ANALISIS RANSOMWARE MENGGUNAKAN METODE ANALISIS STATIS, DINAMIS, DAN *REVERSE ENGINEERING*.

SKRIPSI

LAYLA ROSYIDAH

2107421023

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2025

ANALISIS RANSOMWARE MENGGUNAKAN METODE ANALISIS STATIS, DINAMIS, DAN *REVERSE ENGINEERING*

SKRIPSI

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

LAYLA ROSYIDAH

2107421023

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2025

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	:	Layla Rosyidah
NIM	:	2107421023
Jurusan/Program Studi	:	Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Ransomware Menggunakan Metode Analisis Statis, Dinamis, dan *Reverse Engineering*.

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 ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 4 Juli 2025

Yang Membuat Pernyataan

Layla Rosyidah

NIM. 2107421023

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama	:	Layla Rosyidah
NIM	:	2107421023
Jurusan/Program Studi	:	Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Ransomware Menggunakan Metode Analisis Statis, Dinamis, dan *Reverse Engineering*.

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 9, Bulan Juli, Tahun 2025 dan dinyatakan **LULUS.**

Disahkan Oleh

Pembimbing I	Iik Muhamad Malik Matin, S.Kom., M.T.	( )
Penguji I	Defiana Arnaldy, S.Tp., M.Si.	( )
Penguji II	Asep Kurniawan, S.Pd., M.Kom.	( )
Penguji III	Fachroni Arbi Murad, S.Kom., M.Kom.	( )

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

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

KATA PENGANTAR

Puji dan syukur penulis ucapkan kepada Allah SWT atas berkat dan rahmat-Nya, sehingga penulis mampu menulis dan menyelesaikan skripsi yag berjudul "Analisis Ransomware Menggunakan Metode Analisis Statis, Dinamis, dan *Reverse Engineering*.". Skripsi ini ditulis dalam rangka memenuhi syarat kelulusan di Politeknik Negeri Jakarta.

Dalam proses penulisan skripsi ini, banyak pihak yang telah memberi bantuan, bimbingan, serta dukungan. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih sebesar-besarnya kepada:

1. Jurusan Teknik Informatika dan Komputer, yang telah memberikan seluruh fasilitas terbaik untuk tumbuh dan berkembang.
2. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. sebagai dosen pembimbing yang telah meluangkan waktu untuk senantiasa membimbing, memberi masukan, kritik, saran, dan pengarahan kepada Penulis dalam proses penulisan skripsi ini.
3. Bapak Suratno dan Alm. Ibu Yayah Mujenah, selaku orang tua Penulis, kepada beliau berdualah skripsi ini dipersembahkan. Terima kasih atas segala kasih sayang yang diberikan selama membesarkan Penulis, segala dukungan dan doa yang dipanjatkan dan dukungan untuk kelancaran proses penulisan skripsi ini.
4. Hary Yuliansyah, Mochamad Budi Satria, Puan Melati, Denada Anggia Pradana, dan Shakira Annisa Luthfia, sebagai abang dan kakak yang selalu mendukung, mendengarkan, memberikan ruang untuk Penulis tumbuh menjadi sosok yang akan terus berjuang keras dan menuntaskan harapan terbesar untuk mereka.
5. Hary Alfajri, sebagai sosok yang selalu menyemangati, mendengarkan seluruh keluh kesah, dan menemani Penulis untuk selalu berproses. Terima kasih untuk segala waktu, doa baik, tenaga, tawa, dan kehadiran yang tidak pernah absen disaat Penulis lelah maupun ingin menyerah. Kebersamaan

dan bantuanmu menjadi salah satu hal yang sangat berarti dalam proses menyelasaikan skripsi ini.

6. Yazmin Nur'Aini dan Nurul Aulia Dewi, yang selalu memberikan semangat, energi positif, dan kerap menanyakan kondisi penulis apapun kondisinya.
7. Seluruh sahabat Konjep, Hary Alfajri, Yazmin Nur'Aini, Nurul Aulia Dewi, Sandika Arga Pamungkas, Puguh Muammar Bramantyo, Yusuf Rafif Karback, serta Berlianna Upik N dan M. Daffa Rasyid, yang menjadi tempat berbagi cerita, semangat, dan berjuang bersama hingga akhir. Terima kasih sudah menjadi cerita terbaik yang penulis dapatkan di masa perkuliahan.
8. Teman-teman TMJ 21 yang turut memberikan dukungan selama penulisan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karena itu, segala bentuk saran dan kritik akan sangat diterima untuk menjadi evaluasi di kemudian hari. Semoga karya ini dapat memberikan manfaat dan dampak positif bagi pembaca dan pihak lain yang membutuhkan.

Depok, 4 Juli 2025

Layla Rosyidah

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama	:	Layla Rosyidah
NIM	:	2107421023
Jurusan/Program Studi	:	Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan

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

Analisis Ransomware Menggunakan Metode Analisis Statis, Dinamis, dan Reverse Engineering.

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 pernyatan ini saya buat dengan sebenarnya.

Depok, 4 Juli 2025

Yang Menyatakan

Layla Rosyidah

NIM. 2107421023

Analisis Ransomware Menggunakan Metode Analisis Statis, Dinamis, dan Reverse Engineering.

Abstrak

Ransomware merupakan salah satu jenis ancaman siber yang berkembang pesat dan semakin kompleks dari waktu ke waktu. Penelitian ini dilatarbelakangi oleh maraknya munculnya varian ransomware baru dan terbatasnya referensi yang membahas varian tersebut secara teknis mendalam. Selain itu, tidak semua penelitian terdahulu menggunakan kombinasi tiga pendekatan analisis sekaligus, yaitu analisis statis, dinamis, dan *reverse engineering*, untuk memahami struktur dan perilaku ransomware secara menyeluruh. Penelitian ini dilakukan dengan menganalisis tujuh sampel ransomware utama, yaitu LockBit, Akira, BlackCat, WhisperGate, HellCat, Morpheus dan Prince. Analisis statis menggunakan PEStudio dan teknik ekstraksi string untuk melihat struktur internal file, seperti entropi, struktur PE, dan daftar fungsi API. Analisis dinamis dilakukan menggunakan platform Any.Run untuk mengamati perilaku ransomware saat dijalankan, termasuk aktivitas proses, perubahan file dan registry, serta koneksi jaringan. *Reverse engineering* dilakukan menggunakan Ghidra untuk membedah fungsi internal, mendeteksi teknik *obfuscation*, proses dan jenis algoritma enkripsi, dan pemanggilan API secara dinamis. Hasil penelitian menunjukkan bahwa masing-masing ransomware memiliki karakteristik dan teknik yang berbeda. LockBit dan BlackCat menunjukkan struktur kompleks dan teknik evasi tingkat lanjut, sedangkan HellCat memperlihatkan perilaku hybrid sebagai stealer dan ransomware. Morpheus Stealer digunakan sebagai pembanding untuk memperjelas fitur pencurian data pada HellCat, dan sampel Prince dianalisis dengan hasil menunjukkan teknik enkripsi dan evasi tingkat lanjut. Pendekatan gabungan dari ketiga metode analisis terbukti mampu memberikan gambaran yang lebih menyeluruh terhadap teknik, struktur, dan perilaku ransomware modern.

Kata kunci: ransomware, analisis statis, analisis dinamis, *reverse engineering*, PEStudio, Ghidra, Any.Run.

DAFTAR ISI

DAFTAR GAMBAR

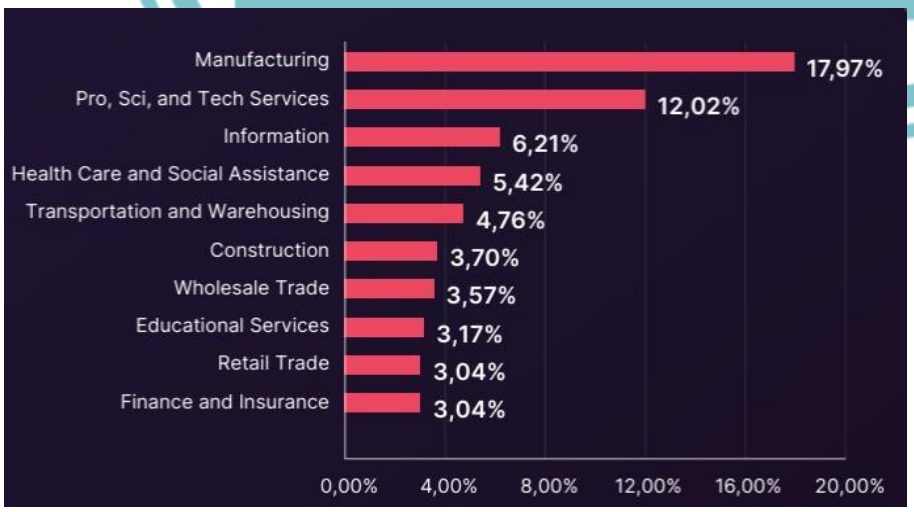
DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, teknologi informasi telah menjadi bagian penting dari kehidupan manusia. Penggunaan perangkat komputer dan internet telah menciptakan berbagai kemudahan dalam aktivitas sehari- hari, seperti komunikasi, transaksi keuangan, hingga pengelolaan data. Namun, kemajuan teknologi ini juga diiringi oleh ancaman keamanan siber yang semakin kompleks, salah satunya adalah malware. Malware memiliki karakteristik tertentu, sehingga diklasifikasikan menjadi beberapa jenis, diantaranya *virus, worm, spyware, adware, keylogger, Trojan House, rootkit,* hingga ransomware. (Mylonas dan Gritzalis, 2012).

Diantara beberapa jenis malware, ransomware menjadi jenis malware yang menjadi ancaman paling merugikan. Ransomware bekerja dengan mengenkripsi data korban dan meminta tebusan untuk pemulihannya. Teknik yang digunakan semakin canggih, seperti enkripsi tingkat lanjut, *anti-sandbox*, dan *anti-debugging*. Menurut laporan Cyberint kuartal II tahun 2024, terdapat 1.227 kasus ransomware secara global, meningkat dari kuartal sebelumnya. Indonesia sendiri mencatat 32.803 insiden yang berhasil diblokir, serta menjadi target utama dalam 24 dari 130 serangan global.Seperti yang tertera pada gambar 1.1 mengenai infografis dibawah ini.



Gambar 1. 1 Infografis Sektor Terdampak

Sumber: SOCRadar-Indonesia-Threat-Landscape-Report-2024

Dalam menghadapi ancaman tersebut, analisis malware menjadi penting untuk memahami perilaku dan dampaknya. Pendekatan yang digunakan meliputi analisis statis (mengkaji struktur tanpa eksekusi), analisis dinamis (menjalankan malware dalam lingkungan terisolasi), serta reverse engineering (membongkar kode internal dan teknik tersembunyi). Kombinasi ketiga metode ini mampu mengungkap teknik enkripsi, evasi, dan komunikasi dengan *server Command and Control* (C2) secara lebih dalam.

Berbagai penelitian telah dilakukan untuk memahami karakteristik dan perilaku malware. Nadira (2024) menganalisis malware WannaCry dan beberapa trojan menggunakan pendekatan statis dan dinamis melalui Any.Run dan Flare VM. Namun, penelitian ini belum menyentuh aspek reverse engineering secara mendalam. Cahyadi (2024) menggunakan pendekatan hybrid dan reverse engineering terhadap malware Zeus dengan tools seperti PEStudio, Cutter, dan YARA, namun terbatas pada satu sampel dan tidak membahas teknik enkripsi atau evasi modern. Noor (2024) mengkaji malware Android dengan analisis statis dan reverse engineering untuk mendeteksi pola pencurian finansial, namun tidak mencakup ransomware atau analisis dinamis. David (2021) meneliti backdoor Beast dan Slackbot menggunakan pendekatan statis dan dinamis serta implementasi aplikasi penghapus malware, namun belum mengeksplorasi teknik lanjutan seperti API dynamic resolution atau manipulasi struktur PE. Terakhir, Nicho et al. (2023) menganalisis ransomware WhisperGate dan BlackCat dengan kombinasi analisis statis, dinamis, dan memory analysis, namun cakupannya masih terbatas pada dua varian dan belum menyoroti teknik dari ransomware lain seperti LockBit atau Akira

Berbagai penelitian sebelumnya telah dilakukan, namun sebagian besar hanya berfokus pada satu jenis ransomware, tidak menyertakan analisis menyeluruh, atau belum mengeksplorasi teknik canggih seperti obfuscation dan API dynamic resolution. Oleh karena itu, penelitian ini dilakukan untuk mengisi kekosongan tersebut dengan menganalisis tujuh varian ransomware, yaitu Akira, LockBit,

BlackCat, WhisperGate, HellCat, Morpheus, dan Prince, dengan menggunakan pendekatan gabungan yang bertujuan mengungkap karakteristik teknis, pola enkripsi, serta metode evasi yang digunakan oleh ransomware modern.

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang, permasalahan yang dapat dirumuskan adalah mengenai bagaimana melakukan analisis statis, dinamis, dan *reverse engineering* terhadap ransomware Akira, LockBit, BlackCat, WhisperGate, HellCat, Morpheus, dan Prince

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang disusun guna memfokuskan ruang lingkup penelitian, adalah sebagai berikut:

a. Sampel-sampel yang digunakan adalah Ransomware Akira, LockBit BlackCat, WhisperGate, HellCat, Morpheus, dan Prince, dengan nilai hash SHA-256:
   - Akira : 5DE1061457E759E022FBC9BB02E8726A49D3ED9663FC8A77D83462C69C96AEA8
   - LockBit : F4FB0F2AE098850F2A8FFB771AE4C6C8AAA81144FE53228A2C01DF2D34307053
   - BlackCat : E160B6348F6FBDC444125B865DBD9406D99D4A8C8334C8E682EE4429F813293
   - WhisperGate : 82EF68548D2E2E4B2C41A1C92D06B30B0A433B17B859590989C89D4CE9162033
   - HellCat : B8E71845CC8CCD668A3436D1952A6C57649974BB8399E599DC33AFC4C0843BE7
   - Morpheus : 4B2EDADC8F90E9FCC976F02A9EDA1640CD92C07718C0271842FBD4CA7E2906E2
   - Prince : B7A6EB4DC4C644FE3611B0F4E69202455D61CF426726343B2FFB182C3DEB6CB8

b. Penggunaan PeStudio dan *command* Strings pada terminal untuk melakukan teknik analisis statis.

c. Penggunaan Any.Run sebagai sandbox untuk melakukan teknik analisis dinamis.
d. Penggunaan Ghidra dalam teknik *reverse engineering* untuk meng-decompile dan meng-disassembly source code malware.

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penelitian Analisis Ransomware Akira, LockBit BlackCat, WhisperGate, HellCat, Morpheus, dan Prince Menggunakan Metode Analisis Statis, Analisis Dinamis dan *Reverse Engineering,* adalah sebagai berikut:

1.4.1 Tujuan

Tujuan dari penelitian ini adalah untuk melakukan analisis statis, dinamis, dan *reverse engineering* terhadap ransomware Akira, LockBit, BlackCat, WhisperGate, HellCat, Morpheus, dan Prince.

1.4.2 Manfaat

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

a. Meningkatkan kemampuan deteksi awal serangan Ransomware Akira, LockBit BlackCat, WhisperGate, HellCat, Morpheus, dan Prince
b. Memberikan pemahaman lebih mendalam mengenai cara kerja dan karakteristik Ransomware Akira, LockBit BlackCat, WhisperGate, HellCat, Morpheus, dan Prince.
c. Menyediakan referensi bagi penelitian selanjutnya untuk mengidentifikasi ransomware serupa.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam membuat laporan penelitian ini:

a. BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

b. BAB II TINJAUAN PUSTAKA

Pada bab ini berisi landasan teori yang digunakan dan menguraikan penelitian-penelitian terkait.

c. BAB III METODE PENELITIAN

Pada bab ini berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan skenario analisis yang digunakan.

d. BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi analisis kebutuhan sistem, perancangan dan implementasi sistem, serta analisis aturan dan hasil yang diperoleh.

e. BAB V PENUTUP

Pada bab ini berisi kesimpulan dari hasil analisis serta saran-saran untuk penelitian selanjutnya.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan temuan dari ketiga pendekatan yang digunakan dalam penelitian ini, terdapat beberapa kesimpulan mengenai hasil analisis. Secara statis, sebagian besar menunjukkan entropi tinggi, entry point tidak lazim, dan struktur PE yang dimodifikasi, mengindikasikan teknik *obfuscation* dan evasi. Analisis dinamis mengungkap aktivitas berbahaya seperti enkripsi file, modifikasi registry, koneksi ke server C2, dan pembuatan proses baru. *Reverse engineering* mengidentifikasi teknik lanjutan seperti TLS *callback*, *ordinal import*, dan *dynamic API resolution*. LockBit dan BlackCat fokus pada persistensi dan penyamaran, WhisperGate bersifat destruktif, sementara HellCat bersifat hybrid dengan kemampuan mencuri data. Prince menunjukkan kompleksitas tinggi dengan kombinasi enkripsi AES-GCM dan ChaCha20 serta teknik injection. Pendekatan multi-analisis terbukti efektif dalam mengungkap struktur, perilaku, dan logika internal masing-masing ransomware.

5.2 Saran

Berdasarkan hasil dan kesimpulan yang telah diperoleh, berikut adalah beberapa saran yang dapat diberikan untuk keperluan penelitian selanjutnya:

1. Penelitian ini hanya menggunakan disassembly sebagai teknik yang digunakan dalam *reverse* engineering, namun belum mencakup proses debugging untuk analisis lebih dalam. Sementara penggunaan metode tersebut sangat berguna untuk mengamati jalannya eksekusi program secara langsung, terutama mengidentifikasi fungsi enkripsi, proses *obfuscation*, runtime, dan manipulasi memori.
2. Dalam analisis statis, penelitian ini belum dilakukan eksplorasi kode biner secara langsung melalui hex editor.
3. Penggunaan Any.Run sebagai sandbox cloud masih terbatas pada konfigurasi tertentu. Penggunaan sandbox lain, seperti cuckoo atau falcon memungkinkan peneliti mampu mengatur scenario analisis yang lebih dalam dan flexible

DAFTAR PUSTAKA

Appelbaum, D. (2012). *Reverse engineering: Fundamental analysis for technical analysts*. Wiley Finance.

Cahyadi, A. (2024*). Deteksi malware Zeus menggunakan analisis hybrid dan YARA rules.* Jurnal Teknologi Informasi dan Keamanan Siber, 5(1), 22–31.

David, A. P. (2021). *Ghidra: Software reverse engineering tool by NSA*. Journal of Cybersecurity Tools, 6(3), 45–52.

Mylonas, A., & Gritzalis, D. (2012). *Malware analysis techniques and cybersecurity measures*. Journal of Information Security, 3(4), 245–254.

Nadira, S. (2024). *Analisis malware WannaCry dan Trojan menggunakan metode statis dan dinamis.* Jurnal Keamanan Siber Indonesia, 4(2), 60–72.

Nicho, D., et al. (2023). *Analyzing WhisperGate and BlackCat malware: Methodology and threat perspective*. Journal of Advanced Threat Intelligence, 7(1), 77–90.

Noor, L. (2024). *Identifikasi pola financial theft dalam file APK menggunakan reverse engineering.* Jurnal Rekayasa Perangkat Lunak, 3(2), 90–101.

Peppers, M. (2018). *Building a malware analysis lab*. Syngress.

Puji Rahayu, & Trianto, N. (2021). *Malware dan keamanan sistem informasi*. Andi Publisher.

Rizqina, F. (2022). *ANY.RUN sebagai platform analisis dinamis malware interaktif*. Jurnal Sistem dan Keamanan Siber, 2(1), 15–22.

Sato, H. (2024). *Real-time malware detection with Any.Run*. Proceedings of the Cyber Defense Symposium.

Siddiq, M., et al. (2020). *Static PE analysis using PEStudio for malware detection*. Journal of Applied Cybersecurity.

Wahib, M., et al. (2022). *Ancaman siber dan strategi pertahanan digital di Indonesia*. Jurnal Teknologi dan Keamanan Digital, 3(3), 180–195.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security (4th ed.)*. Cengage Learning.

Asghar, H. J., Zhao, B. Z. H., Ikram, M., Nguyen, G., Kaafar, D., Lamont, S., & Coscia, D. (2024). Use of cryptography in malware obfuscation. *Journal of Computer Virology and Hacking Techniques*, *20*(1), 135–152. https://doi.org/10.1007/s11416-023-00504-y

Banik, S. (2023). *STATIC ANALYSIS & IDENTIFICATION OF*. *11*(5), 243–258.

Bhardwaj, S., & Singh Arri, H. (2024). A Comprehensive Study of Efficient and Accurate Malware Detection Using Static and Dynamic Analysis Methods. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4502178

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2022). Comparison of Entropy Calculation Methods for Ransomware Encrypted File Identification. *Entropy*, *24*(10). https://doi.org/10.3390/e24101503

Gururaj H, L., Soundarya B, C., Janhavi, V., Lakshmi, H., & Prassan Kumar, M. J. (2022). Analysis of Cyber Security Attacks using Kali Linux. *IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2022*, *November*. https://doi.org/10.1109/ICDCECE53908.2022.9793164

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

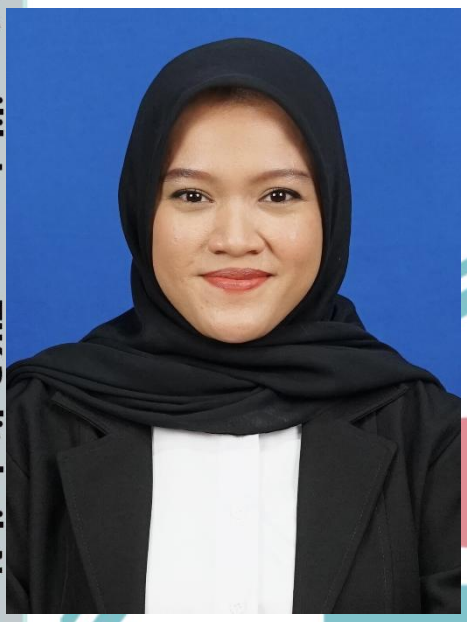
Kurnia Hatika, L., Budiyono, A., & Almaarif, A. (2019). *Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis Accuracy Analysis of Malware Detection in Antivirus Software Using Static Analysis Method*. *6*(2), 7812–7819.

Mehmood, R., Ahmed, W., Riaz, R., & Awan, W. H. (2024). *Modern Malware Evasion and Bypass Strategies Against Contemporary Antivirus Software*. *3429*(2).

Mylonas, A., & Gritzalis, D. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. In *Computers & Security* (Vol. 31, Issue 6). No Starch Press. https://doi.org/10.1016/j.cose.2012.05.004

Sato, L. (2024). *Analysing malware evasion techniques Decoding Malicious Camouflage : Analysing Evasion Techniques in Malware Against EDR and AMSI Detection by*. *December*, 0–64. https://doi.org/10.13140/RG.2.2.12937.76641

DAFTAR RIWAYAT HIDUP



Layla Rosyidah

Lahir di Jakarta, 1 Maret 2002, anak ketiga dari tiga bersaudara. Lulus dari SDN 18 Kramat Jati pada tahun 2014, kemudian melanjutkan pendidikan di SMPN 150 Jakarta Timur dan lulus pada tahun 2017, dan selanjutnya di SMAN 93 Jakarta Timur dan lulus pada tahun 2020. Setelah *gap year* selama kurun waktu 1 tahun, tepatnya 2021 melanjutkan studi di Politeknik Negeri Jakarta pada Jurusan Teknik Informatika dan Komputer di Program Studi Teknik Multimedia dan Jurusan.