



**DETEKSI *MALWARE* BERBASIS CITRA
MENGUNAKAN *DEEP LEARNING* PADA ANDROID**

SKRIPSI

UMMU ATHIYA 2207411005

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2026



**DETEKSI *MALWARE* BERBASIS CITRA
MENGUNAKAN *DEEP LEARNING* PADA ANDROID**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik**

UMMU ATHIYA

2207411005

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2026



SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Ummu Athiya

NIM : 2207411005

Jurusan/Program Studi : T. Informatika dan Komputer / Teknik Informatika

Judul Skripsi : DETEKSI *MALWARE* BERBASIS CITRA
MENGUNAKAN *DEEP LEARNING* PADA
ANDROID

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 3 Juli 2026

Yang membuat pernyataan



Ummu Athiya

NIM. 2207411005

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Ummu Athiya
NIM : 2207411005
Program Studi : Teknik Informatika
Judul Skripsi : Deteksi *Malware* Berbasis Citra Menggunakan *Deep Learning* Pada Android

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 24, Bulan Juni, Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom, M.T. (.....)

Penguji I : Rizki Elisa Nalawati, S.T., M.T. (.....)

Penguji II : Dr. Dewi Yanti Liliana, S.Kom, M.Kom. (.....)

Penguji III : Chairul Fikri, M.Kom. (.....)

Mengetahui:

Jurusan Teknik Informatika dan Komputer
Ketua



Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya skripsi ini dapat diselesaikan dengan baik. Penulis menyadari bahwa selesainya karya ini tidak lepas dari dukungan, bantuan, dan kesabaran berbagai pihak yang luar biasa. Secara khusus, penulis ingin menyampaikan terima kasih kepada:

- Dr. Alejandro Guerra-Mazanares *for his exceptional kindness in providing access to the research dataset and prompt responsiveness in my email correspondence.*
- Bapak Iik Muhamad Malik Matin, S.Kom, M.T., selaku Dosen Pembimbing, terima kasih atas waktu dan arahan Bapak selama pengerjaan skripsi ini.
- Ibu Dr. Anita Hidayati, S.Kom., M.Kom., selaku Dosen PA TI-A 2022, terima kasih selalu memberikan dukungan dan motivasi sejak awal masa perkuliahan.
- Ibu Euis Oktavianti, S.Si., M.T.I, selaku Kepala Program Studi Teknik Informatika, terima kasih atas dedikasi penuh Ibu sehingga penulis mampu menempuh dan menyelesaikan studi dengan baik.
- Niky dan Io dari *Podcast* Keluarga Artis dan Kak Nadia Omara, yang sudah menemani penulis dengan video-video *YouTube* mereka.
- Kucing Takjil, si *emotional support* sekaligus "majikan".

Semoga skripsi ini dapat memberikan manfaat bagi pembaca dan perkembangan ilmu pengetahuan.

Depok, 5 Juni 2026

Ummu Athiya



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Ummu Athiya

NIM : 2207411005

Jurusan/Program Studi : T.Informatika dan Komputer / Teknik Informatika

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

DETEKSI *MALWARE* BERBASIS CITRA MENGGUNAKAN *DEEP LEARNING* PADA ANDROID

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 3 Juli 2026

Yang Menyatakan



Ummu Athiya

NIM. 2207411005



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DETEKSI MALWARE BERBASIS CITRA MENGGUNAKAN DEEP LEARNING PADA ANDROID

ABSTRAK

Perkembangan ekosistem Android yang sangat pesat turut meningkatkan risiko penyebaran malware pada perangkat seluler. Metode deteksi tradisional berbasis signature memiliki keterbatasan dalam mendeteksi malware baru dan rentan terhadap teknik obfuscation. Penelitian ini bertujuan mengembangkan sistem deteksi malware Android berbasis citra menggunakan deep learning dengan representasi multi-channel image. File APK dikonversi menjadi citra RGB melalui ekstraksi komponen AndroidManifest.xml, classes.dex, dan resources.arsc menggunakan metode Multi-channel Image Size Adaptation (MC-ISA). Model klasifikasi dibangun menggunakan arsitektur CNN berbasis transfer learning dengan eksperimen pada MobileNet, EfficientNetB0, dan ResNet50V2. Dataset yang digunakan berasal dari KronoDroid dengan total 73.104 citra hasil sintesis. Hasil penelitian menunjukkan bahwa MobileNet memberikan performa terbaik dengan nilai accuracy sebesar 94,97%, precision sebesar 96,44%, recall sebesar 93,39%, dan F1-score sebesar 94,89%. Model kemudian diimplementasikan ke dalam aplikasi Android ATHENA untuk melakukan deteksi malware secara fungsional. Selain itu, penggunaan metode Explainable AI melalui Grad-CAM dan LIME membantu meningkatkan interpretabilitas hasil prediksi model. Penelitian ini menunjukkan bahwa representasi citra multi-channel efektif digunakan untuk deteksi malware Android berbasis deep learning.

Kata kunci: Android Malware, Deep Learning, CNN, Multi-channel Image, MobileNet

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR.....	iv
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	v
ABSTRAK	vi
DAFTAR ISI	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan dan Manfaat	4
1.5 Sistematika Penulisan	5
BAB II.....	7
TINJAUAN PUSTAKA.....	7
2.1 <i>Android Operating System</i>	7
2.2 Struktur Berkas APK.....	8
2.3 Metode Analisis <i>Malware</i>	9
2.4 <i>Convolutional Neural Network</i>	9
2.5 <i>Transfer Learning</i>	10
2.6 <i>Explainable AI (XAI)</i>	11
2.7 Penelitian Terdahulu.....	12
BAB III	16
METODE PENELITIAN.....	16
3.1 Rancangan Penelitian	16
3.2 Tahapan Penelitian	16
3.3 Objek Penelitian	18



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV	20
HASIL DAN PEMBAHASAN	20
4.1 Analisis Kebutuhan	20
4.2 Perancangan Sistem	22
4.3 Implementasi Sistem	36
4.4 Pengujian.....	55
BAB V	81
PENUTUP	81
5.1 Simpulan	81
5.2 Saran.....	82
DAFTAR PUSTAKA	83
DAFTAR RIWAYAT HIDUP PENULIS	86
LAMPIRAN.....	87

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 1. Penelitian Terdahulu.....	12
Tabel 2. Hasil Seleksi dan Uji Kelayakan Dataset.....	29
Tabel 3. Distribusi Pembagian Dataset	29
Tabel 4. Skema Pelatihan Model.....	31
Tabel 5. Perbandingan Performa Model.....	37
Tabel 6. Skenario Black Box Testing	56
Tabel 7. Informasi Sampel APK CICMalDroid 2020	58
Tabel 8. Daftar Pertanyaan System Usability Scale.....	59
Tabel 9. Bobot Penilaian Skala Likert.....	59
Tabel 10. Pertanyaan Net Promoter Score	60
Tabel 11. Kategori Sampel Pengguna	60
Tabel 12. Hasil Pengujian Black Box Testing.....	61
Tabel 13. Hasil External Data Testing.....	62
Tabel 14. Hasil Kuesioner SUS.....	66
Tabel 15. Contoh Perhitungan SUS Responden R01-G1-U3-B2.....	67
Tabel 16. Skor SUS Seluruh Responden.....	67
Tabel 17. Hasil Kuesioner NPS.....	69
Tabel 18. Distribusi Kategori Hasil NPS	70
Tabel 19. Perbandingan Performa Model RGB dan Grayscale.....	77



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian	16
Gambar 3.2 Proses Sintesis Citra Multi-Channel	17
Gambar 4.1 Fungsi get_file_bytes	23
Gambar 4.2 Kode Ekstraksi Komponen APK.....	24
Gambar 4.3 Potongan Nilai Sequence Byte dari File DEX	24
Gambar 4.4 Fungsi Mapping Sequence isa.....	25
Gambar 4.5 Fungsi color_enhancement.....	27
Gambar 4.6 Perbandingan Citra Sebelum dan Sesudah Enhancement.....	27
Gambar 4.7 Sampel Hasil Citra Multi-Channel.....	28
Gambar 4.8 Arsitektur Model	30
Gambar 4.9 Use Case Diagram Aplikasi ATHENA.....	32
Gambar 4.10 Activity Diagram Deteksi Malware APK.....	34
Gambar 4.11 Color Palette Aplikasi ATHENA.....	35
Gambar 4.12 Inter Font Family.....	35
Gambar 4.13 Desain Wireframe Aplikasi ATHENA.....	36
Gambar 4.14 Grafik Akurasi MobileNet Tahap 1	38
Gambar 4.15 Grafik Akurasi MobileNet Tahap 2	38
Gambar 4.16 Grafik Loss MobileNet Tahap 1	39
Gambar 4.17 Grafik Loss MobileNet Tahap 2.....	39
Gambar 4.18 Confusion Matrix Model MobileNet	40
Gambar 4.19 Kurva ROC Model MobileNet.....	41
Gambar 4.20 Grafik Akurasi EfficientNetB0 Tahap 1	42
Gambar 4.21 Grafik Akurasi EfficientNetB0 Tahap 2	42
Gambar 4.22 Grafik Loss EfficientNetB0 Tahap 1	43
Gambar 4.23 Grafik Loss EfficientNetB0 Tahap 2.....	43
Gambar 4.24 Confusion Matrix Model EfficientNetB0	44
Gambar 4.25 Kurva ROC Model EfficientNetB0.....	44
Gambar 4.26 Grafik Akurasi ResNet50V2 Tahap 1.....	45
Gambar 4.27 Grafik Akurasi ResNet50V2 Tahap 2.....	45
Gambar 4.28 Grafik Loss ResNet50V2 Tahap 1.....	46
Gambar 4.29 Grafik Loss ResNet50V2 Tahap 2.....	46



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.30 Confusion Matrix Model ResNet50V2	47
Gambar 4.31 Kurva ROC Model ResNet50V2.....	48
Gambar 4.32 Grafik Perbandingan Metrik Evaluasi Model	49
Gambar 4.33 Grafik Perbandingan Size Model	50
Gambar 4.34 Konversi Model .keras Menjadi .tflite	51
Gambar 4.35 Konfigurasi Google Cloud Run.....	51
Gambar 4.36 Pipeline Sistem.....	52
Gambar 4.37 Halaman <i>Upload</i>	53
Gambar 4.38 Proses <i>Uploading</i>	53
Gambar 4.39 Proses <i>Scanning</i>	54
Gambar 4.40 Result Benign (Aman).....	55
Gambar 4.41 Result Malware (Berbahaya).....	55
Gambar 4.42 Grafik Jenis Kelamin dan Bidang Responden.....	63
Gambar 4.43 Grafik Rentang Usia Responden.....	64
Gambar 4.44 Pengalaman Menginstal Aplikasi Tidak Resmi.....	65
Gambar 4.45 Visualisasi XAI Sampel True Positive	72
Gambar 4.46 Visualisasi XAI Sampel True Negative.....	73
Gambar 4.47 Visualisasi XAI Sampel False Positive	74
Gambar 4.48 Visualisasi XAI Sampel False Negative.....	75
Gambar 4.49 Proses Sintesis Citra Grayscale	76
Gambar 4.50 Grafik Perbandingan Metrik Evaluasi RGB vs Grayscale	77
Gambar 4.51 Nilai SUS Berdasarkan Jenis Kelamin.....	79
Gambar 4.52 Nilai SUS Berdasarkan Latar Belakang Bidang	79
Gambar 4.53 Nilai SUS Berdasarkan Rentang Usia.....	80



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR LAMPIRAN

Lampiran 1 - Dokumentasi Pengujian External Data Testing.....	87
Lampiran 2 - Dokumentasi Uji Coba Aplikasi oleh Pengguna	90
Lampiran 3 - Lembar Tanda Tangan Responden Pengujian	92





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Pesatnya perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan adopsi perangkat seluler secara masif dalam berbagai aspek kehidupan masyarakat. Di Indonesia, data (Badan Pusat Statistik, 2025) menunjukkan bahwa persentase penduduk yang memiliki atau menguasai telepon seluler pada tahun 2024 telah mencapai 68,65%. Secara global, fenomena ini didominasi oleh penggunaan sistem operasi Android. Berdasarkan data dari *Forrester Research*, Android menguasai sekitar 74% pangsa pasar perangkat seluler dunia (Yadav et al., 2022).

Namun, dominasi ini secara eksponensial menjadikan Android sebagai target utama bagi para pengembang *malicious software* (*malware*). Laporan dari *GData Internet Security Centre* mengonfirmasi tren ini dengan temuan sekitar 2.040.293 sampel *malware* baru pada semester pertama tahun 2018, yang merepresentasikan kenaikan sebesar 31% dibandingkan periode sebelumnya. Sejalan dengan temuan tersebut, *SecureLIST Mobile Malware Evolution Report* mencatat bahwa teknologi *Kaspersky Lab* berhasil mendeteksi lebih dari 5,3 juta paket instalasi berbahaya, yang mencakup 151.359 *trojan* perbankan dan 60.176 *ransomware* seluler. Kondisi ini diperparah oleh fakta bahwa distribusi *malware* seperti *Android.DownLoader*, *Android.Banker*, dan *Android.HiddenAds* bahkan mampu menembus kanal resmi seperti *Google Play*, yang secara langsung mengancam keamanan data dan integritas perangkat para pengguna Android (Ünver and Bakour, 2020).

Dampak yang ditimbulkan oleh serangan *malware* pada ekosistem Android sangat beragam dan membawa konsekuensi kerugian yang signifikan bagi pengguna. Tipologi ancaman yang paling dominan adalah deduksi biaya secara ilegal (*malicious fee deductions*) yang mencapai 34,9% dari total kasus. Selain aspek finansial, *malware* juga mengeksploitasi aspek teknis dan privasi, yang mencakup konsumsi sumber daya perangkat secara berlebihan (24,2%), perilaku anomali atau *rogue behavior* (22,8%), serta pencurian data privasi (12,3%). Statistik ini menegaskan bahwa tanpa adanya proteksi yang mumpuni, pengguna terpapar pada



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

risiko kehilangan aset material maupun data sensitif yang sulit dipulihkan (Zhu et al., 2023).

Meskipun berbagai mekanisme pertahanan telah diterapkan, efektivitas perangkat lunak *anti-malware* saat ini masih sangat bergantung pada penggunaan *signature-based detection*. Metode ini bekerja dengan membandingkan sampel perangkat lunak terhadap repositori *signature* atau basis data *string* unik yang merepresentasikan perilaku berbahaya tertentu. Namun, mekanisme ini memiliki dua kelemahan fundamental. Pertama, proses ekstraksi *signature* merupakan prosedur manual yang bersifat *laborius* dan memakan waktu lama karena memerlukan analisis mendalam oleh pakar keamanan, sehingga sebuah ancaman baru sering kali hanya dapat dikenali setelah menyebar secara luas. Kedua, metode berbasis *signature* sangat rentan terhadap teknik *obfuscation* sederhana yang memungkinkan *malware* mengubah strukturnya tanpa mengubah fungsi berbahayanya, sehingga dengan mudah dapat mengelabui sistem deteksi tradisional (Mercaldo and Santone, 2020).

Untuk mengatasi keterbatasan metode deteksi konvensional tersebut, berbagai penelitian mulai mengeksplorasi pendekatan berbasis representasi visual terhadap *malware* seperti yang dilakukan oleh (Yadav et al., 2022) dan (Nethala et al., 2025). Dalam pendekatan ini, berkas aplikasi Android yang tersusun atas data biner direpresentasikan menjadi citra digital melalui pemetaan nilai *byte* ke dalam matriks dua dimensi (Moussas and Andreatos, 2021; Qi et al., 2023). Transformasi tersebut mengubah permasalahan deteksi *malware* menjadi permasalahan pengenalan citra, sehingga memungkinkan pemanfaatan arsitektur *Convolutional Neural Network* (Moussas and Andreatos, 2021). Berbeda dengan pendekatan konvensional yang bergantung pada proses *feature engineering* manual, pendekatan berbasis CNN memungkinkan proses pembelajaran representasi fitur dilakukan secara otomatis dari citra yang dihasilkan (Qi et al., 2023). Oleh karena itu, representasi visual menjadi salah satu pendekatan yang menjanjikan untuk mendukung proses deteksi *malware* berbasis *deep learning*.

Berdasarkan studi literatur, mayoritas penelitian sebelumnya masih menggunakan dataset lawas seperti penggunaan Drebin dan AMD pada (Nethala et al., 2025),



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

CICAndMal2017 pada (Lekssays et al., 2020), dan R2-D2 pada (Yadav et al., 2022) dengan rentang waktu terbatas hingga 2017. Penelitian ini menggunakan dataset KronoDroid (2021) yang mencakup sampel *malware* dari tahun 2008 hingga 2020, sehingga memberikan representasi ancaman yang lebih modern dan relevan terhadap evolusi *malware*.

Selain itu, guna memperkuat kemampuan ekstraksi fitur, penelitian ini mengusulkan metode *Multi-channel Image Representation* yang mengadopsi metode MC-ISA oleh (Qi et al., 2023). Jika penelitian terdahulu umumnya hanya menggunakan citra dari file DEX seperti pada (Yadav et al., 2022) dan (Ding et al., 2023), metode ini mensintesis citra RGB dengan memanfaatkan tiga komponen krusial APK sekaligus, yaitu *AndroidManifest.xml*, *classes.dex*, dan *resources.arsc*. Pendekatan ini bertujuan untuk menangkap korelasi fitur global antara izin aplikasi, logika kode, dan sumber daya aplikasi. Integrasi dataset yang komprehensif dengan representasi citra *multi-channel* ini kemudian diimplementasikan menggunakan arsitektur *MobileNet*, yang efisien namun tetap memiliki akurasi tinggi dalam mengenali pola spasial kompleks pada perangkat seluler.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merepresentasikan berkas APK ke dalam bentuk citra *multi-channel* melalui ekstraksi berkas *AndroidManifest.xml*, *classes.dex*, dan *resources.arsc* untuk menghasilkan fitur spasial yang komprehensif?
2. Bagaimana merancang dan mengimplementasikan arsitektur *Deep Learning* yang optimal untuk mengenali pola visual dari citra *malware* Android?
3. Sejauh mana tingkat akurasi dan performa sistem yang dikembangkan dalam mendeteksi *malware*?
4. Bagaimana mengintegrasikan model yang telah dilatih ke dalam sebuah aplikasi Android fungsional?



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan tidak menyimpang dari tujuan yang telah ditetapkan, maka diberikan batasan-batasan masalah sebagai berikut:

1. Penelitian ini hanya mendukung pendeteksian aplikasi Android dengan format berkas .apk.
2. Metode yang digunakan berfokus pada arsitektur *CNN-based*, dengan penggunaan *transfer learning MobileNet* untuk optimalisasi performa.
3. Evaluasi model dilakukan dengan menggunakan metrik *accuracy*, *precision*, *recall*, dan *F1-score*, serta penggunaan *confusion matrix*.
4. *Output* dari penelitian ini terbatas pada pengembangan aplikasi berbasis sistem operasi Android.
5. Aplikasi dirancang untuk melakukan klasifikasi biner, yaitu menentukan apakah sebuah berkas .apk termasuk dalam kategori *malware* atau *benign*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan metode transformasi berkas APK ke dalam bentuk citra *multi-channel* dengan mengekstraksi komponen *Manifest*, *DEX*, dan *ARSC* guna menghasilkan representasi fitur spasial yang komprehensif.
2. Mengimplementasikan arsitektur *CNN-based*, termasuk eksplorasi metode *transfer learning*, untuk melakukan klasifikasi otomatis terhadap aplikasi berbahaya.
3. Mengevaluasi performa model deteksi menggunakan metrik *accuracy*, *precision*, *recall*, dan *F1-score* guna memastikan efikasi sistem dalam membedakan *malware* dan aplikasi *benign*.
4. Membangun prototipe aplikasi Android fungsional yang mengintegrasikan model yang sudah dibangun.

1.4.2 Manfaat

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. Bagi Pengguna: Memberikan alternatif solusi keamanan untuk mendeteksi ancaman *malware*.
2. Bagi Akademisi: Menjadi referensi ilmiah tambahan mengenai efektivitas representasi citra dalam deteksi *malware* serta menjadi dasar pengembangan penelitian selanjutnya di bidang *mobile security* dan *artificial intelligence*.
3. Bagi Keamanan Siber: Berkontribusi dalam memperkuat ekosistem digital Android melalui metode deteksi yang lebih adaptif.

1.5 Sistematika Penulisan

Pada penulisan laporan ini, penulis menyusun sistematika penulisan yang terbagi ke dalam beberapa bab. Setiap bab disusun secara terstruktur dan saling berkaitan dengan tujuan penelitian, dengan uraian sebagai berikut:

BAB I PENDAHULUAN

Bab ini memuat latar belakang penyusunan laporan tugas akhir, tujuan penulisan, manfaat yang diharapkan dari penelitian, serta sistematika penulisan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini berisi kajian teori yang relevan, konsep dasar, serta pendapat para ahli yang digunakan sebagai landasan dan pendukung dalam penelitian yang dilakukan.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan, meliputi rancangan dan tahapan penelitian, objek penelitian, serta perangkat dan aplikasi yang digunakan dalam pengembangan sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan, pemaparan dan analisis hasil pengembangan model dan aplikasi deteksi *malware* berbasis citra yang dibuat serta penyajian data hasil pengujian.

BAB V PENUTUP



© Hak Cipta milik Politeknik Negeri Jakarta

Bab ini berisi kesimpulan akhir dari seluruh rangkaian penelitian serta saran untuk pengembangan penelitian selanjutnya.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

5.1 Simpulan

Berdasarkan hasil penelitian yang telah dilakukan, diperoleh beberapa simpulan sebagai berikut:

1. Penelitian ini berhasil mengembangkan metode transformasi berkas APK menjadi citra *multi-channel* RGB dengan memanfaatkan tiga komponen utama aplikasi Android, yaitu *AndroidManifest.xml*, *classes.dex*, dan *resources.arsc*. Proses transformasi dilakukan menggunakan metode *Multi-channel Image Size Adaptation* (MC-ISA) yang menghasilkan representasi visual berukuran 256×256 piksel dan mampu merepresentasikan informasi struktural aplikasi secara komprehensif.
2. Penelitian ini berhasil mengimplementasikan arsitektur CNN berbasis *transfer learning* untuk klasifikasi *malware* Android. Berdasarkan hasil eksperimen terhadap tiga arsitektur yang diuji, yaitu *MobileNet*, *EfficientNetB0*, dan *ResNet50V2*, model *MobileNet* menunjukkan performa terbaik dalam mengenali pola visual pada citra *malware* Android.
3. Hasil evaluasi menunjukkan bahwa model *MobileNet* memperoleh nilai *accuracy* sebesar 94,97%, *precision* sebesar 96,44%, *recall* sebesar 93,39%, dan *F1-score* sebesar 94,89%. Hasil tersebut menunjukkan bahwa pendekatan representasi citra *multi-channel* yang dikombinasikan dengan *transfer learning* mampu melakukan deteksi *malware* Android secara efektif dengan tingkat performa yang tinggi.
4. Model yang telah dilatih berhasil diintegrasikan ke dalam aplikasi Android ATHENA yang mampu melakukan proses deteksi *malware* terhadap berkas APK secara fungsional. Hasil pengujian menunjukkan bahwa aplikasi dapat menjalankan seluruh fitur utama sesuai kebutuhan sistem dan memperoleh tingkat *usability* yang sangat baik berdasarkan evaluasi pengguna menggunakan *System Usability Scale* (SUS).
5. Analisis interpretabilitas menggunakan Grad-CAM dan LIME menunjukkan bahwa model tidak hanya mampu menghasilkan prediksi yang akurat, tetapi juga dapat memberikan penjelasan mengenai area citra



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yang berkontribusi terhadap keputusan klasifikasi. Selain itu, penggunaan representasi citra *multi-channel* RGB terbukti memberikan performa yang lebih baik dibandingkan representasi citra *grayscale*, sehingga integrasi informasi dari beberapa komponen APK dapat meningkatkan kemampuan deteksi *malware*.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan penelitian selanjutnya, yaitu sebagai berikut:

1. Melakukan pengembangan model dengan mencoba metode sintesis citra lain, menggunakan arsitektur *pre-trained* yang berbeda, maupun menggabungkan beberapa model atau algoritma (*ensemble/hybrid model*) guna meningkatkan performa klasifikasi *malware*.
2. Mengembangkan sistem deteksi agar tidak hanya berupa aplikasi mandiri, tetapi dapat diintegrasikan langsung ke platform distribusi aplikasi seperti *app store* resmi atau dikembangkan dalam bentuk *plugin* keamanan, sehingga proses pemeriksaan *malware* dapat dilakukan secara otomatis sebelum aplikasi diinstal oleh pengguna.
3. Memperluas kemampuan sistem dari klasifikasi biner menjadi klasifikasi multi-kelas untuk mengidentifikasi jenis atau keluarga *malware* secara lebih spesifik.
4. Pengujian sistem dapat diperluas menggunakan dataset yang lebih baru dan lebih beragam untuk meningkatkan kemampuan generalisasi model terhadap ancaman *malware* Android terkini.

Dengan adanya pengembangan lebih lanjut pada aspek model, data, maupun implementasi sistem, penelitian ini diharapkan dapat menjadi dasar dalam pengembangan solusi deteksi *malware* Android yang lebih akurat, adaptif, dan aplikatif di masa mendatang.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Abdillah, M.T., Kurniastuti, I., Susanto, A., Yudianto, F., Studi, P., Informasi, S., Bisnis, E., Digital, D.T., 2023. Implementasi Black box Testing dan Usability Testing pada Website Sekolah MI Miftahul Ulum Warugunung Surabaya. Jurnal Ilmu Komputer dan Desain Komunikasi Visual 8.
- Al-Fawa'reh, M., Saif, A., Jafar, M.T., Elhassan, A., 2020. Malware Detection by Eating a Whole APK, in: 2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.23919/ICITST51030.2020.9351333>
- AOSP Documentation, 2025. Ringkasan Arsitektur AOSP [WWW Document]. Android Documentation. URL <https://source.android.com/docs/core/architecture?hl=id> (accessed 1.11.26).
- Badan Pusat Statistik, 2025. Persentase Penduduk yang Memiliki/Menguasai Telepon Seluler Menurut Provinsi dan Klasifikasi Daerah.
- Brosolo, M., 2023. Demystifying Malware Image Visualization: Enhancing Reproducibility and Explainability. Universita Degli Studi Di Padova.
- Chaganti, R., Ravi, V., Pham, T.D., 2022. Image-based malware representation approach with EfficientNet convolutional neural networks for effective malware classification. Journal of Information Security and Applications 69. <https://doi.org/10.1016/j.jisa.2022.103306>
- Ding, Y., Zhang, X., Hu, J., Xu, W., 2023. Android malware detection method based on bytecode image. J. Ambient Intell. Humaniz. Comput. 14, 6401–6410. <https://doi.org/10.1007/s12652-020-02196-4>
- Dwivedi, R., Dave, D., Naik, H., Singhal, S., Omer, R., Patel, P., Qian, B., Wen, Z., Shah, T., Morgan, G., Ranjan, R., 2023. Explainable AI (XAI): Core Ideas, Techniques, and Solutions. ACM Comput. Surv. 55. <https://doi.org/10.1145/3561048>
- Gibert, D., Mateu, C., Planes, J., Vicens, R., 2019. Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques 15, 15–28. <https://doi.org/10.1007/s11416-018-0323-0>
- Guerra-Manzanares, A., Bahsi, H., Nömm, S., 2021. KronoDroid: Time-based hybrid-featured dataset for effective android malware detection and characterization. Comput. Secur. 110. <https://doi.org/10.1016/j.cose.2021.102399>
- Halloum, K., Ez-Zahraouy, H., 2025. Enhancing Medical Image Classification through Transfer Learning and CLAHE Optimization. Current Medical



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- Imaging Formerly Current Medical Imaging Reviews 21. <https://doi.org/10.2174/0115734056342623241119061744>
- Lekssays, A., Falah, B., Abufardeh, S., 2020. A novel approach for android malware detection and classification using convolutional neural networks, in: ICSoft 2020 - Proceedings of the 15th International Conference on Software Technologies. SciTePress, pp. 606–614. <https://doi.org/10.5220/0009822906060614>
- Li, Z., Liu, F., Yang, W., Peng, S., Zhou, J., 2022. A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. IEEE Trans. Neural Netw. Learn. Syst. 33, 6999–7019. <https://doi.org/10.1109/TNNLS.2021.3084827>
- Mahdavifar, S., Abdul Kadir, A.F., Fatemi, R., Alhadidi, D., Ghorbani, A.A., 2020. Dynamic Android Malware Category Classification using Semi-Supervised Deep Learning, in: 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). IEEE, pp. 515–522. <https://doi.org/10.1109/DASC-PiCom-CBDCom-CyberSciTech49142.2020.00094>
- Matin, I.M.M., 2023. Hyperparameter Tuning menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware. Depok.
- Mercaldo, F., Santone, A., 2020. Deep learning for image-based mobile malware detection. Journal of Computer Virology and Hacking Techniques 16, 157–171. <https://doi.org/10.1007/s11416-019-00346-7>
- Moussas, V., Andreatos, A., 2021. Malware detection based on code visualization and two-level classification. Information (Switzerland) 12, 1–14. <https://doi.org/10.3390/info12030118>
- Navantino, F.F., Fahreza, M.F., Rilvani, E., 2025. TINJAUAN LITERATUR: PERBANDINGAN SISTEM KEAMANAN PADA APLIKASI ANDROID DAN IOS. Jurnal Ilmiah Teknik dan Ilmu Komputer 4, 22–28. <https://doi.org/10.55123>
- Nazim, S., Alam, M.M., Rizvi, S.S., Mustapha, J.C., Hussain, S.S., Suud, M.M., 2025. Advancing malware imagery classification with explainable deep learning: A state-of-the-art approach using SHAP, LIME and Grad-CAM. PLoS One 20. <https://doi.org/10.1371/journal.pone.0318542>
- Nethala, S., Chopra, P., Kamaluddin, K., Alam, S., Alharbi, S., Alsaffar, M., 2025. A Deep Learning-Based Ensemble Framework for Robust Android Malware Detection. IEEE Access 13, 46673–46696. <https://doi.org/10.1109/ACCESS.2025.3551152>



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- Nurmaini, S., Darmawahyuni, A., Sapitri. Ade Iriani, Rachmatullah, M.N., Firdaus, Tutuko, B., 2021. PENGENALAN DEEP LEARNING DAN IMPLEMENTASINYA. UPT. Penerbit dan Percetakan Universitas Sriwijaya 2021, Palembang.
- Qi, X., Liu, W., Lou, R., Li, Q., Jiang, L., Tang, Y., 2023. MC-ISA: A Multi-Channel Code Visualization Method for Malware Detection. Electronics (Switzerland) 12. <https://doi.org/10.3390/electronics12102272>
- Salehi, A.W., Khan, S., Gupta, G., Alabdullah, B.I., Almjally, A., Alsolai, H., Siddiqui, T., Mellit, A., 2023. A Study of CNN and Transfer Learning in Medical Imaging: Advantages, Challenges, Future Scope. Sustainability (Switzerland). <https://doi.org/10.3390/su15075930>
- Shah, S.S.H., Ahmad, A.R., Jamil, N., Khan, A. ur R., 2022. Memory Forensics-Based Malware Detection Using Computer Vision and Machine Learning. Electronics (Switzerland) 11. <https://doi.org/10.3390/electronics11162579>
- Simarmata, B.T., 2019. MENGUKUR TINGKAT KEPUASAN NASABAH DENGAN NET PROMOTER SCORE PADA PT.BPD JAWA BARAT DAN BANTEN TBK. CABANG MEDAN. Jurnal Ilmiah Skylandsea 3, 257–264.
- Susila, A.A.N.H., Arsa, D.M.S.A., 2023. ANALISIS SYSTEM USABILITY SCALE (SUS) DAN PERANCANGAN SISTEM SELF SERVICE PEMESANAN MENU DI RESTORAN BERBASIS WEB. Majalah Ilmiah UNIKOM 21, 3–8.
- TensorFlow Documentation, 2024. TensorFlow v2.16.1 Documentation [WWW Document]. TensorFlow. URL https://www.tensorflow.org/api_docs/python/tf/keras/layers (accessed 6.30.26).
- Ünver, H.M., Bakour, K., 2020. Android malware detection based on image-based features and machine learning techniques. SN Appl. Sci. 2. <https://doi.org/10.1007/s42452-020-3132-2>
- Yadav, P., Menon, N., Ravi, V., Vishvanathan, S., Pham, T.D., 2022. EfficientNet convolutional neural networks-based Android malware detection. Comput. Secur. 115. <https://doi.org/10.1016/j.cose.2022.102622>
- Zhu, H., Wei, H., Wang, L., Xu, Z., Sheng, V.S., 2023. An effective end-to-end android malware detection method. Expert Syst. Appl. 218. <https://doi.org/10.1016/j.eswa.2023.119593>



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP PENULIS



Ummu Athiya

Mengawali pendidikan di SDIT Misbahussudur sampai tahun 2015, melanjutkan ke SMPN 2 Cibinong dan lulus pada tahun 2018, kemudian masuk ke Jurusan Sistem Informatika Jaringan dan Aplikasi di SMKN 1 Cibinong dengan masa studi 4 tahun hingga tahun 2022.

Sedang menempuh Pendidikan Sarjana Terapan pada Program Studi Teknik Informatika di Politeknik Negeri Jakarta dengan fokus peminatan pada bidang *Machine Learning* dan *Data Science*.

**POLITEKNIK
NEGERI
JAKARTA**

LAMPIRAN

Lampiran 1 - Dokumentasi Pengujian *External Data Testing*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hasil Pengujian B-01



Hasil Pengujian B-02



Hasil Pengujian B-03



Hasil Pengujian B-04



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

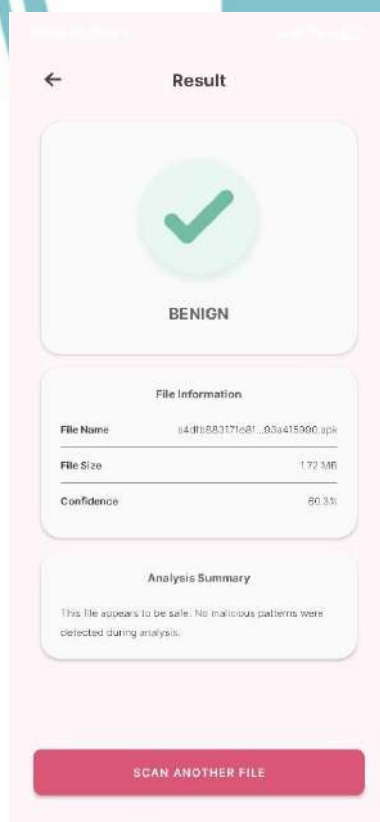
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hasil Pengujian B-05



Hasil Pengujian M-06



Hasil Pengujian M-07



Hasil Pengujian M-08



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hasil Pengujian M-09



Hasil Pengujian M-10

**POLITEKNIK
NEGERI
JAKARTA**

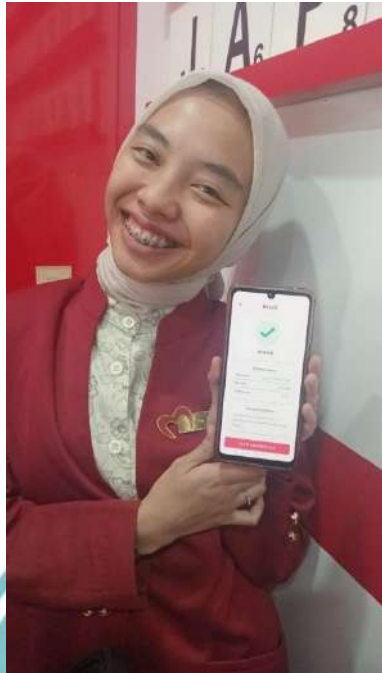


© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 2 - Dokumentasi Uji Coba Aplikasi oleh Pengguna



Uji Coba ATHENA oleh Ishika



Uji Coba ATHENA oleh Dok. Cla



Uji Coba ATHENA oleh Ammar



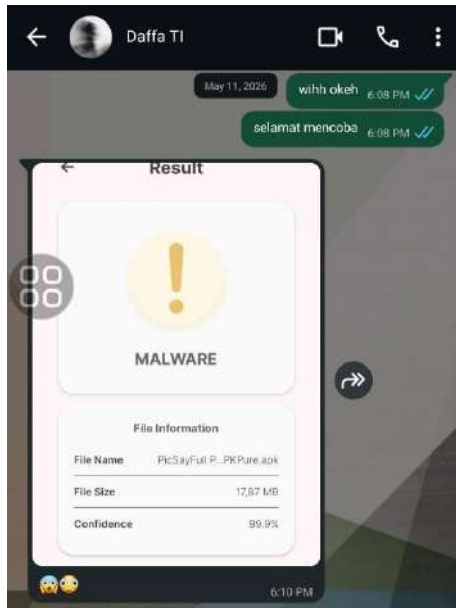
Uji Coba ATHENA oleh Andi



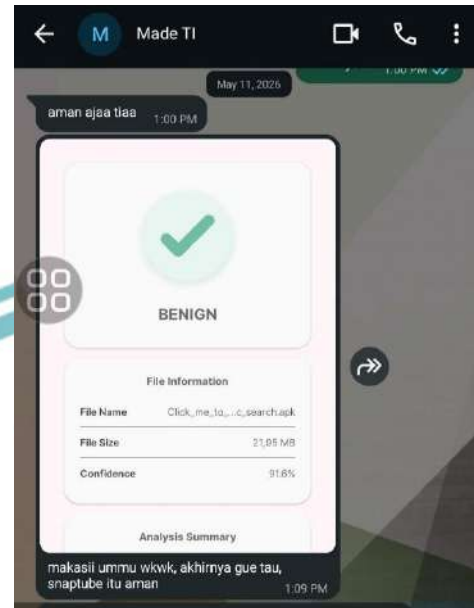
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

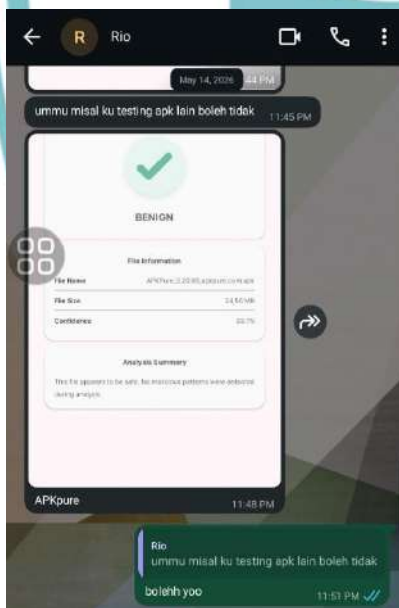
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



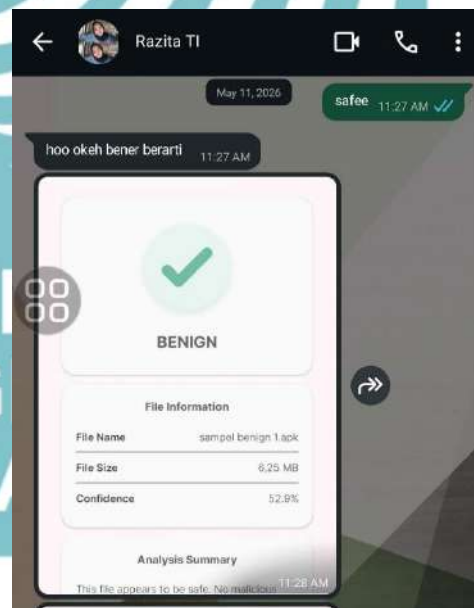
Uji Coba ATHENA oleh Daffa



Uji Coba ATHENA oleh Made



Uji Coba ATHENA oleh Rio



Uji Coba ATHENA oleh Razita



© Hak Cipta milik Politeknik Negeri Jakarta

Lampiran 3 - Lembar Tanda Tangan Responden Pengujian

RESPONDEN PENGUJIAN

System Usability Scale & Net Promoter Score

ATHENA

Terima kasih atas partisipasinya, Friends!
❤️ ❤️ ❤️

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta