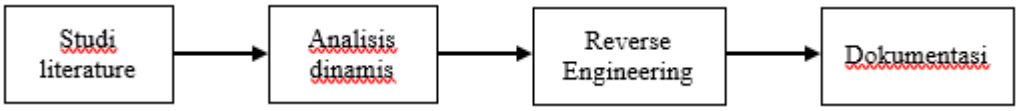
BAB III

METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Penelitian ini menggunakan metodologi deskriptif dimana penelitian melakukan studi literatur di samping uji coba langsung untuk melakukan analisis *malware*, dengan alur penelitian diunjukan pada gambar 3.1 sebagai berikut:

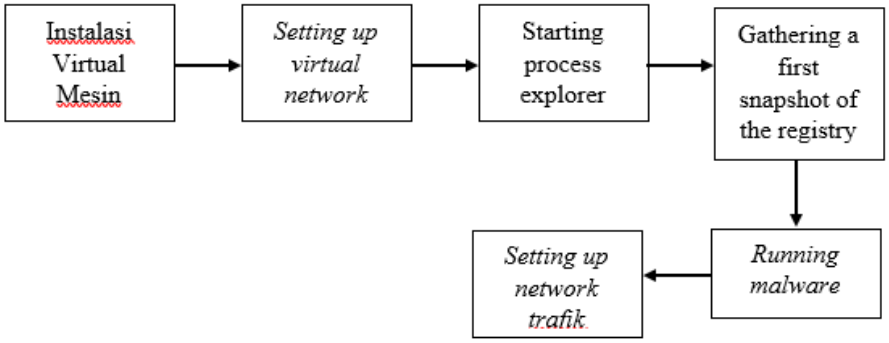


Gambar 3.1 alur metodologi penelitian

3.2 *Study literature*

Study literature uraian tentang teori, temuan, dan bahan penelitian lainnya yang diperoleh dari bahan acuan untuk dijadikan landasan kegiatan penelitian untuk menyusun kerangka pemikiran yang jelas dari perumusan masalah yang ingin diteliti. Bahan acuan yang digunakan adalah jurnal-jurnal dan buku mengenai analisis *malware* dan *reverse engineering malware*.

3.3 Analisis Dinamis



Gambar 3.2 alur metode analisis dinamis

Gambar 3.2 menunjukkan alur metode analisis dinamis. Penjelasan lebih jelas sebagai berikut:

a. *Instalasi Virtual Mesin*

Menentukan ruang lingkup, penelitian ini mengkhususkan pada ruang penelitian yang akan dilakukan pada lingkungan aman dimana menggunakan lingkungan *virtual* untuk pengujian *sample malware*. Lingkungan mesin *virtual* atau yang dikenal dengan *virtual mechine* (VM). *Spesifikasi* yang akan di gunakan sebagai penelitian ditunjukkan pada tabel 3.1 dan tabel 3.2 sebagai berikut:

Tabel 3.1 *Spesifikasi computer*

Sistem operasi	*Windows 7 Ultimate 32-bit (6.1, Build 7601) Service Pack 1*
Prosesor	*Intel(R) Core(TM) i3-2350M CPU @ 2.30GHz (4 CPUs), ~2.3GHz*
Memori	*2048MB RAM*
Hardisk Capacity	*500*

Tabel 3.2 Spesifikasi Virtual

Aplikasi VM	*Virtual Box / VMware workstation*
Sistem operasi	*Windows7*
Memori	*512MB / 1GB RAM*
Processor	*Single core*

Pengujian dilakukan dalam lingkungan *virtual* dimana untuk menjaga komputer fisik (*real*) aman terhadap *malware* yang akan di teliti. Perbandingan dalam menggunakan *Virtual* dan *Real* ditunjukkan pada tabel 3.3 sebagai berikut:

Tabel 3.3 Perbandingan *Virtual* dengan *Real*

Virtual	*Real*
Lingkungan sistem aman	Lingkungan system tidak aman
Penggunaan waktu relatif cepat	Penggunaan waktu relative lama
Biaya lebih murah bahkan gratis	Biaya lebih mahal
Malware kadang tidak akan menyebar	Fungsional *malware* sepenuhnya berjalan

b. *Setting up virtual network*

Setting up virtual network menggunkana tools *ApateDNS*. *ApateDNS* untuk melihat apakah permintaan *DNS* dilakukan. *ApateDNS* memalsukan respons *DNS* ke alamat *IP* yang ditentukan pengguna pada komputer lokal, ini menanggapi permintaan *DNS* dengan respons *DNS* diatur ke alamat *IP* yang ditentukan. *ApateDNS* dapat ditampilkan hasil heksadesimal dan *ASCII* dari semua permintaan yang diterimanya.

c. *Starting process explorer*

Monitoring process menggunakan *process Hacker* 2.39, *Process Hacker* 2.39 menunjukan informasi tentang penanganan dan proses *DLL* yang telah berjalan. Pembahasan lengkap untuk analisis menggunakan *Process Explorer* 2.39 akan dilakukan pada bab berikutnya.

d. *Gathering a first snapshot of the registry*

Analisis berikutnya adalah memonitor perubahan pada registri. Hasil dari *Regshot* 1.9.0 ini bisa dipilih, berupa *file* teks atau HTML, yang menunjukkan berapa jumlah perubahan registri dan apa serta dimana saja perubahan tersebut. Pembahasan lengkap untuk analisis menggunakan *Regshot* akan dilakukan pada bab selanjutnya.

e. *Running malware*

Tahap ini dilakukan pengujian dengan menjalankan sampel *file malware* (*Flawed Ammy RAT*) pada *virtual* lab, sehingga dapat menghasilkan informasi mengenai perilaku apa saja yang dilakukan oleh *malware* terhadap sistem ketika *file* tersebut dijalankan. *Malware Flawed Ammy rat* ini *file exe* maka menjalankannya dengan double clik *malware* tersebut.

f. *Setting up network traffic*

Monitoring lalu lintas jaringan, *Wireshark* karena memiliki tampilan antarmuka (GUI) dan fitur filtrasi sehingga sangat mudah dalam penggunaannya. *Wireshark* sudah cukup untuk meneliti paket yang berada pada jaringan yang mungkin dikirim oleh *malware*. Analisis menggunakan *Wireshark* untuk pembahasan lengkap akan dilakukan pada bab selanjutnya.

3.4 *Reverse Engineering*

Disassembler

Proses *disassembly* menggunakan *tools IdaPro* untuk melakukan disassembler pada *malware Flawed Ammyy RAT* yang akan dilakukan pada bab 4.

3.5 Dokumentasi

Dokumentasi menyimpan hasil keluaran data dari pengolahan proses s*can* dari sample *malware* dari berbagai *softwar*e analisis, untuk kemudian diterapkan pada laporan penelitian.