BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang begitu pesat telah membawa banyak kemudahan dalam berbagai aspek kehidupan, mulai dari komunikasi, pendidikan, bisnis, hingga pemerintahan (Schelenz & Pawelec, 2022). Namun, kemajuan ini juga dibarengi dengan meningkatnya ancaman di dunia maya atau yang dikenal dengan istilah *cybersecurity* (Saeed dkk., 2023). Salah satu ancaman yang paling sering ditemui dan memiliki dampak besar adalah *malware* (*malicious software*), *malware* merupakan program yang sengaja dirancang untuk menyusup ke dalam sistem komputer dengan tujuan merusak, mencuri data, atau mengganggu kinerja sistem tanpa sepengetahuan maupun izin dari pengguna (Yousuf dkk., 2023)

Malware dapat muncul dalam berbagai bentuk yang beragam, antara lain virus, *worm*, *trojan*, *ransomware*, *spyware*, *adware*, serta jenis-jenis perangkat lunak berbahaya lainnya (Djenna dkk., 2023). Serangan *malware* dapat menyebabkan kerusakan sistem komputer, pencurian data yang bersifat sensitif, hingga gangguan atau bahkan penghentian layanan penting. Dampak ini menjadi sangat signifikan apabila menyerang sektor-sektor strategis seperti perbankan, layanan kesehatan, maupun instansi pemerintahan, (Shehab dkk., (2024). Sistem operasi *Windows* merupakan sistem yang paling banyak digunakan di seluruh dunia, menjadi target utama berbagai jenis *malware* yang terus berkembang dalam hal teknik penyebaran maupun penyamaran (Devi dkk., 2021).

Dalam upaya untuk mengatasi tantangan *malware*, pendekatan-pendekatan dalam analisis *malware* terus dikembangkan. Salah satu pendekatan yang cukup efektif adalah *memory forensics* (Das, 2022). *Memory forensics* yaitu proses pemeriksaan memori utama *RAM* komputer untuk menemukan artefak digital yang menunjukkan adanya aktivitas mencurigakan atau indikasi keberadaan *malware* (Azzery dkk., 2022). Teknik ini sangat berguna terutama dalam mendeteksi jenis *malware* yang tidak meninggalkan jejak di disk (*fileless malware*) dan hanya beroperasi di memori selama waktu eksekusi (Mujtaba dkk., 2025).

YARA merupakan *framework* untuk mengidentifikasi *malware* berdasarkan pola atau karakteristik tertentu dituliskan dalam bentuk aturan yang kemudian bisa digunakan untuk mencocokkan berbagai data termasuk *file*, *folder*, maupun *memory dump* (Patil dkk., 2025). *YARA rules* memiliki fleksibilitas dan keakuratan tinggi menjadikannya alat penting dalam proses pendeteksian *malware* yang tidak terdeteksi oleh metode tradisional berbasis *signature* (Jadhav & Jadhav, 2024).

Penelitian ini akan melakukan analisis sampel *malware* yang berjenis *Remote Access Trojan* dengan nama *ramez.exe* menggunakan pendekatan *memory forensics* dan *YARA rules* pada sistem operasi *Windows 10*. Pemilihan *malware* ini didasarkan pada karakteristiknya yang mewakili tipe ancaman umum yang sering ditemui dalam berbagai insiden keamanan siber di dunia nyata. *Malware* ini juga menunjukkan perilaku mencurigakan saat dijalankan di lingkungan uji, sehingga dianggap relevan dan penting untuk diteliti lebih lanjut guna memahami cara kerjanya serta potensi dampak yang dapat ditimbulkan.

Beberapa penelitian sebelumnya telah menunjukkan efektivitas pendekatan serupa. Contohnya, studi oleh (Shree dkk., 2021) Forensik memori juga berperan dalam memahami dan mendeteksi *malware* melalui analisis statis dan dinamis, serta digunakan sebagai strategi pertahanan terhadap ancaman seperti *rootkit* dan eksploitasi *zero-day*. Penelitian lain oleh (Gupta dkk., 2024) berjudul "*Living off the Analyst: Harvesting Features from Yara Rules for Malware Detection*" bahwa fitur yang diekstrak dari *YARA rules* dapat meningkatkan deteksi *malware* secara efisien dengan memanfaatkan *sub-signatures* dari *YARA* sebagai fitur tambahan.

Penelitian ini memiliki tujuan untuk mengeksplorasi potensi penerapan teknik *memory forensics* bersama dengan *YARA rules* dalam melakukan analisis *malware* pada sistem operasi Windows 10. Sinergi kedua metode tersebut diharapkan mampu menghasilkan pemahaman yang lebih mendalam dan terperinci terkait aktivitas serta perilaku *malware*. Selain itu, penelitian ini juga memanfaatkan pendekatan analisis lainnya, meliputi analisis statis, analisis dinamis, dan analisis *hybrid*, untuk mengkaji struktur internal *malware* secara komprehensif. Dengan demikian, penelitian ini dapat memberikan gambaran yang lebih lengkap dan akurat mengenai aktivitas maupun karakteristik *malware*, serta menjadi kontribusi nyata dalam mengembangkan metode analisis *malware* yang lebih efektif guna mendukung penguatan keamanan sistem informasi di tengah ancaman digital yang kian kompleks.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, dihasilkan rumusan masalah yang diangkat pada penelitian ini sebagai berikut:

1. Bagaimana analisis *memory forensics* dalam mengidentifikasi artefak *malware* pada sistem operasi *Windows 10*?
2. Bagaimana efektivitas penggunaan *YARA rules* dalam mendeteksi pola *malware* dari hasil file dan *memory dump*?
3. Bagaimana hasil analisis kombinasi antara *memory forensics* dan *YARA rules* dalam mengevaluasi perilaku serta karakteristik *malware*?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah, maka tujuan penelitian ini adalah sebagai berikut:

1. Menganalisis *malware* menggunakan teknik *memory forensics* pada sistem operasi *Windows 10.*
2. Menguji efektivitas *YARA Rules* dalam mendeteksi pola malware dari hasil *file* dan *memory dump*.
3. Mengevaluasi hasil analisis kombinasi antara *memory forensics* dan *YARA Rules* guna memahami perilaku serta karakteristik *malware* secara menyeluruh.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis dalam bidang analisis *malware*, keamanan informasi dan *digital forensics* antara lain:

1. Menerapkan studi kasus tentang sebuah *malware* pada sistem operasi.
2. Meningkatkan pemahaman pengguna terhadap mekanisme kerja *malware*.
3. Mengimplementasikan ilmu yang telah didapatkan selama perkuliahan.
4. Mengembangkan metode analisis *malware* berbasis *memory forensics* dan *YARA rules*.
5. Memberikan kontribusi terhadap penguatan keamanan sistem informasi.

1.5 Batasan Masalah

Penelitian ini memiliki batasan-batasan masalah yang digunakan untuk membuat proses

1. Sistem operasi yang digunakan sebagai lingkungan pengujian adalah *Windows 10 versi 64-bit*, tanpa membandingkan dengan sistem operasi lain.
2. Penelitian ini hanya berfokus pada analisis satu sampel *malware*, yaitu *ramez.exe*, sebagai objek utama yang dianalisis perilaku dan strukturnya.
3. Teknik analisis yang digunakan meliputi analisis statis, analisis dinamis, *hybrid analysis*, analisis *memory forensics* dan penggunaan *YARA rules* sebagai metode deteksi pola *malware*.

4. *Tools* yang digunakan dalam penelitian ini dibatasi pada *tools* yang mendukung kegiatan analisis *memory forensics*, seperti *Volatility* dan penerapan *YARA Rules* dalam proses identifikasi *malware*.
5. Penelitian ini tidak membahas pembuatan *malware*, teknik penyebaran, maupun metode eksploitasi terhadap sistem target. Fokus penelitian sepenuhnya diarahkan pada tahapan analisis terhadap sampel *malware* yang telah ada, guna memahami perilaku dan aktivitasnya pada sistem operasi.