadi. Sedangkan pada *publik key* kunci tersedia bagi siapa saja yang ingin berinteraksi dengan server secara aman. *SSL Bypass* yang menggunakan jaringan HTTP ditemukan pada aplikasi *Game Booster 4x Faster* dan *GearUp Game Booster Lower Lag* bagian Urls. Berikut ini adalah urlnya:

1. http://play.google.com/store/apps/details?id=
2. http://www.topnad.com

4.3.3 Dangerous Permissions

Pada Tabel 4.4 merupakan hasil analisis dari keempat aplikasi *Game Booster* yang telah diuji menggunakan *Mobile Security Framework. Dangerous Permissions* dapat ditemukan pada bagian *Application Permissions.*

Tabel 4.4 Analisis pada *Dangerous Permissions*

No	Permission	Status	Info	Description
1	android.permission .CAMERA	Dangerous	Take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
2	android.permission .GET_TASKS	Dangerous	Retrieve running	Allows application to retrieve information

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

			applications	about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
3	android.permission.POST_NOTIFICATIONS	Dangerous	allows an app to post notifications.	Allows an app to post notifications.
4	android.permission.READ_EXTERNAL_STORAGE	Dangerous	Read external storage contents	Allows an application to read from external storage.
5	android.permission.READ_LOGS	Dangerous	Read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
6	android.permission.READ_MEDIA_IMAGES	Dangerous	Allows reading image files from external storage.	Allows an application to read image files from external storage.
7	android.permission.READ_PHONE_STATE	Dangerous	Read phone state and identity	Allows the application to access the phone features of the device.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

				An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
8	android.permission.SYSTEM_ALERT_WINDOW	Dangerous	Display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
9	android.permission.WRITE_EXTERNAL_STORAGE	Dangerous	Read/modify/ delete external storage contents	Allows an application to write to external storage.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Berikut ini merupakan penjelasan dari tabel diatas, hasil diperoleh melalui pengujian yang telah dilaksanakan.

1. android.permission.CAMERA: Memungkinkan aplikasi menggunakan kamera untuk mengambil foto dan video. Hal ini memungkinkan aplikasi untuk mengumpulkan gambar yang diambil oleh kamera kapan pun.
2. android.permission.GET_TASKS: Aplikasi dapat memperoleh informasi tentang tugas saat ini dan yang baru saja dijalankan. Hal Ini bisa memungkinkan aplikasi berbahaya untuk mengakses informasi pribadi tentang aplikasi lain.
3. android.permission.POST_NOTIFICATIONS: Mengizinkan aplikasi mengirim pemberitahuan.

4. android.permission.READ_EXTERNAL_STORAGE: Memungkinkan aplikasi dapat membaca dari penyimpanan eksternal.
5. android.permission.READ_LOGS: Aplikasi dapat membaca dari berbagai file log sistem. Ini dapat digunakan untuk mengetahui informasi umum tentang pengoperasian ponsel Anda, termasuk informasi pribadi dan pribadi
6. android.permission.READ_MEDIA_IMAGES: Memberi izin pada aplikasi untuk membaca file gambar dari penyimpanan eksternal.
7. android.permission.READ_PHONE_STATE: Memberikan akses aplikasi ke fitur telepon di perangkat. Aplikasi yang diberi izin ini dapat mengidentifikasi nomor telepon dan nomor seri ponsel, mengecek status panggilan, melihat nomor yang terhubung dengan panggilan, dan melakukan fungsi lainnya.
8. android.permission.SYSTEM_ALERT_WINDOW: Memberi kemampuan pada aplikasi untuk menampilkan jendela peringatan sistem. Aplikasi yang berpotensi membahayakan dapat menguasai tampilan layar ponsel sepenuhnya.
9. android.permission.WRITE_EXTERNAL_STORAGE: Memungkinkan aplikasi menulis ke penyimpanan eksternal.

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

4.3.4 Root Detection

Pada Tabel 4.5 merupakan hasil analisis aplikasi *Game Booster Fire GFX-Lag Fix* dan aplikasi *GearUp Game Booster: Lower Lag* yang telah diuji menggunakan *Mobile Security Framework. Root Detection* dapat ditemukan pada bagian *Code Analysis.*

Tabel 4.5 Analisis pada *Root Detection*

No	App	Issue	Severity	Standards	Files
1	Game Booster Fire GFX-Lag Fix	This App may have root detection capabilities.	Secure	**OWASP MASVS:** MSTG-RESILIENCE-1	h6/e. java
2	GearUp Game Booster: Lower Lag	This App may have root detection capabilities.	Secure	**OWASP MASVS:** MSTG-RESILIENCE-1	ec/vs1.java

Pada aplikasi *Game Booster 4x Faster* dan aplikasi *UU Game Booster-Lower Lag* tidak memiliki fitur *root detection* karena tidak ada file atau kode *root detection* dibagian *code analysis.* Pada aplikasi *Game Booster Fire GFX-Lag Fix* dan aplikasi *GearUp Game Booster: Lower Lag* memiliki kemampuan *root detection.* OWASP MASVS: MSTG-RESILIENCE-1 mendeteksi, dan merespon, keberadaan perangkat yang di-rooting atau di-jailbreak dengan memperingatkan pengguna atau menghentikan aplikasi.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

4.3.5 Domain Malware Check

Pada Tabel 4.6 merupakan hasil analisis dari keempat aplikasi *Game Booster* yang telah diuji menggunakan *Mobile Security Framework. Domain Malware* dapat ditemukan pada bagian *Domain Malware Check.*

Tabel 4.6 Analisis pada *Domain Malware Check*

No	App	Domain	Status	Geolocation
1	Game Booster 4x Faster	game-booster-4x-faster-free.firebaseio.com	Ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
2	Game Booster Fire GFX-Lag Fix	game-booster-free-fire.firebaseio.com	Ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
3	GearUp Game Booster: Lower Lag	da.anythinktech.com	Malware	**IP:** 47.241.109.64 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

				View: Google Map
4	UU Game Booster-Lower Lag	wap.cmpassport.com	Ok	**IP:** 120.197.235.27 **Country:** China **Region:** Guangdong **City:** Guangzhou **Latitude:** 23.116671 **Longitude:** 113.250000 **View:** Google Map

Domain Malware Check tidak terdapat pada apikasi *Game Booster 4x Faster, Game Booster Fire GFX-Lag Fix, dan UU Game Booster-Lower Lag* karena semua domain bersatus Ok, artinya domain tersebut tidak diklasifikasikan sebagai malware. Namun, domain malware berikut ada untuk aplikasi *GearUp Game Booster Lower Lag.*

1. URL da.anythinktech.com
2. Alamat IP tidak ditemukan
3. Domain Malicius dengan tag Maltrail

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

4.4 ANALISIS ATAS PENGUJIAN

Dari keempat aplikasi *Game Booster* yang telah diuji mengunakan *Mobile Security Framework*, didapatkan hasil bahwa aplikasi di nilai aman untuk digunakan karena pada lima parameter penelitian *(Weak Crypto, SSL Bypass, Dangerous Permissions, Root Detection, Domain Malware Check)* hanya ada satu kategori yang dapat mengakses perangkat Android yaitu pada aplikasi *UU Game Booster-Lower Lag* di bagian *Dangerous Permissions* dan memiliki *Score Security* yang paling kecil. Seperti terlihat pada Tabel 4.7

Tabel 4.7 Hasil Analisis Statis

No	App	Weak Crypto	SSL Bypass	Dangerous Permissions	Root Detection	Domain Malware Check	Security Score
1	Game Booster 4x Faster	Yes	Yes	Yes	No	Ok	42
2	Game Booster Fire GFX-Lag Fix	Yes	No	Yes	Yes	Ok	45
3	GearUp Game Booster: Lower Lag	Yes	Yes	Yes	Yes	No	38
4	UU Game Booster-Lower Lag	No	No	Yes	No	Ok	24

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA