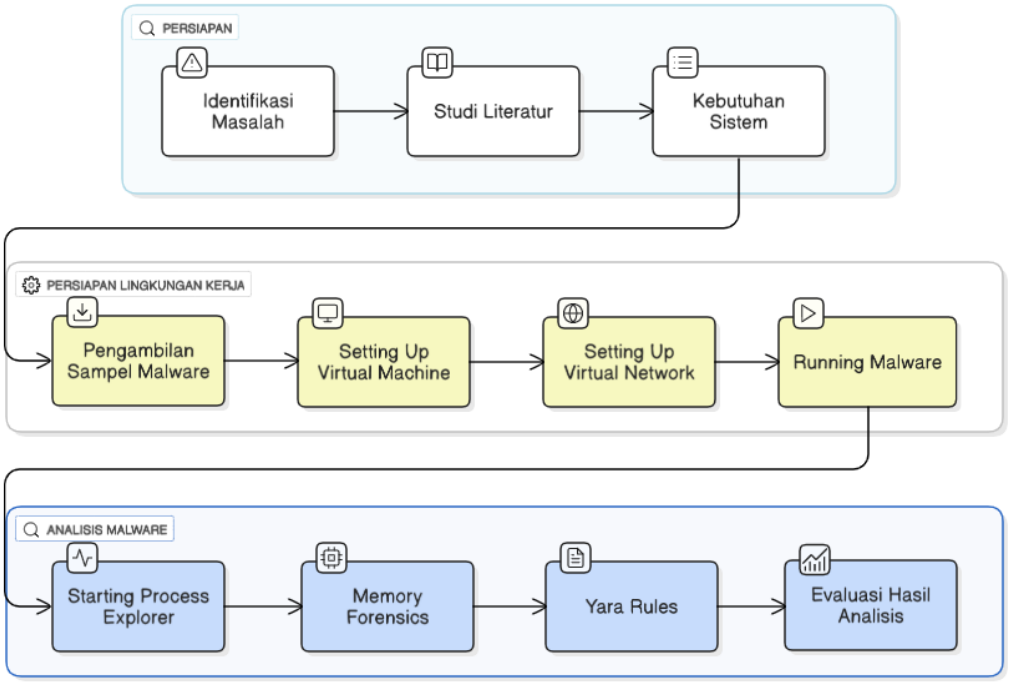
BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode peneltitian yang digunakan pada penelitian ini adalah metode kualitatif. Metode ini bersifat deskriptif dan analitis, serta dilakukan secara berkesinambungan untuk menggambarkan tahapan penelitian yang ditunjukkan pada Gambar 3.1.



Gambar 3.1 Tahapan Penelitian

Pada Gambar 3.1 dijelaskan mengenai diagram tahapan penelitian yang meliputi Identifikasi Masalah, Studi Literatur, Kebutuhan Sistem, Pengambilan Sampel *Malware*, *Setting Up Virtual Machine, Setting Up Virtual Network, Running Malware*, *Starting Process Monitor, Memory Forensics*, *Yara Rules* dan Evaluasi Hasil Analisis.

3.2 Identifikasi Masalah

Melakukan identifikasi masalah terkait *malware* yang digunakan, yaitu jenis *RAT* (*Remote Access Trojan*) yang mampu mencuri, memodifikasi, atau menghapus data pribadi pada komputer korban. *Malware* yang diteliti bernama *ramez.exe*, yang menginfeksi sistem operasi dengan menempel pada *file* berformat (*.doc*) dan akan aktif saat *file* tersebut dibuka oleh pengguna.

3.3 Studi Literatur

Setelah tahap identifikasi masalah selesai, langkah selanjutnya adalah mencari berbagai referensi yang berkaitan dengan informasi mengenai cara kerja *malware* serta metode-metode yang akan digunakan dalam penelitian ini. Tahap ini penting untuk memperkuat pemahaman dan landasan teori yang mendukung proses analisis *malware* secara menyeluruh.

3.4 Mengambil Sampel *Malware*

Malware yang digunakan dalam penelitian ini diperoleh dari situs https://any.run/, yaitu sebuah platform *sandbox online* yang menyediakan berbagai sampel *malware* untuk keperluan analisis, penelitian, serta pembelajaran di bidang keamanan siber dan forensik digital.

3.5 *Setting Up Virtual Machine*

Ruang lingkup penelitian ini menggunakan lingkungan virtual karena dianggap lebih aman untuk menguji sampel *malware* yang diteliti, sehingga dapat mencegah infeksi *malware* pada sistem fisik yang digunakan.

3.6 *Setting Up Virtual Network*

Tahap ini memanfaatkan *tools* ApateDNS, yaitu sebuah perangkat lunak yang berfungsi untuk memberikan respons DNS palsu atau terkontrol terhadap permintaan alamat IP yang dituju oleh *malware* pada komputer lokal, sehingga memungkinkan peneliti untuk memantau dan menganalisis aktivitas jaringan *malware* tanpa harus terhubung langsung ke internet yang sebenarnya.

3.7 *Running Malware*

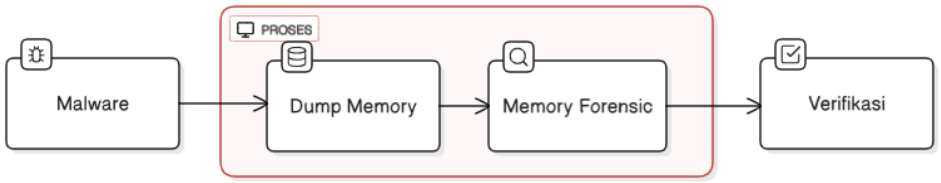
Proses ini memiliki tujuan utama untuk mengamati dan merekam secara detail perilaku *malware* saat dieksekusi di dalam sistem. Pengujian ini dilakukan di dalam lingkungan *virtual* atau *virtual machine* guna memastikan keamanan, sehingga apabila *malware* melakukan tindakan berbahaya, dampaknya tidak akan menyebar atau menginfeksi komputer fisik.

3.8 *Starting Process Explorer*

Tahap ini bertujuan untuk menampilkan informasi secara lengkap mengenai proses-proses yang berjalan di latar belakang sistem operasi, termasuk aktivitas *file*, *registry*, dan *thread* yang diakses oleh setiap proses. *Tools* yang digunakan dalam tahap ini adalah Process Monitor versi 3.89, sangat berguna dalam memantau dan menganalisis aktivitas *runtime* aplikasi secara *real-time* untuk keperluan analisis *malware* maupun *troubleshooting* sistem.

3.9 *Memory Forensics*

Alur analisis ini memanfaatkan *tools Volatility*, yang kemudian akan dibagi menjadi dua proses seperti yang ditampilkan pada Gambar 3.2.



Gambar 3.2 Alur Metode *Memory Forensic*

Pada gambar 3.2 dijelaskan alur proses analisis *malware* menggunakan metode *memory forensics*. Proses dimulai dari *malware* yang dieksekusi, kemudian dilakukan *dump memory* untuk mengambil data dari memori saat *malware* berjalan. Setelah itu, data *dump* tersebut dianalisis melalui tahap *memory forensic* untuk mengidentifikasi aktivitas, artefak, atau indikasi keberadaan *malware*. Tahap terakhir adalah verifikasi, yaitu memastikan hasil analisis sesuai dengan tujuan, seperti memastikan deteksi *malware* atau memahami perilaku *malware* tersebut.

3.10 *Yara Rules*

Yara Rules digunakan untuk menganalisis *file malware* yang telah berhasil diisolasi dalam lingkungan *virtual*, kemudian melakukan identifikasi awal menggunakan perintah *file* untuk mengetahui tipe *file*, dilanjutkan dengan *strings* untuk melihat *string-string* yang terkandung di dalam *file*. Hasil *output* dari *strings* akan digunakan sebagai acuan dalam merumuskan aturan *YARA* yang menandai *string* tertentu, *API Windows*, atau elemen lain yang terdeteksi pada sampel.

Peneliti akan membuat *file rule YARA* yang berisi *string-string* unik yang ditemukan dari hasil analisis *malware*. Setelah itu, *rule* tersebut dijalankan menggunakan perintah *YARA* untuk memeriksa bagian mana saja dari *file malware* yang cocok dengan aturan tersebut. Hasilnya diharapkan dapat menunjukkan lokasi *string* dalam *file*, sehingga membantu peneliti memahami struktur *file malware*, cara kerjanya, dan teknik apa saja yang digunakan, seperti *packer, mutex,* atau penggunaan *crypto*.

Tahapan berikutnya dengan menyempurnakan *rule* secara bertahap dengan menambah string lain yang ditemukan melalui analisis lanjutan menggunakan *tools* seperti *peframe* dan *metadata file*. *YARA Rules* diharapkan menjadi sarana untuk menggali karakteristik internal *file malware* secara lebih terarah. Hasil dari setiap *rule* yang dijalankan akan didokumentasikan untuk mendukung kesimpulan mengenai pola-pola yang ditemukan di dalam *file* sampel.

3.11 Evaluasi Hasil Analisis

Pada tahap ini akan melakukan evaluasi terhadap efektivitas dua pendekatan utama yang digunakan dalam analisis malware, yaitu *Memory Forensics* dan *YARA Rules*. Evaluasi ini bertujuan untuk mengetahui sejauh mana masing-masing metode mampu mengidentifikasi artefak atau indikator dari sampel *malware* yang dianalisis, baik dari sisi perilaku runtime maupun pola karakteristik dalam *file*.

Rencana evaluasi dilakukan dengan membandingkan hasil analisis berdasarkan beberapa contoh parameter yang diambil dari penelitian terdahulu, seperti Das (2022), Triantoro dkk. (2021), dan Gupta dkk. (2024). Adapun rancangan tabel evaluasi dapat dilihat pada Tabel 3.1.

Tabel 3.1 Parameter Hasil Analisis

Parameter	***Memory Forensics***	***Yara Rules***
Deteksi proses mencurigakan di memori (Das, 2022).	……..	……..
Koneksi jaringan aktif dan IP tujuan *malware* (Triantoro dkk., 2021).	……..	……..
Identifikasi *string* unik (Gupta dkk., 2024).	……..	……..

Pada tabel 3.1 dapat dilihat contoh parameter yang diadaptasi dari penelitian-penelitian sebelumnya, yang bersifat sebagai referensi awal dan bukan acuan baku dalam perancangan evaluasi. Proses evaluasi akan dilaksanakan setelah tahap analisis *malware*, dengan mengolah serta mengkaji data hasil analisis tersebut. Parameter yang digunakan dapat dimodifikasi atau ditambahkan sesuai dengan temuan selama proses analisis, sehingga evaluasi yang dilakukan mampu memberikan gambaran yang lebih tepat mengenai efektivitas metode *Memory Forensics* dan *YARA Rules* dalam mendeteksi *malware*.