PERBANDINGAN ANALISIS STATIS DAN DINAMIS PADA DETEKSI *WANNACRY RANSOMWARE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

Luqman Agus Dwiyono
09011382025148

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

PERBANDINGAN ANALISIS STATIS DAN DINAMIS PADA DETEKSI *WANNACRY RANSOMWARE*

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh:

Luqman Agus Dwiyono

09011382025148

Palembang, 16 Januari 2025

Pembimbing I	Pembimbing II
Prof. Ir. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP.197806172006041002	NIP. 199211102023212049

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

AUTHENTICATION PAGE

COMPARISON OF STATIC AND DYNAMIC ANALYSIS IN WANNACRY RANSOMWARE DETECTION

THESIS

Dept. of Computer Syatem

Bachelor's Degree

By:

Luqman Agus Dwiyono

09011382025148

Palembang, 16 January 2025

Supervisor	Co-Supervisor
Prof. Ir. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP.197806172006041002	NIP. 199211102023212049

Acknowledge,

Head of Computer System Department

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada:

Hari : **Kamis**

Tanggal : **9 Januari 2024**

Tim Penguji

1. **Ketua** : **Huda Ubaya, S.T., M.T.**
2. **Penguji** : **Dr. Ahmad Zarkasi, M.T.**
3. **Pembimbing I** : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II** : **Nurul Afifah, M.Kom.**

Mengetahui, 4/1/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Luqman Agus Dwiyono

NIM : 09011382025148

Judul : Perbandingan Analisis Statis dan Dinamis Pada Deteksi *WannaCry Ransomware*

Hasil Pengecekan Software iThenticate/Turnitin: 9%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, Januari 2025

Luqman Agus Dwiyono

NIM.09011382025148

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbil'alamin. Segala Puji dan Syukur Panjatkan Kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya. Sholawat serta salam kepada Rasulullah Shallalllahu Alaihi Wasallam yang senantiasa menjadi sumber inspirasi dan teladan terbaik untuk umat manusia Dimana hingga saat ini penulis bisa menyelesaikan penulisan Tugas Akhir ini yang berjudul **"Perbandingan Analisis Statis Dan Dinamis Pada Deteksi *WannaCry Ransomware*"** dengan baik dan lancar.

Tujuan dari penulisan Tugas Akhir ini adalah untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian serta observasi dari berbagai sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Atas selesainya Tugas Akhir ini, penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa, dan juga terima kasih kepada yang terhormat:

1. Allah SWT yang telah memberikan saya nikmat Kesehatan, kesempatan serta Rahmat-Nya sehingga saya dimudahkan dalam penyelesaian skripsi ini dengan baik.
2. Kedua orang tua saya tercinta Bapak Mulyono dan Ibu Tri Turini, S.Pd. dan keluarga besar yang selalu mendoakan serta memberikan dukungan dan semangat yang besar selama penyelesaian Tugas Akhir ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Tugas Akhir.
6. Ibu Nurul Afifah, M.Kom., Dosen Pembimbing II Tugas Akhir.
7. Bapak Iman Saladin B. Azhar, S.Kom., M.MSI., selaku Dosen Pembimbing Akademik.

8. Mba Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
9. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya yang tidak bisa saya sebutkan satu persatu.
10. Seluruh teman-teman seperjuangan Angkatan 2020 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan doa dan bantuan dalam penyelesaian Tugas Akhir ini.
12. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Oleh karena itu, segala saran dan kritik sangatla penting bagi penulis. Akhir kata, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi Akademik.

Palembang, Januari 2025
Penulis,

Luqman Agus Dwiyono
NIM. 09011382025148

PERBANDINGAN ANALISIS STATIS DAN DINAMIS PADA DETEKSI *WANNACRY RANSOMWARE*

Luqman Agus Dwiyono (09011382025148)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : luqman.agus2002@gmail.com

ABSTRAK

Ransomware adalah jenis *malware* yang mengenkripsi data korban dan meminta tebusan untuk mengembalikan aksesnya, dengan *WannaCry* sebagai salah satu varian terkenal yang memanfaatkan eksploitasi EternalBlue pada protokol SMB. Penelitian ini membandingkan metode analisis statis dan dinamis dalam mendeteksi *WannaCry ransomware* untuk menilai efektivitas keduanya. Analisis statis dilakukan tanpa mengeksekusi *ransomware*, menggunakan tools seperti Exeinfo PE, HxD Editor, dan PeStudio untuk mengidentifikasi struktur internal, sedangkan analisis dinamis melibatkan eksekusi *ransomware* dalam lingkungan terisolasi dengan *tools* seperti Process Monitor, Wireshark, dan RegShot untuk mengamati perilaku *runtime*. Hasil penelitian menunjukkan bahwa kedua metode memiliki tingkat deteksi 100% dengan keunggulan masing-masing, di mana analisis statis unggul dalam kecepatan deteksi awal dan keamanan, sementara analisis dinamis memberikan pemahaman mendalam tentang perilaku *ransomware*. Kombinasi keduanya memberikan pendekatan yang lebih komprehensif dalam mendeteksi dan memahami *WannaCry ransomware*, yang diharapkan dapat menjadi dasar pengembangan metode deteksi yang lebih efektif di masa depan.

Kata Kunci: *WannaCry, ransomware,* analisis statis, analisis dinamis, deteksi *malware.*

COMPARISON OF STATIC AND DYNAMIC ANALYSIS IN WANNACRY RANSOMWARE DETECTION

Luqman Agus Dwiyono (09011382025148)

Dept. Of Computer System, Faculty of Computer Science, Sriwijaya University

Email : luqman.agus2002@gmail.com

ABSTRACT

Ransomware is a type of malware that encrypts the victim's data and demands a ransom to restore access, with WannaCry being one of the most notorious variants exploiting EternalBlue on the SMB protocol. This study compares static and dynamic analysis methods in detecting WannaCry ransomware to evaluate their effectiveness. Static analysis is performed without executing the ransomware, using tools such as Exeinfo PE, HxD Editor, and PeStudio to identify its internal structure. On the other hand, dynamic analysis involves executing the ransomware in an isolated environment using tools like Process Monitor, Wireshark, and RegShot to observe its runtime behavior. The study results show that both methods achieve a 100% detection rate, each with its strengths: static analysis excels in initial detection speed and safety, while dynamic analysis provides a deeper understanding of the ransomware's behavior. The combination of these methods offers a more comprehensive approach to detecting and understanding WannaCry ransomware, which is expected to serve as a foundation for developing more effective detection methods in the future.

Keywords*: WannaCry, ransomware, static analysis, dynamic analysis, malware detection.*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Ransomware adalah jenis *malware* yang mengenkripsi data korban dan menuntut pembayaran sebagai imbalan untuk kunci dekripsi [1]. Informasi yang mungkin terenkripsi melibatkan data keuangan, catatan bisnis, database, dan kenangan pribadi seperti foto dan video [2]. Setelah identifikasi data, *ransomware* menggunakan kunci unik yang hanya diketahui oleh penyerang untuk mengunci akses ke informasi tersebut. Korban perlu membayar uang tebusan yang diminta oleh penyerang untuk mendapatkan kunci dekripsi, untuk bisa memulihkan data dan sistem mereka [3]. Salah satu serangan *ransomware* yang cukup terkenal adalah *WannaCry*, yang menyerang ribuan komputer di seluruh dunia pada tahun 2017 [4].

Tanggal 12 Mei 2017, serangan *WannaCry* dimulai dan dalam waktu singkat berhasil menyebar ke lebih dari 230.000 komputer di lebih dari 150 negara, termasuk Amerika Serikat, Inggris, Spanyol, Rusia, Prancis, dan Jepang [5]. *WannaCry* menargetkan komputer yang menggunakan sistem operasi Windows dengan mengeksploitasi kerentanan dalam protokol *Server Message Block* (SMB) yang dikenal sebagai *EternalBlue* [6]. Kerentanan ini awalnya ditemukan oleh Badan Keamanan Nasional AS (NSA) dan kemudian dibocorkan oleh kelompok peretas *Shadow Brokers* pada April 2017 [7].

WannaCry bekerja dengan mengenkripsi file di komputer yang terinfeksi dan meminta pembayaran tebusan dalam *Bitcoin* untuk membuka enkripsi file tersebut [8]. Setelah berhasil menginfeksi sistem, *WannaCry* akan memindai jaringan lokal untuk mencari komputer lain yang juga rentan terhadap eksploitasi serupa, sehingga mempercepat penyebarannya. Ketika file sudah dienkripsi, pengguna akan menerima pesan tebusan yang menuntut pembayaran antara $300 hingga $600 dalam bentuk *Bitcoin* untuk mendapatkan kunci dekripsi [5].

Serangan *WannaCry* menyoroti kebutuhan akan deteksi cepat dalam menangani risiko keamanan digital. Dua metode yang umum digunakan dalam mendeteksi *malware* seperti *ransomware* adalah analisis statis dan dinamis [9]. Dalam tahap

pelaksanaan penelitian ini, langkah awalnya adalah menciptakan lingkungan yang aman melalui penggunaan *virtual machine*. Setelah itu, pencarian sampel *ransomware* dilakukan untuk analisis lebih lanjut. Prosedur berikutnya melibatkan analisis statis dengan mengecek langsung struktur file *ransomware*, termasuk *import* dan pustaka yang digunakan, tanpa menjalankannya. Langkah terakhir melibatkan analisis dinamis, di mana sampel *ransomware* dijalankan dalam lingkungan terisolasi untuk memahami perilaku yang muncul saat *ransomware* aktif.

Penelitian ini [10], membahas tentang analisis statis menggunakan *reverse engineering*. Alasan utama melakukan *reverse engineering WannaCry ransomware* adalah untuk memahami perilakunya, mengidentifikasi modul kode yang melaksanakan fungsi tertentu, dan mengungkap alasannya disebut demikian.

Penelitian [11], membahas tentang analisis dinamis yang melibatkan eksekusi *malware* dan perbandingan perubahan antara status terinfeksi dan lingkungan awal. Selama proses eksekusi, *malware* berinteraksi dengan sistem *host* melalui empat aspek utama: proses, sistem file, *registry*, dan aktivitas jaringan.

Penelitian selanjutnya [12], membahas tiga pendekatan utama dalam mendeteksi *malware* yaitu analisis statis, dinamis, dan hibrid. Analisis statis melibatkan pemeriksaan kode *malware* tanpa menjalankannya, memungkinkan deteksi melalui *signature based* dan aturan heuristik. Sementara itu, analisis dinamis melibatkan eksekusi *malware* dalam lingkungan yang terkendali untuk mengamati perilaku saat *runtime*. Pendekatan hibrid menggabungkan kelebihan kedua metode ini untuk meningkatkan akurasi deteksi dan pemahaman lebih dalam tentang *malware*.

Pada penelitian [13], Membahas analisis *ransomware* menggunakan teknik *reverse engineering* dalam menganalisis *ransomware* guna menciptakan langkah-langkah pencegahan yang efisien. Penulis menggambarkan cara memahami perilaku *ransomware* melalui dekompilasi kode serta mengkaji struktur dan perilaku *malware* tersebut. Dengan menerapkan teknik analisis statis dan dinamis, peneliti berhasil menemukan pola serangan dan kelemahan dalam kode *malware*.

Penelitian [14], membahas metode deteksi menyeluruh untuk *WannaCry ransomware*. Jurnal ini mencakup prinsip utama, aturan deteksi, serta eksperimen yang dilakukan untuk mengenali dan mencegah penyebarannya. Jurnal ini menggabungkan analisis statis dan dinamis untuk mengidentifikasi ciri khas *ransomware* tersebut dan mengevaluasi efektivitas metode deteksi melalui serangkaian eksperimen. Hasil penelitian menunjukkan bahwa pendekatan deteksi komprehensif ini mampu secara efektif mengenali dan mengatasi ancaman *WannaCry ransomware*.

Penelitian ini [8], membahas teknik analisis forensik yang digunakan untuk memahami dan menangani *ransomware*. Penelitian ini juga menguraikan berbagai pendekatan yang digunakan untuk mendeteksi, menganalisis, dan mengurangi dampak *ransomware*. Peneliti menyarankan penggunaan metode manual untuk menganalisis *malware* secara dinamis, memfasilitasi pemahaman yang lebih baik terhadap perilaku *ransomware* bagi peneliti keamanan dan analis *malware*. *Tools* seperti Forensik Volatilitas, Regshot, dan FTK Imager Lite digunakan dalam lingkungan yang aman dan *virtual*.

Pada penelitian [9], membahas berbagai teknik dan *tools* terbaru dalam analisis *malware*, dengan mengulas perbandingan antara analisis statis, dinamis, dan hibrid. Analisis statis meneliti kode tanpa menjalankan program, sementara analisis dinamis mengamati aktivitas program saat dijalankan. Metode hibrid mengkombinasikan kedua pendekatan untuk meningkatkan akurasi dan efisiensi deteksi *malware*. Jurnal ini juga meninjau *tools* populer yang digunakan dalam setiap metode, serta mengevaluasi efektivitasnya dalam berbagai lingkungan.

Hasil analisis data dari penelitian ini dapat digunakan untuk mengidentifikasi metode mana yang lebih efektif. Untuk mendukung penelitian ini, informasi tambahan dari riset lainnya diperlukan. Dengan adanya studi analisis *ransomware* ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan keilmuan forensik terkait *ransomware* di masa mendatang.

Bedasarkan uraian diatas, maka dari itu penulis akan melakukan penelitian dengan judul **"Perbandingan Analisis Statis Dan Dinamis Pada Deteksi Wannacry Ransomware".**

1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan tugas akhir ini:

1. Bagaimana cara identifikasi *ransomware* menggunakan metode analisis statis?
2. Bagaimana cara identifikasi *ransomware* menggunakan metode analisis dinamis?
3. Bagaimana performa dari kedua metode yang digunakan?

1.3 Tujuan

Adapun tujuan dari penulisan tugas akhir ini yaitu:

1. Dapat mengidentifikasi serangan *ransomware* dengan metode analisis statis.
2. Dapat mengidentifikasi serangan *ransomware* dengan metode analisis dinamis.
3. Dapat Mengukur hasil performa dari kedua metode yang digunakan.

1.4 Manfaat

Berikut manfaat dari penulisan tugas akhir ini, yaitu:

1. Melalui analisis statis, dapat diidentifikasi serta dijelaskan struktur *ransomware* dan perilaku tersembunyi yang tidak terlihat saat dilakukan analisis dinamis.
2. Melalui analisis dinamis dapat mengetahui dan menampilkan bagaimana *ransomware* bekerja saat dijalankan pada sistem.
3. Memberikan pemahaman yang lebih mendalam tentang performa kedua metode.

1.5 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu:

1. Serangan *ransomware* yang dibahas adalah *WannaCry ransomware*.

2. Deteksi serangan *WannaCry ransomware* yang menggunakan metode analisis statis dan dinamis.
3. Deteksi akan dilakukan pada *virtual machine* dengan sistem operasi Windows 10 yang dijalankan pada virtualbox.
4. Dalam penelitian ini tidak membahas bagaimana cara pencegahan dari serangan *WannaCry ransomware*.

1.6 Metode Penelitian

Dalam tugas akhir ini akan menggunakan metodologi dan melewati beberapa tahapan sebagai berikut:

1. Tahap Pertama (Studi Pustaka/Studi Literatur)

   Tahap ini dilakukan setelah masalah yang didapatkan telah sesuai untuk dijadikan sebagai penelitian, membaca artikel, jurnal atau makalah yang berhubungan dengan tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

   Pada Tahap ini menyiapkan *ransomware* yang akan dideteksi, *software* untuk mendeteksi *ransomware*, yaitu Windows 10 yang terdapat pada VirtualBox. Bertujuan untuk membuat tempat yang terisolasi untuk mendeteksi *ransomware* sehingga tidak terjadi hal yang tidak diinginkan.

3. Tahap Ketiga (Pengujian)

   Pada tahap ini proses analisis dinamis dilakukan dengan cara mengeksekusi *ransomware* sehingga perilaku *ransomware* dapat terlihat. Sedangkan analisis statis dilakukan tanpa mengeksekusi *ransomware*, melainkan dengan melihat struktur file dari *ransomware* tersebut.

4. Tahap Keempat (Hasil dan Analisa)

   Tahap ini dilakukan analisa dari setiap metode untuk dapat melihat kelebihan dan kekurangan setiap analisis dan meliihat analisis yang lebih efektif.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahapan ini merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan.

1.7 Sistematika Penelitian

Adapun sistematika dalam penulisan tugas akhir ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, identifikasi masalah, menentukan batasan masalah yang akan dibahas, menjabarkan tujuan dan manfaat dari penelitian ini, asumsi metodologi serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi berbagai teori yang digunakan sebagai landasan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini, bahasan dalam bagian ini mengenai pembahasan teori dasar yang digunakan dalam penelitian, terkait *ransomware* serta *tools* untuk melaksanakan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang objek dan jenis penelitian, data dan sumber data, teknik mengumpulkan data, dan skema pengerjaan penelitian.

BAB IV HASIL DAN ANALISA

Bab ini berisi hasil dari pengujian serta penjelasan sesuai perencanaan yang telah dibuat sebelumnya. Pengujian dilakukan untuk memastikan dan membuktikan bahwa hasil akhir yang didapat sesuai dengan ekspektasi, perkiraan dan fakta yang ada.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang menjelaskan hasil akhir dari penelitian, tercapai atau tidaknya tujuan penelitian, serta

menjelaskan kelebihan dan kekurangan yang terdapat pada sistem yang telah dibuat. Sementara itu saran berisi tentang hal-hal yang dapat diperbaiki dan dikembangkan lagi ke depannya, terutama mengenai kekurangan yang masih terdapat pada sistem tersebut.

DAFTAR PUSTAKA

[1] A. L. Y. Ren, C. T. Liang, I. J. Hyug, S. N. Brohi, and N. Z. Jhanjhi, "A three-level ransomware detection and prevention mechanism," *EAI Endorsed Trans. Energy Web*, vol. 7, no. 26, pp. 1–7, 2020, doi: 10.4108/eai.13-7-2018.162691.

[2] S. D. Mukesh, "An Analysis Technique to Detect Ransomware Threat," *2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2018*, pp. 1–5, 2018, doi: 10.1109/ICCCI.2018.8441502.

[3] T. Xia, Y. Sun, S. Zhu, Z. Rasheed, and K. Shafique, "Toward A Network-Assisted Approach for Effective Ransomware Detection," *ICST Trans. Secur. Saf.*, p. 168506, 2018, doi: 10.4108/eai.28-1-2021.168506.

[4] S. Razaulla *et al.*, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access*, vol. 11, no. February, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.

[5] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, pp. 180–185, 2018, doi: 10.1109/SPW.2018.00033.

[6] Q. Kang and Y. Gu, "A Survey on Ransomware Threats: Contrasting Static and Dynamic Analysis Methods," *Researchgate*, 2023, doi: 10.20944/preprints202311.0798.v1.

[7] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry," *Comput. Electr. Eng.*, vol. 76, pp. 111–121, 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[8] A. K. Agrawal*, S. Sah, and D. P. Khatri, "Forensic Analysis of a Ransomware," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 3, pp. 3618–3622, 2020, doi: 10.35940/ijitee.c8385.019320.

[9] A. Datta, K. A. Kumar, and A. D, "An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis," *Int. J. Eng. Res. Technol.*, vol. 10, no. 4, pp. 112–116, 2021, [Online]. Available: www.ijert.org

[10] S. C. Hsiao and D. Y. Kao, "The static analysis of WannaCry ransomware," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018-Febru, pp. 153–158, 2018, doi: 10.23919/ICACT.2018.8323680.

[11] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware - IEEE Conference Publication," *Int. Conf. Adv. Commun. Technolo gy(ICACT*, pp. 159–166, 2018, [Online]. Available: http://ieeexplore.ieee.org/document/8323682/media

[12] A.-R. Belea, “Methods for Detecting Malware Using Static, Dynamic and Hybrid Analysis,” vol. X, p. 2023, 2023.

[13] N. Alsharabi, M. F. Alshammari, and Y. Alharbi, “Analysis of Ransomware Using Reverse Engineering Techniques to Develop Effective Countermeasures,” *J. Adv. Inf. Technol.*, vol. 14, no. 2, pp. 284–294, 2023, doi: 10.12720/jait.14.2.284-294.

[14] G. Lu, Y. Liu, Y. Chen, C. Zhang, Y. Gao, and G. Zhong, “A Comprehensive Detection Approach of Wannacry: Principles, Rules and Experiments,” *Proc. - 2020 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2020*, pp. 41–49, 2020, doi: 10.1109/CyberC49757.2020.00017.

[15] Y. A. Ahmed, B. Koçer, and B. A. S. Al-Rimy, “Automated Analysis Approach for the Detection of High Survivable Ransomware,” *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 5, pp. 2236–2257, 2020, doi: 10.3837/tiis.2020.05.021.

[16] J. Hwang, J. Kim, S. Lee, and K. Kim, “Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques,” *Wirel. Pers. Commun.*, vol. 112, no. 4, pp. 2597–2609, 2020, doi: 10.1007/s11277-020-07166-9.

[17] B. Jethva, I. Traoré, A. Ghaleb, K. Ganame, and S. Ahmed, “Multilayer ransomware detection using grouped *registry* key operations, file entropy and file signature monitoring,” *J. Comput. Secur.*, vol. 28, no. 3, pp. 337–373, 2020, doi: 10.3233/JCS-191346.

[18] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, and W. J. Buchanan, “Ransomware: Analysing the Impact on Windows Active Directory Domain Services,” *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030953.

[19] M. Izham Jaya and M. F. A. Razak, “Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers,” *Int. J. Informatics Vis.*, vol. 6, no. 2, pp. 469–474, 2022, doi: 10.30630/joiv.6.2-2.1093.

[20] D. Maria Devi and Rs. Kumar, “Malware Analysis in Windows System,” *Int. J. Adv. Trends Eng.*, no. 3, pp. 2456–1126, 2021, [Online]. Available: www.ijatest.org

[21] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms,” *J. Telecommun. Inf. Technol.*, no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[22] D. F. Netto, K. M. Shony, and E. R. Lalson, “An Integrated Approach for Detecting Ransomware Using Static and Dynamic Analysis,” *2018 Int. CET Conf. Control. Commun. Comput. IC4 2018*, pp. 410–414, 2018, doi: 10.1109/CETIC4.2018.8531017.

[23] C. J. W. Chew and V. Kumar, “EPiC Series in Computing Behaviour Based Ransomware Detection,” vol. 58, pp. 127–136, 2019.

[24] A. Oktaviani and M. Syafrizal, “GandCrab Ransomware Analysis on Windows Using Static Method,” *Bul. Ilm. Sarj. Tek. Elektro*, vol. 3, no. 2, pp. 163–175, 2021, doi: 10.12928/biste.v3i2.4884.

[25] Red Hat, “What is a virtual machine (VM)?,” *Red Hat*, 2024. https://www.redhat.com/en/topics/virtualization/what-is-a-virtual-machine

[26] Bitdefender Enterprise, “The Differences Between Static and Dynamic Malware Analysis,” *Bitdefender Enterprise*, 2023. https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/