

# Analisis dan Pengujian Performa *Library Safe Device* Terhadap Emulator Android dan *Fake GPS*

Yiyi Supendi

Program Studi Teknik Informatika, Universitas Langlangbuana, Bandung  
yiyi.supendi@gmail.com

**Abstrak** - Penelitian ini berfokus pada analisa dan pengujian *library safe device* terhadap emulator android dan *fake gps* dengan metodologi pengujian *blackbox testing* dengan *stress test* menggunakan adb monkey. Penelitian ini memakai metode penelitian rekayasa dengan pendekatan observasi, perencanaan, dan implementasi. Tujuan utama dari penelitian ini adalah untuk memperlihatkan hasil efektifitas deteksi emulator android dan *fake gps*. Penelitian ini hanya dilakukan dengan perangkat yang menggunakan sistem operasi Android. Dengan terus berkembangnya teknologi pentingnya validasi terhadap kecurangan yang dilakukan bisa terdeteksi dan bisa mencegah terhadap kecurangan. Melalui Analisa dan pengujian *library safe device* bisa mendeteksi penggunaan *fake gps* dari 5 spesimen tersebut, sedangkan untuk mendeteksi emulator android *library safe device* hanya bisa mendeteksi 1 dari 5 spesimen. Jadi dapat disimpulkan bahwa *library safe device* aman untuk digunakan sebagai validasi penggunaan *fake gps* daripada validasi emulator android.

**Kata Kunci** - Metode penelitian rekayasa, deteksi, *library safe device*, emulator android, *fake gps*, kecurangan, *blackbox testing*, *stress test*, adb monkey, android.

## 1. Pendahuluan

Di dalam pelaksanaan kegiatan, tidak bisa dipungkiri bahwa seseorang bisa saja melakukan kecurangan dalam melakukan kegiatan tersebut. Kecurangan merupakan perbuatan yang dilakukan oleh orang yang ada didalam organisasi maupun tingkah laku untuk mengambil keuntungan bagi dirinya sendiri atau sekelompok golongan tertentu. Hal ini serupa dengan yang diungkapkan oleh Widjaja(2012:1) yang mengidentifikasi *fraud* sebagai suatu pengertian umum dan mencakup beragam cara yang dapat digunakan oleh kecerdikan manusia, yang digunakan dengan cara kekerasan oleh seseorang, untuk mendapatkan suatu keuntungan dari orang lain melalui perbuatan yang tidak benar.

Perkembangan dunia teknologi informasi saat ini semakin cepat memasuki berbagai bidang,

sehingga kini semakin banyak instansi yang berusaha untuk meningkatkan pelayanannya dan melakukan pencegahan terhadap kecurangan yang sangat erat dengan teknologi informasi itu sendiri. Dalam kegiatan ketenagakerjaan terdapat elemen penting, salah satunya adalah absensi karyawan. Karena absensi karyawan menjadi bukti atas kehadiran karyawan dalam suatu pekerjaan, dimana untuk menentukan kinerja bagi karyawan daftar kehadiran menjadi salah satu penentu.

Kegiatan melakukan pengabsenan saat ini masih banyak yang menggunakan sistem absensi manual, yaitu melalui tanda tangan disetiap masuk dan keluar kerja. Sistem tanda tangan ini menjadi sangat tidak efisien karena memiliki kekurangan seperti memberikan kemungkinan besar terjadinya kecurangan dalam mengisi kehadiran. Kecurangan tersebut akan menjadi hal yang menguntungkan bagi seseorang karena mereka bisa saja tidak perlu untuk melakukan pengabsenan, tetapi mereka sudah melakukan absensi. Hal itu akan sangat menghambat proses dalam kegiatan dan merugikan bagi instansi.

Dengan berkembangannya Teknologi Informasi, instansi akan semakin dimudahkan dalam melakukan segala macam proses, salah satu contohnya adalah proses melakukan verifikasi untuk menentukan emulator android dan penggunaan *fake gps*. Hal ini adalah untuk melakukan suatu pencegahan dalam melakukan kecurangan. Untuk itu pada penelitian ini akan mencoba untuk melakukan pengujian terhadap emulator android dan *fake gps* menggunakan *library safe device*.

## 2. METODOLOGI PENELITIAN

### 2.1 Metode Penelitian

Penelitian ini menggunakan metode penelitian rekayasa (*Engineering Research metode*). Berdasarkan pada metode penelitian ini yaitu penelitian rekayasa perangkat lunak, maka pendekatan yang digunakan untuk penelitian ini adalah dengan observasi, perencanaan, dan

implementasi.

Teknik dan cara ini diperlukan untuk mengumpulkan dan mengolah data yang didapat dari lapangan sehingga diharapkan penelitian ini berjalan dengan lancar dan sistematis.. berikut penjelasan dari jenis pendekatan yang digunakan untuk penelitian ini:

1. Observasi yang akan dilakukan adalah mencari beberapa spesimen emulator android untuk dilakukan pengujian menggunakan *library safe device*.
2. Perencanaan dalam melakukan pengujian terhadap spesimen yang sudah ditentukan dari hasil observasi.
3. Implementasi dan penerapan *safe device* ke beberapa spesimen untuk dilihat seberapa efektif dalam melakukan pencegahan dan pendeteksi-an terhadap emulator android dan *fake gps*.

## 2.2 Tahapan Penelitian

### 1. Identifikasi Masalah

Tahapan ini merupakan tahapan dimana peneliti menentukan permasalahan yang akan diteliti. Adapun masalah yang akan diteliti meliputi efektifitas penggunaan *library safe device* pada emulator android, mendeteksi *fake gps*, dan melakukan verifikasi terhadap penggunaan emulator dan *fake gps*. Pada penelitian ini akan menguji dan menganalisis efektifitas penggunaan *library safe device* serta memberikan rekomendasi untuk meningkatkan keamanan dalam sistem yang akan dibuat menggunakan *library safe devices*.

### 2. Studi literatur

Pada tahapan ini peneliti akan melakukan studi Pustaka untuk memahami dasar teori yang terkait dengan penggunaan *library safe device*. Pada tahapan ini juga peneliti akan melakukan studi pada sistem yang menggunakan *library safe device*.

### 3. Metode *Blackbox Testing*

Setelah melakukan studi Pustaka pada tahapan sebelumnya maka langkah selanjutnya adalah melakukan pendeskripsian alat alat atau *tools* yang akan dipakai untuk menguji efektifitas *Library Safe Devices*.

### 4. Identifikasi *Test Objectives*

Pada tahapan ini peneliti akan mengidentifikasi tujuan dari melakukan *stress testing*. Identifikasi ini bisa dibuat dengan membuat daftar pertanyaan yang membantu peneliti untuk membuat keluaran yang diinginkan dari pengujian *stress test* yang dilakukan. Berikut pertanyaan yang diajukan diantaranya :

- a. Apakah emulator android bisa terdeteksi secara terus menerus dalam pengujian ini?
- b. Apakah penggunaan *fake gps* bisa terdeteksi secara terus menerus dalam pengujian ini?

2.

### 5. Identifikasi *workload*

Setelah kita melakukan identifikasi objektif, tahapan selanjutnya yang dilakukan adalah identifikasi *workload*. Skenario *workload* yang dilakukan adalah *stress testing* yang cukup untuk melebihi *threshold limits*. Dengan begitu peneliti dapat mengobservasi apakah *Library Safe Devices* ini akan ada efek dari *stress condition*.

### 6. Membuat *test cases*

Setelah membuat matrik tersebut, peneliti akan membuat dan menjabarkan test case dan hasil yang peneliti ekspektasikan. Berikut scenario test yang akan di uji :

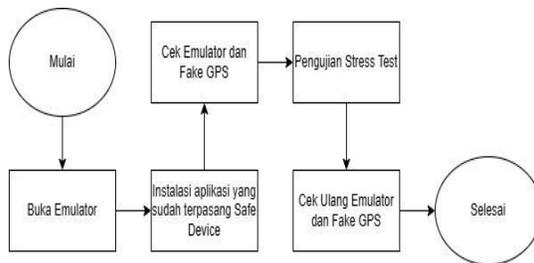
- Workload : 10000 *Events*
  - Durasi tes : sampai tes selesai Ekspektasi hasil :
- Emulator akan tetap terdeteksi sebagai emulator jika aplikasi menggunakan *library safe device*
- Penggunaan *Fake gps* terdeteksi jika pengguna meng install aplikasi *fake gps*

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Analisa Proses Pengujian

Proses pengujian yang akan di laksanakan yaitu bermulai dari instalasi aplikasi yang sudah terpasang *library safe device* terhadap emulator android, setelah itu kita lakukan pengujian pertama, emulator tersebut terdeteksi sebagai emulator atau terdeteksi sebagai perangkat asli, dan emulator tersebut bisa menggunakan *fake gps*. Setelah itu melakukan pengujian *stress test* menggunakan ADB Monkey agar mengetahui apakah *library safe device* tersebut akan tetap bisa mendeteksi emulator dan *fake gps* dengan baik atau tidak.

Gambar 1 Alur Proses Pengujian



#### 3.2 Hasil Pengujian

Hasil pengujian disini menyesuaikan dengan identifikasi matrik yang sudah dibuat di bab 3, dan pengujian akan menggunakan ADB Monkey untuk menentukan *stress test* yang dapat diterima oleh emulator. Setiap emulator akan diuji coba 10000 *events* dan akan dihitung berapa lama emulator tersebut menjalankan 10000 *events* dalam sekali tes.

#### 3.3 Spesimen Pertama

Android emulator yang dicoba pertama kali adalah android emulator yang sudah disediakan oleh google yaitu Android *Virtual Device*. Pada hasil yang di uji coba android emulator ini bisa terdeteksi oleh *library safe device* bahwa android ini adalah emulator dan juga emulator ini terdeteksi bahwa bisa menggunakan *fake GPS*. Pengujian *stress test* yang dilakukan pada emulator ini menjalankan 10000 *events*.

selama 78 detik. Pada saat pengujian tidak terdapat *error* yang membuat aplikasi *library safe device* tertutup atau berhenti mendeteksi, dan *library safe device* menyimpulkan bahwa

Saat pengujian *stress test* emulator ini dapat menyelesaikan pengujian tersebut perangkat ini tidak aman karena perangkat tersebut bisa menggunakan *fake GPS*.

Gambar 2 Spesimen emulator Android Virtual Device



```

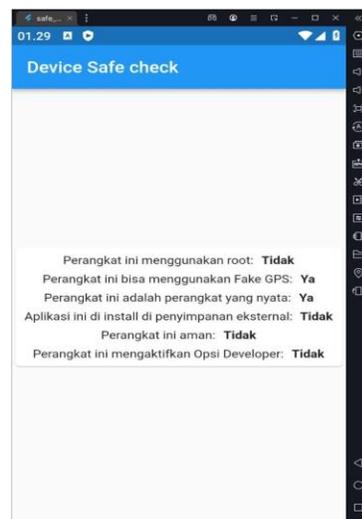
Events injected: 10000
:Sending rotation degree=0, persist=false
:Dropped: keys=10 pointers=1 trackballs=0 flips=27 rotations=
## Network stats: elapsed time=78281ms (0ms mobile, 0ms wifi)
// Monkey finished
    
```

Gambar 3 Hasil Pengujian Spesimen Android Virtual Device

#### 1. Spesimen Kedua

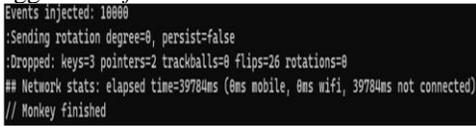
Android emulator yang kedua adalah android emulator LDPlayer. Pada hasil yang di uji coba pada android emulator ini *library safe device* gagal mendeteksi bahwa perangkat ini adalah emulator. Tampilan aplikasi menyatakan bahwa perangkat ini adalah perangkat yang nyata. Tetapi *library safe device* bisa mendeteksi bahwa emulator tersebut bisa menggunakan *fake GPS*.

Gambar 4 Spesimen emulator LDPlayer



Pengujian stress tes pada emulator ini juga menjalankan 10000 *events*. Saat pengujian *stress test* emulator ini dapat menyelesaikan pengujian tersebut selama 39 detik. Pada saat pengujian tidak

terdapat *error* yang membuat aplikasi *library safe device* tertutup atau berhenti berjalan, dan *library safe device* menyimpulkan bahwa perangkat ini tidak aman karena perangkat tersebut bisa menggunakan *fake GPS*.

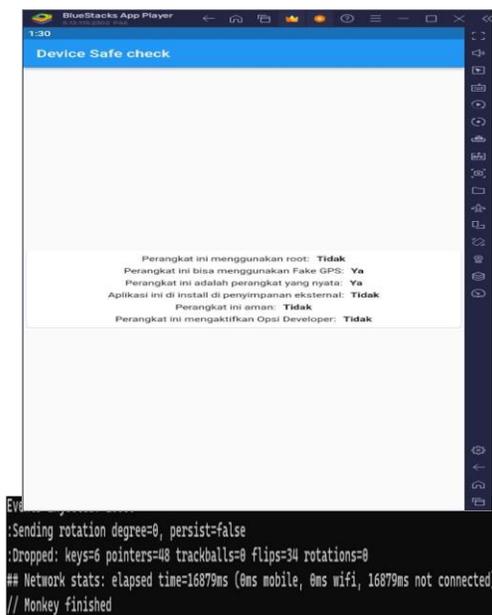


Gambar 5 Hasil Pengujian Spesimen LDPlayer

## 2. Spesimen Ketiga

Android emulator yang ketiga adalah android emulator BlueStack. Pada hasil pengujian terhadap emulator BlueStack aplikasi *library safe device* mendeteksi bahwa perangkat tersebut adalah perangkat nyata, namun nyatanya perangkat tersebut adalah sebuah emulator, dan *library safe device* mendeteksi bahwa perangkat tersebut bisa melakukan *fake GPS*.

Gambar 6 Spesimen emulator BlueStack



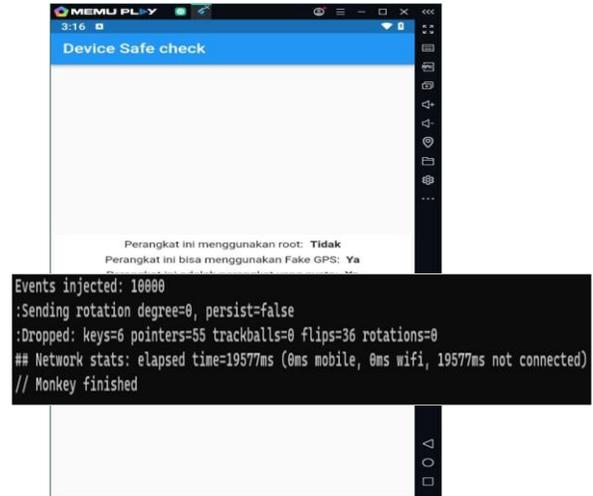
Pada tahap pengujian stress tes emulator ini juga menjalankan 10000 *events*. Namun saat pengujian ternyata emulator tersebut tidak bisa menjalankan *stress test* secara penuh. Emulator tersebut mengalami kegagalan saat menjalani tes, tes tersebut gagal pada detik ke 27 dan gagal saat *events* ke 9205 dari 10000.

## 3. Spesimen Keempat

Android emulator yang keempat adalah android emulator MEmu Play. Pada hasil pengujian terhadap emulator MEmu aplikasi *library safe device* gagal mendeteksi emulator tersebut, yang ditampilkan oleh *library safe device* menyatakan bahwa perangkat tersebut nyata. *Library safe device* bisa mendeteksi perangkat tersebut bisa melakukan *fake GPS*.

Gambar 7 Spesimen Emulator Memu Play

Pada tahap pengujian stress tes emulator ini juga menjalankan 10000 *events*. Emulator ini dapat menyelesaikan *stress test* tersebut dengan sangat cepat, dan berhasil dalam 19 detik. Dalam



pengujian *stress test* ini aplikasi *library safe device* sempat mengalami perubahan perangkat tersebut jadi terdeteksi menjadi perangkat emulator, tetapi tidak bertahan lama setelah itu terganti lagi menjadi perangkat nyata. Aplikasi *library safe device* menyimpulkan bahwa perangkat ini tidak aman karena perangkat tersebut bisa menggunakan *fake GPS*.

Gambar 8 Hasil Pengujian Spesimen MEmu player

## 4. Spesimen Kelima

Android emulator yang keempat adalah android emulator MEmu Player. Pada hasil pengujian terhadap emulator MEmu Player aplikasi *library safe device* gagal mendeteksi emulator tersebut, yang ditampilkan oleh *library safe device* menyatakan bahwa perangkat tersebut nyata. *Library safe device* bisa mendeteksi perangkat tersebut bisa melakukan *fake GPS*.

Gambar 9 Spesimen emulator MEmu Player

Pada tahap pengujian *stress test* emulator ini juga sama seperti yang lain menjalankan 10000 *events*, emulator ini dapat menyelesaikan lebih cepat dibandingkan dengan emulator Memu yaitu berhasil dalam waktu 16 detik. Dalam pengujian *stress test* aplikasi *library safe device* tidak mengalami *error* ataupun kegagalan dalam *test* nya. Aplikasi tersebut pun menyimpulkan bahwa perangkat ini tidak aman karena perangkat bisa menggunakan *fake GPS*.

Gambar 10 Hasil pengujian spesimen Mumu Player



### 3.4 Hasil Matriks

Dari hasil analisa dan pengujian peneliti bisa mencantumkan hasil dari tiap spesimen ke dalam matriks yang sudah dibuat. Berikut hasil matriks dari analisa dan pengujian sebelumnya.

Tabel 1

Emulator	Uji Emulator	Uji Fake GPS	Workload	Waktu
Mumu Player	Lolos	Tidak Lolos	10.000 Events	16 Detik
MEmu Play	Lolos	Tidak Lolos	10.000 Events	19 Detik
LDPlayer	Lolos	Tidak Lolos	10.000 Events	39 Detik
Android Virtual Device	Tidak Lolos	Tidak Lolos	10.000 Events	78 Detik
Bluestack	Lolos	Tidak Lolos	10.000 Events	Tidak Lolos

## 4. KESIMPULAN

### 4.1 Simpulan

Setelah melakukan Analisa dan pengujian kepada *library safe device*, Maka dapat

disimpulkan bahwa dari 5 spesimen yang menginstall aplikasi *library safe device* hanya 1 spesimen saja yang bisa dideteksi sebagai emulator oleh aplikasi *library safe device* yaitu emulator Android *Virtual Device* Android Studio. Oleh karena itu *library safe device* masih kurang efektif untuk berfungsi sebagai validasi perangkat emulator, sedangkan untuk melakukan validasi terhadap penggunaan *fake GPS* aplikasi *library safe device* ini mampu mendeteksi semua spesimen bisa menggunakan *fake GPS*. Dengan demikian *library safe device* sangat efektif untuk digunakan sebagai validasi penggunaan *fake GPS* diaplikasi yang akan dibuat nantinya.

Dari pengujian *stress test* yang dilakukan terhadap 5 spesimen bisa dilihat bahwa pengujian *stress test* tidak terlalu berpengaruh terhadap performa validasi dari aplikasi *library safe device*. Waktu yang di tempuh untuk menyelesaikan pengujian *stress test* nya pun beragam. Spesimen kesatu berhasil menyelesaikan *stress test* dalam waktu 78 detik, Spesimen kedua menyelesaikan *stress test* dalam waktu 39 detik, Spesimen ketiga tidak dapat menyelesaikan *stress test*, pengujian berhenti di tes yang ke 9205 dari 10000 dari waktu 27 detik, Spesimen keempat berhasil menyelesaikan *stress test* dalam waktu 19 detik, sedangkan untuk spesimen kelima pengujian *stress test* dapat diselesaikan dengan waktu yang paling cepat yaitu selama 16 detik. Kesimpulan yang didapatkan adalah *library safe device* aman untuk digunakan didalam aplikasi untuk melakukan sebuah validasi terhadap emulator android dan *fake GPS*.

## 5. SARAN

Terdapat beberapa saran yang dapat diterapkan untuk memperbaiki dan mengembangkan penelitian ini agar menjadi semakin mendalam dan relevan.

1. Dalam pembuatan aplikasi menggunakan *safe device* disarankan untuk membuat tampilan agar validasi tidak hanya mengeluarkan data ya dan tidak saja.
2. Dalam melakukan pengujian disarankan menggunakan teknik pengujian yang berbeda dari yang peneliti lakukan.
3. Membuat laporan yang lebih detail terhadap analisa dan pengujian terkait pendeteksian *library safe device*.

## REFERENSI

- Ramdhani, Rizky, "Pengaruh Audit Internal dan Whistleblowing System Terhadap Pencegahan Kecurangan (Fraud) (Studi Kasus Pada PT. PLN (Persero) Distribusi Jawa Barat)", <http://repository.unpas.ac.id/37856/> diambil pada tanggal 3 Agustus 2023 pukul 12.00 WIB
- Septarini, Dinda (2020):Pembuatan Game Edukasi Mengenai Materi

- Hafalan Doa Harian Sebagai Media Pembelajaran Berbasis Android, *Jurnal Multi Media dan IT Vol.04 No.01(2020)*
- Sari, Annisa Medina, "Emulator android: Pengertian, Fungsi, Cara Kerja, Kelebihan, dan Kekurangan", <https://fikti.umsu.ac.id/emulator-android-pengertian-fungsi-cara-kerja-kelebihan-dan-kekurangan/> diambil pada tanggal 6 Agustus 2023 pukul 19.00 WIB
- Rosyida, Ryvina Izza, "Analisis Yuridis Sosiologis Praktik Penggunaan Fake GPS Pada Driver Okejek di Kota Malang Yang Mengakibatkan Kerugian Pada Sesama Driver Okejek di Kota Malang (Studi di PT.Okejek Kreasi Indonesia Kota Malang)", <http://eprints.umm.ac.id/id/eprint/95537> diambil pada tanggal 6 Agustus 2023 pukul 20.00 WIB
- Uminingsih., dkk (2022):Pengujian Fungsional Perangkat Lunak Sistem Informasi Perpustakaan Dengan Metode Black Box Testing Bagi Pemula, *JurnalIlmiah Teknik dan Ilmu Komputer, Vol. 1 No. 2, Mei, 2022.*
- Sofi M. & Reza Dharmawan. (2022):Perancangan Aplikasi Bengkel CSM Berbasis Android Menggunakan Framework Flutter (Bahasa Dart), *Jurnal Teknik dan Science, Vol. 1 No. 2, Juni, 2022.*
- Nugraha, W.M. (2022):Pengujian White Box Berbasis Path Pada Form Autentikasi Berbasis Mobile, *Jurnal Siliwangi Vol. 8 No. 2, 2022*
- Poetra D.R. & Nur Hayati (2022):Performa Algoritma Bubble Sort dan Quick Sort Pada Framework Flutter dan Dart SDK, *Jurnal Teknik Informatika dan Sistem Informasi Vol. 9 No. 2, Juni 2022*
- Developer.android.com(2023), "UIExerciserMonkey", <https://developer.android.com/studio/test/other-testing-tools/monkey> diambil pada tanggal 23 Agustus 14.00 WIB