# JUDUL

**Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi Pola *Financial Theft* dalam File APK)**

# SKRIPSI

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

Nadhilah Noor
2007421005

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**
**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**
**POLITEKNIK NEGERI JAKARTA**
**TAHUN 2024**

# SURAT PERNYATAAN BEBAS PLAGIARISME

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Nadhilah Noor

NIM : 2007421005

Jurusan/ProgramStudi : T.Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul skripsi : Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi Pola *Financial Theft* dalam File APK)

Menyatakan dengan sebenarnya bahwa skripsiini 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, 1 Agustus 2024

Yang membuat pernyataan


(Nadhilah Noor)

NIM 2007421005

## LEMBAR PENGESAHAN

© Hak Cipta milik Jurusan TIK 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 dari Jurusan TIK Politeknik Negeri Jakarta

**LEMBAR PENGESAHAN**

Skripsi diajukan oleh:

| | | |
|---|---|---|
| Nama Mahasiswa | : | Nadhilah Noor |
| NIM | : | 2007421005 |
| Program Studi | : | Teknik Multimedia dan Jaringan |
| Judul Skripsi | : | Analisis Statik dengan Teknik Reverse Engineering dan Signature Based Detection pada Perangkat Android (Studi Kasus: Identifikasi Pola Financial Theft dalam File APK) |

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa, Tanggal 6, Bulan Agustus, Tahun 2024 dan dinyatakan **LULUS.**

Disahkan oleh

| | | | |
|---|---|---|---|
| Pembimbing I | : | Iik Muhamad Malik Matin, S.Kom., M.T. | ( ) |
| Penguji I | : | Dr. Indra Hermawan, S.Kom., M.Kom | ( ) |
| Penguji II | : | Ayu Rosyida Zain, S.ST., M.T. | ( ) |
| Penguji III | : | Ariawan Andi Suhandana S.Kom., M.T.I | ( ) |

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

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

NIP. 197908032003122003

## KATA PENGANTAR

*Assalamualaikum Wr., Wb.*

Puji dan syukur selalu kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi Pola *Financial Theft* dalam File APK)" dengan baik atas bantuan, motivasi, dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. selaku pembimbing penulis yang telah banyak membantu, mendukung, dan memberikan masukan serta saran kepada penulis selama mengerjakan skripsi ini hingga selesai.
2. Kedua orang tua tercinta yang telah memberikan banyak dukungan, doa dan cinta tanpa syarat yang diberikan kepada penulis selama proses penyelesaian skripsi.
3. Sahabat dan teman-teman yang telah banyak membantu dan memberikan dukungan dalam pengerjaan skripsi.

Akhir kata penulis mengucapkan banyak terima kasih kepada semuanya. Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak terdapat kekurangan dan keterbatasan, oleh karena itu penulis memohon maaf atas ketidaksempurnaan ini. Semoga skripsi yang ditulis ini bermanfaat dan menjadi motivasi untuk penelitian selanjutnya dan bagi pembaca.

*Wassalamualaikum Wr., Wb.*

Depok, 1 Agustus 2024

Penulis

## SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI
SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertandatangan dibawah ini:

| | |
|---|---|
| Nama | : Nadhilah Noor |
| NIM | : 2007421005 |
| Jurusan/Program Studi | : T.Informatika dan Komputer/T.Multimedia dan Jaringan |

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

Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi Pola *Financial Theft* dalam File APK)

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 pernyatan ini saya buat dengan sebenarnya.

Depok, 1 Agustus 2024

Yang Menyatakan


(Nadhilah Noor)

NIM. 2007421005

**Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi Pola *Financial Theft* dalam File APK)**

***Abstrak***

*Seiring dengan meningkatnya penggunaan, muncul ledakan kode berbahaya, yaitu malware seluler yang dirancang untuk menargetkan smartphone. Dilansir dari data Bank Indonesia, banyak sekali tujuan pelaku adalah pencurian keuangan dengan modus online yang dilakukan dengan mengirimkan file surat undangan pernikahan berformat (.apk) yang dikirimkan melalui WhatsApp. Data yang dicuri mulai dari informasi pribadi, SMS, hingga informasi perbankan seperti (One Time Password) OTP. Berdasarkan hal tersebut dilakukan penelitian dengan mengumpulkan sampel malware dan memilih salah satu dari sampel malware untuk dilakukan analisis statik dengan teknik reverse engineering. Didapatkan karakteristik dari sampel tersebut untuk dibuatkan rule dengan teknik siganture-based detection menggunakan YARA. Aspek dari rule yang dibuat mencakup PERMISSIONS, URL, RECEIVED_SMS, API TELEGRAM BOT, NOTIFICATION_LISTENER, SERVICE_RECEIVER_PROVIDER. Pengukuran tingkat kinerja berdasarkan kecocokan rule yang dibuat dengan merujuk studi kasus pencurian keuangan menggunakan metric Recall. Kinerja signature-based detection dalam mendeteksi malware financial theft menunjukkan hasil moderat dengan total recall sebesar 55,17%, yang berarti hampir setengah dari sampel tidak terdeteksi. Meskipun beberapa rules sangat efektif (dengan recall hingga 93%), ada rules lain yang memiliki performa rendah, menunjukkan perlunya perbaikan dan optimasi lebih lanjut untuk meningkatkan cakupan deteksi secara keseluruhan.*

**Kata kunci:** analisis statik, malware android, reverse engineering, signature-based detection, YARA.

## DAFTAR ISI

## DAFTAR GAMBAR

## DAFTAR TABEL

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Perangkat seluler tidak lagi terbatas pada layanan komunikasi dalam halnya penggunaan perangkat seluler tradisional. Perangkat ini telah berevolusi menjadi sebuah perangkat yang berfungsi untuk melakukan *personal payments, social communication, entertainment activities,* dan *electronic commerce.* Berdasarkan data pada Badan Pusat Statistik (BPS), sebanyak 67,88% penduduk Indonesia berusia di atas 5 tahun sudah menggunakan ponsel di tahun 2022 (Z.Yonatan, 2023). Diikuti dengan pendataan Survei Susenas (Survei Sosial Ekonomi Nasional) 2022, terdapat 66,48% persen penduduk Indonesia telah mengakses internet di tahun 2022 (BPS, 2023). Tingginya penggunaan internet ini mencerminkan keterbukaan informasi dan penerimaan masyarakat terhadap perkembangan teknologi dan perubahan menuju masyarakat informasi. Dilihat dari penggunaan *Operating System* (OS) pada ponsel pintar sistem operasi Android menempati pasang pasar teratas di Indonesia.

Berdasarkan data dari GlobalStats *mobile operating system* di pasar indonesia pada per-Juni 2024 di angka 87.9% untuk pengguna OS android, 11.99% untuk pengguna OS IPhone, dan Unknown 0.01% (StatCounter, 2024). Perkembangan perangkat Android yang pesat membawa pasar aplikasi Android berkembang pesat juga. Namun, seiring dengan meningkatnya penggunaan, muncul ledakan kode berbahaya, yaitu malware seluler yang dirancang untuk menargetkan ponsel cerdas. Salah satu malware yang menargetkan ponsel cerdas adalah Trojan dengan sistem RAT (Remote Access Trojan), menempati peringkat pertama malware yang terdeteksi pada kuartal 4 di Indonesia 2023 dengan presentase infeksi 32,45%. Cara kerja malware trojan, yaitu dengan memasang diri sendirinya ke dalam aplikasi lain dan menunggu hingga sambungan internet tersedia untuk tersambung ke server guna dapat melakukan serangan *initial access* kepada *CnC-nya (Command & Control)* yang digunakan untuk mengirim perintah ke perangkat pengguna dan melakukan tindakan berbahaya (Putra, Santoso and Ardiansyah, 2022).

Dilansir dari data Bank Indonesia banyak sekali tujuan dari pelaku adalah melakukan pencurian keuangan dilakukan modus penipuan online dengan mengirimkan file surat undangan pernikahan berformat (.apk) melalu media komunikasi *online,* yaitu Whatsapp (Badan Siber dan Sandi Negara, 2023). Data yang dicuri bisa beragam, mulai dari informasi pribadi, SMS, hingga informasi perbankan rahasia seperti *One Time Password* (OTP) (Bank Indonesia, 2023).

Malware yaitu perangkat lunak berbahaya yang melakukan serangan dengan melibatkan suatu *system* (Saputro, Alfitra and Oktaviaji, 2020). Berkembangnya teknologi pun memicu dikembangkannya malware-malware baru, sehingga semakin banyak pihak yang dirugikan karena adanya malware-malware ini. Bahkan saat ini, malware telah dapat menjangkit hampir seluruh jenis sistem operasi. Malware yang berjalan pada ponsel cerdas ini berbentuk file yang dengan format Android Package Kit (APK), yang bekerja salah satunya dengan menyembunyikan aplikasi atau menghapus jejak, yang disebut "Self Hiding Behavior" (SHB). Self Hiding Behavior (SHB) dapat didefinisikan sebagai malware yang bekerja dengan menyembunyikan tindakannya agar tidak terlihat oleh user (Shan, Neamtiu dan Samuel, 2018).

Pada penelitian (Shan, Neamtiu dan Samuel, 2018) peneliti menggunakan analisis statik dengan source code analysis untuk mengetahui cara kerja malware dengan konsep SHB dengan menyembunyikan aplikasi, menyembunyikan sumber daya aplikasi, memblokir panggilan, menghapus catatan panggilan, atau memblokir dan menghapus pesan teks. Dari analisis ini sifat SHB ini mengakibatkan pengguna tidak dapat melihat aktivitas malware, namun pengguna masih dapat menggunakan aplikasi lain, tepat dibawah aktivitas malware.

Pada penelitian (Sudjayanti and Hamdani, 2024) melakukan investigasi forensik digital yang komprehensif dengan menggunakan metodologi kerangka kerja *National Institute of Standard and Technology* (NIST). Dengan teknik reverse engineering untuk memeriksa struktur dan mekanisme *hidden encoded* file APK yang bertujuan untuk mencuri informasi sensitif, seperti SMS yang

berisi OTP dan mengirimkannya melalui aplikasi telegram ke penyerang yang dapat menggunakannya untuk mengakses data pribadi dan perbankan.

Pada penelitian (Moises and Dwi Santoso, 2023) didapat gabungan dari analisis statik dan dinamik. Analisis statis dilakukan dengan teknik reverse engineering dan signature-based detection untuk mendapatkan karakteristik dari file malware tersebut, sedangkan analisis dinamik didapat dengan melakukan uji coba dengan emulator yang diberikan full access untuk mendapatkan class yang berisi host 127.0.0.1, sehingga semua data korban akan dikirim ke host.

Pada penelitian (Saputro, Alfitra and Oktaviaji, 2020) menganalisis *permission* spyware pada aplikasi Code4hk.apk dengan teknik *reverse engineering*. Setelah dilakukan dekompilasi pada file tersebut, terlihat ditemukan file qq.apk pada folder assets malware tersebut diinstall tanpa sepengetahuan pengguna. pada qq.apk (file yang didownload pada backgroud apps), malware tersebut bekerja untuk dapat mengontrol ponsel korban. Selanjutnya data dari korban akan dirik melalui akses yang terkonek ke website untuk mengcapture location pengguna. serta data dikirim ke server dengan ipaddress.

Pada penelitian (Farhan Febrianto, Budiono and Almaarif, 2019) peneliti dapat menjelaskan model konseptual pada penelitian yang memiliki tujuan untuk memeriksa paket yang dikirimkan oleh malware dan membaca karakteristik dari malware dengan membandingkan network trafficnya dengan menggunakan wireshark. Dengan menggunakan teknik *signature-based detection* untuk mencocokan api call memory yang digunakan, untuk diduga file itu malware atau tidak dan teknik reverse engineering, dengan metode static analisis ini dapat menentukan sampel untuk malware yang mengakses jaringan dilihat dari *permission*-nya.

Dalam memahami bagaimana malware bekerja di perlukan suatu analisis, salah satunya adalah analisis statik, yaitu analisis untuk mengamati perilaku malware dengan menganalisa segmen code, tanpa mengeksekusinya (Shan, Neamtiu dan Samuel, 2018). Dalam kasus ini analisis malware dengan menggunakan *reverse engineering* merupakan salah satu solusi yang bisa digunakan. *Reverse*

*engineering* dalam analisis malware berguna untuk ekstraksi data yang memuat informasi yang ada didalam malware (Putra Aldya, Widiyasono dan Pajar Setia, 2019).

Selain itu, dalam mencari karakteristik yang sama didalam sampel malware lainnya dilakukan analisis statik dengan teknik *signature-based detection*. Pada teknik ini membuat *signature* dari perilaku atau karakteristik pada malware yang memiliki *behavior* dalam upaya kebocoran informasi, upaya *jailbreak*, penyalahgunaan hak istimewa root, dan akses izin penting (Sihag et al., 2020).

Terlihat pada penelitian sebelumnya pada teknik *signature-based detection* hanya melakukan deteksi bahwa file tersebut mengandung malware, dengan membandingkan file yang diunggah terhadap database *signature* yang sudah ada, tanpa memperinci jenis aktivitas kriminal yang dilakukan seperti mengetahui karakteristik yang spesifik terhadap malware tersebut.

Karena pada permasalahan sebelumnya banyaknya kasus pencurian keuangan dengan modus menggunakan file berbentuk apk (Android Package Kit) yang dikirim melalui platform *online messanger*, sehingga file tersebut akan menjadi objek penelitian. Penelitian ini dilakukan dengan analisis statik untuk mengetahui karakteristik dari malware yang melakukan pencurian keuangan dengan teknik *reverse engineering*, dan dilakukan pencocokan pada sampel malware lainnya dengan menggunakan teknik *signature-based detection* yang akan dibuat berdasarkan *rules* yang didalamnya terdapat pola karakteristik dari malware yang melakukan pencurian keuangan.

Judul penelitian yang diusulkan, yaitu "Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android: Studi Kasus Identifikasi Pola Financial Theft dalam File APK", dengan mengimplikasikan penggunaan tools tambahan pada teknik *signature-based detection* untuk membuat aturan yang dapat mengidentifikasi komponen atau pola pencurian keuangan.

Hasil yang diharapkan pada penelitian ini adalah dapat mengetahui karakteristik

dari file sampel malware mengandung komponen pencurian keuangan serta dapat mengetahui kinerja dari kerangka pembentukan pola dari aturan yang dibuat terhadap malware yang memiliki karakteristik pencurian keuangan.

### 1.2 Rumusan Masalah

Berdasarkan hal-hal yang sudah disampaikan diatas maka rumusan permasalahan yang dijadikan fokus pada penelitian ini, sebagai berikut:

1. Bagaimana karakteristik dari malware yang memiliki potensi untuk melancarkan serangan *financial theft* pada perangkat Android?
2. Bagaimana kinerja dari nilai kecocokan *siganture-based detection* dengan rules yang dibuat terhadap sampel malware studi fokus pada serangan financial theft?

### 1.3 Batasan Masalah

Berikut batasan-batasan tersebut dibuat untuk mempersempit ruang lingkup penelitian:

1. Penelitian tidak dilakukan menggunakan analisis model machine learning.
2. Penelitian dilakukan dengan analisis statik saja, dengan *teknik reverse engineer*ing dan *signature-based detection.*
3. Dataset sample file dengan format .apk dengan fokus yang diambil dari kasus nyata berupa file yang dikirim melalui aplikasi messenger.
4. Penggunaan tools APKTools dan Enjarify dalam teknik *reverse engineering* untuk meng-decompile dan men-disassembly source code malware.
5. Penggunaan tools Bytecodeviewer dalam teknik *reverse engineering* digunakan untuk membaca code dari hasil decompile file .apk.
6. Penggunaan tools Androguard dalam teknik *reverse Engineering* digunakan untuk mempermudah analisa langsung file (.apk) dengan memasukan input command.
7. Penggunaan tools VirusTotal dalam teknik *signature-based detection* untuk mendeteksi file teridentifikasi malware atau tidak dari hash yang dimiliki.

8. Penggunaan tools YARA dalam teknik signature-based detection untuk membuat pola karakteristik dari sampel malware untuk dilakukan identifikasi sampel malware lainnya, dengan karakteristik yang sama.
9. Melakukan analisis dari file AndroidManifest.xml, MainActivity.class, string android seperti URL dan API.

## 1.4 Tujuan dan Manfaat Penelitian

Adapun tujuan dan manfaat dari dilakukannya penelitian Analisis Statik dengan Teknik *Reverse Engineering* dan *Signature Based Detection* pada Perangkat Android (Studi Kasus: Identifikasi *Pola Financial Theft* dalam File APK) adalah sebagai berikut:

### 1.4.1 Tujuan

Penelitian ini bertujuan untuk mengatasi permasalahan terkait dengan malware yang memiliki komponen atau pola yang ditujukan untuk serangan pencurian keuangan. Berikut tujuan adanya penelitian ini adalah:

1. Dapat mengidentifikasi karakteristik dari sampel malware dengan rules sesuai pada serangan financial theft.
2. Serta dapat mengetahui tingkat kinerja dari rules yang sudah dibuat sesuai dengan serangan malware yang merujuk pada *financial theft*.

### 1.4.2 Manfaat

Penelitian ini diharapkan dapat meningkatkan keamanan finansial dengan mengembangkan dan mengevaluasi metode deteksi malware yang spesifik untuk serangan pencurian keuangan, berpotensi mengurangi risiko kehilangan finansial dan memperkuat praktik keamanan siber.

## 1.5 Sistematika Penulisan

Sistematika penulisan adalah kerangka dalam penulisan skripsi. Adapun sistematika penulisan skripsi ini adalah:

BAB I PENDAHULUAN

Bab 1 berisikan penjelasan mengenai latar belakang permasalahan pada malware yang berjalan pada mobile operating system, yaitu Android. Lalu menentukan rumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan proposal penelitian.

BAB II TINJAUAN PUSTAKA

Bab 2 berisikan penjelasan mengenai landasan teori atau kajian ilmu yang berhubungan dengan berbagai pokok pikiran topik penyusunan proposal penelitian yang relevan dari sumber yang valid.

BAB III PERENCANAAN DAN REALISASI ATAU RANCANG BANGUN

Bab 3 berisikan penjelasan mengenai tahapan penelitian yang akan dilakukan, yaitu dengan melakukan analisis statik dengan teknik reverse engineering melakukan penelitian terhadap file format (.apk) sebagai objek penelitian model/framework yang akan dianalisis teknik pengumpulan serta analisis data, jadwal pelaksanaan, dan anggaran.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan pembahasan mengenai proses serta hasil dari melakukan analisis pada penelitian yang dilakukan. Pembahasan meliputi, analisa kebutuhan sistem, perancangan sistem, implementasi sistem, pengujian, data hasil pengujian, analisa data.

BAB V PENUTUP

Bab ini berisikan kesimpulan atau hasil akhir dari penelitian yang telah dilakukan, serta saran untuk penelitian berikutnya.

# BAB V
# PENUTUP

## 5.1 Kesimpulan

Dalam penelitian ini telah melakukan analisis statis malware menggunakan teknik reverse engineering dan pembuatan signature-based detection dengan YARA tools. Mengambil 1 sampel dari 30 sampel malware untuk dilakukan analisis sebagai acuan terhadap sampel lainnya yang memiliki karakteristik pencurian keuangan. Berdasarkan karakteristik yang ditemukan, dilakukan pembuatan rule dengan tool YARA. Rule yang didapatkan dari karakteristik mencakup berbagai aspek seperti Permissions, URL, BroadcastReceiver, API Bot Telegram, Notification Listener, Service, Receiver, dan Providers. Kinerja signature-based detection berdasarkan rule yang dibuat diuji ke 29 sampel malware lainnya dalam mendeteksi malware financial theft menunjukkan hasil moderat dengan total recall sebesar 55,17%, yang berarti hampir setengah dari sampel tidak terdeteksi. Meskipun beberapa rules sangat efektif (dengan recall hingga 93%), ada rules lain yang memiliki performa rendah, menunjukkan perlunya perbaikan dan optimasi lebih lanjut untuk meningkatkan cakupan deteksi secara keseluruhan.

## 5.2 Saran

Berikut saran untuk penelitian lebih lanjut, yaitu penyempurnaan pada pembuatan rule YARA dengan memperhatikan masih terdapat rule YARA dengan recall yang rendah, sehingga lebih baik menambahkan banyak signature atau kondisi yang lebih spesifik, serta melakukan analisa lebih mendalam terhadap sampel yang tidak terdeteksi. Selanjutnya melakukan pengujian dengan lebih banyak sampel malware, serta mempertimbangkan untuk mengintegrasi teknik signature-based berbasis machine learning untuk meningkatkan tingkat deteksi secara keseluruhan. Terakhir selain recall, lakukan evaluasi terhadap nilai kecocokan malware dengan metrik lainnya.

## DAFTAR PUSTAKA

Alswaina, F. and Elleithy, K. (2020) 'Android malware family classification and analysis: Current status and future directions', *Electronics (Switzerland)*. MDPI AG, pp. 1–20. Available at: https://doi.org/10.3390/electronics9060942.

Apvrille, A. (2017) 'ANDROID REVERSE ENGINEERING TOOLS: NOT THE USUAL SUSPECTS', in *VIRUS BULLETIN CONFERENCE* . France: Fortinet. Available at: https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2017-Apvrille.pdf (Accessed: 11 August 2024).

Badan Siber dan Sandi Negara (2023) *Imabuan Keamanan Penipuan dengan Modus Berkas Aplikasi Berbasis Android (.apk) melalui Surat Undangan Pernikahan*. Jakarta Selatan.

Bank Indonesia (2023) *Waspada! Modus Penipuan Online Terbaru lewat File .APK*, *Bank Indonesia*. Available at: https://www.bi.go.id/id/publikasi/ruang-media/cerita-bi/Pages/modus-penipuan-online-apk.aspx (Accessed: 1 August 2024).

BPS (2023) *Statistik Telekomunikasi Indonesia 2022*. Badan Pusat Statistik Indonesia.

Broadcom (2024) *Indonesia – Wedding invites used as lure by an SMS thief*, *Broadcom*. Available at: https://www.broadcom.com/support/security-center/protection-bulletin/indonesia-wedding-invites-used-as-lure-by-an-sms-thief (Accessed: 17 August 2024).

Cisar, P. and Pinter, R. (2019) 'Some Ethical Hacking Possibilities in Kali Linux Environment', 9(4), pp. 129–149. Available at: https://doi.org/10.24368/jates.v9i4.139.

Drabent, K., Janowski, R. and Mongay Batalla, J. (2024) 'How to Circumvent and Beat the Ransomware in Android Operating System—A Case Study of Locker.CB!tr', *Electronics (Switzerland)*, 13(11). Available at: https://doi.org/10.3390/electronics13112212.

Farhan Febrianto, A., Budiono, A. and Almaarif, A. (2019) 'ANALISIS MALWARE PADA SISTEM OPERASI ANDROID MENGGUNAKAN METODE NETWORK TRAFFIC ANALYSIS MALWARE ANALYSIS IN ANDROID OPERATING SYSTEM USING NETWORK TRAFFIC ANALYSIS METHOD', *e-Proceeding of Engineering* [Preprint].

Gyunka, B.A., Oladele, A.T. and Adegoke, O. (2023) 'Adaptive Android APKs Reverse Engineering for Features Processing in Machine Learning Malware Detection', *International Journal of Data Science*, 4(1), pp. 10–25. Available at: https://doi.org/10.18517/ijods.4.1.10-25.2023.

Hilding, M. and NORDSTRÖM, M. (2021) *DEGREE PROJECT IN MEDICAL ENGINEERING Exploring Ethical Hacking by Identifying Vulnerabilities in Motorola BabyMonitor MBP855CONNECT(4855)*.

Isecjobs (2023) *VirusTotal: A Comprehensive Analysis of a Powerful Cybersecurity Tool*, *VirusTotal*. Available at: https://isecjobs.com/insights/virustotal-explained/ (Accessed: 1 August 2024).

Juude (2016) *droidReverse*, *Github*. Available at: https://github.com/Juude/droidReverse/blob/master/README-EN.md (Accessed: 11 August 2024).

Kadir, A.F.A., Stakhanova, N. and Ghorbani, A.A. (2018) 'Understanding Android financial malware attacks: Taxonomy, characterization, and challenges', *Journal of Cyber Security and Mobility*, 7(3), pp. 1–52. Available at: https://doi.org/10.13052/jcsm2245-1439.732.

Kaspersky (2023) *IT threat evolution in Q3 2023. Mobile statistics*, *Kaspersky*. Available at: https://securelist.com/it-threat-evolution-q3-2023-mobile-statistics/111224/ (Accessed: 19 January 2024).

Lockett, A. (2021) 'Assessing the Effectiveness of YARA Rules for Signature-Based Malware Detection and Classification', in. UK. Available at: https://arxiv.org/pdf/2111.13910 (Accessed: 11 August 2024).

Lutfiana Putri, D. and Ferri Kurniawan, R. (2023) *Ramai soal Penipuan Berkedok Undangan Nikah, Pakar: Saldo Bisa Terkuras Habis*, *Kompas*.

Lysne, O. (2018) 'Reverse Engineering of Code', in *The Huawei and Snowden Questions*. Springer International Publishing, pp. 47–55. Available at: https://doi.org/10.1007/978-3-319-74950-1_6.

Masri, R. and Aldwairi, M. (2017) 'Automated malicious advertisement detection using VirusTotal, URLVoid, and TrendMicro', in *2017 8th International Conference on Information and Communication Systems, ICICS 2017*. Institute of Electrical and Electronics Engineers Inc., pp. 336–341. Available at: https://doi.org/10.1109/IACS.2017.7921994.

Moises, F. and Dwi Santoso, J. (2023) 'ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING', *JIKMA)*, 1(2).

Myat, S.M. and Kyaw, M.T. (2019) 'Analysis of Android Applications by Using Reverse Engineering Techniques', *International Journal of Innovative Science and Research Technology*, 4(3). Available at: www.ijisrt.com.

Prasetyo, B., Suryani, V. and Anbiya, D.R. (2021) 'Analisis Deteksi Malware pada Aplikasi Android Fintech berdasarkan Permissions dengan menggunakan Naive Bayes dan Random Forest', *e-Proceeding of Engineering*, p. 3.

Putra, A.D., Santoso, J.D. and Ardiansyah, I. (2022) 'Analisis Malicious Software Trojan Downloader Pada Android Menggunakan Teknik Reverse Engineering (Studi Kasus: Kamus Kesehatan v2.apk)', *Building of Informatics, Technology and Science (BITS)*, 4(1), pp. 69–79. Available at: https://doi.org/10.47065/bits.v4i1.1515.

Putra Aldya, A., Widiyasono, N. and Pajar Setia, T. (2019) 'Reverse Engineering untuk Analisis Malware Remote Access Trojan'.

Saputro, B.A., Alfitra, L.I. and Oktaviaji, R.B. (2020) 'Analisis Malware Android Menggunakan Metode Reverse Engineering', *REPOSITOR*, 2(10), pp. 1331–1337.

Shan, Z., Neamtiu, I. and Samuel, R. (2018) 'Self-hiding behavior in Android apps: Detection and characterization', in *Proceedings - International Conference on Software Engineering*. IEEE Computer Society, pp. 728–739. Available at: https://doi.org/10.1145/3180155.3180214.

Sihag, V. *et al.* (2020) *Signature based malicious behavior detection in android*, *Communications in Computer and Information Science*. Springer. Available at: https://doi.org/10.1007/978-981-15-6648-6_20.

StatCounter (2024) *Mobile Operating System Market Share Indonesia*, *StatCounter*. Available at: https://gs.statcounter.com/os-market-share/mobile/indonesia (Accessed: 29 December 2023).

Sudjayanti, S. alya and Hamdani, D. (2024) 'Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method', *Brilliance: Research of Artificial Intelligence*, 4(1), pp. 100–110. Available at: https://doi.org/10.47709/brilliance.v4i1.3800.

Zan, arunachala *et al.* (2022) 'EasyChair Preprint Security Risk Assessment Model for Cryptographic Algorithms Misuse in Mobile Payment Applications Security risk assessment model due to cryptographic algorithms misuse in mobile payment applications'.

Z.Yonatan, A. (2023) *Indonesia Jadi Negara Pemakai Handphone Terlama di Dunia 2023*, *GoodStats*. Available at: Indonesia Jadi Negara Pemakai Handphone Terlama di Dunia 2023 (Accessed: 29 December 2023).

## DAFTAR RIWAYAT HIDUP

Nadhilah Noor, akrab disapa Noor atau Dena. Lahir di Jakarta, pada tanggal 27 Agustus 2002. Penulis memulai pendidikan formal di SD Negeri 1 Tambun Selatan pada tahun 2008, setelah itu melanjutkan pendidikan di SMP Negeri 1 Bekasi pada tahun 2014, kemudian meneruskan pendidikan di SMA Negeri 1 Tambun Selatan pada tahun 2017. Pada tahun 2020 penulis menempuh pendidikan Diploma IV di Politeknik Negeri Jakarta dengan jurusan Teknik Informatika dan Komputer pada Program Studi Teknik Multimedia dan Jaringan. Penulis memiliki antusias yang tinggi dalam dunia bisnis dan teknologi.