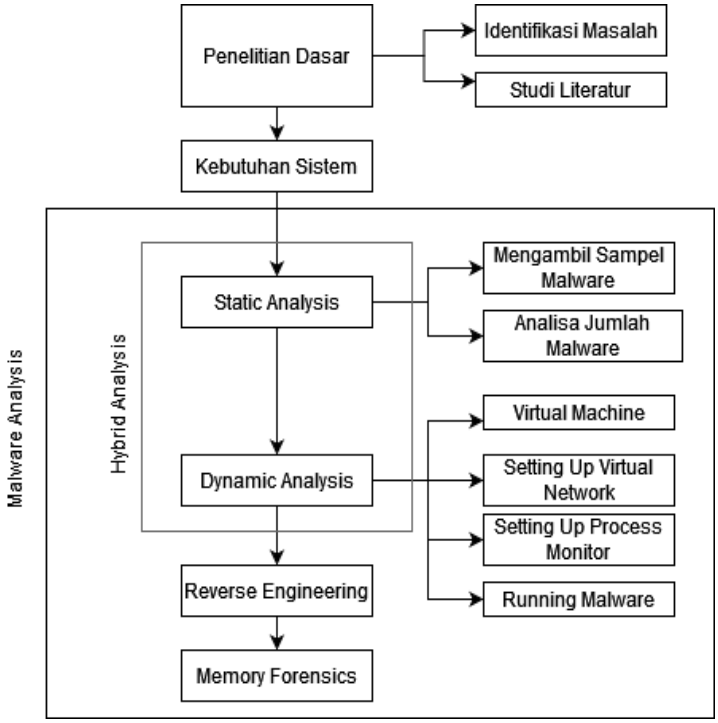
BAB III

METODOLOGI PENELITIAN

3.1. Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah metode kualitatif yang memperkuat pendekatan deduktif dan infuktif. Metode kualitatif adalah penelitian yang deskriptif dan menerapkan analisis pada sebuah penelitian (Hadi, 2016). Kelengkapan pada proses penelitian adalah hal menarik dengan adanya observasi informasi dalam menghasilkan sebuah ilmu pengetahuan. Proses metodologi penelitian dilakukan berkesinambungan agar dapat melihat tahapan dari sebuah penelitian (Fadli, 2021). Gambar 3.1 merupakan tahapan-tahapan penelitian yang dilakukan pada penelitian ini.



GAMBAR 3.1 TAHAPAN-TAHAPAN PENELITIAN

Alur metodologi yang digunakan dapat dilihat pada Gambar 3.1, penelitian ini menguji *malware* yang diteliti secara langsung berdasarkan referensi yang sudah dikaji sebelumnya.

3.2. Penelitian Dasar

Penelitian dasar merupakan tahap pertama dalam melaksanakan sebuah penelitian. Tujuan dari tahapan ini dimaksudkan untuk mengidentifikasi sekaligus studi literatur terkait objek penelitian berupa *malware* yang diteliti. Ada 2 (dua) cara dalam melakukan tahap awal dalam sebuah penelitian, yaitu:

3.2.1. Identifikasi Masalah

Melaksanakan identifikasi masalah terkait *malware* yang digunakan. *Malware* yang digunakan memilki jenis *RAT* (*Remote Acces Trojan*) yang dapat mengambil, mengubah, atau menghapus data pribadi pada komputer yang terinfeksi. *Malware* yang diteliti bernama *AQUVAPRN.exe* yang menginfeksi sebuah sistem operasi dengan cara menempel pada sebuah file dengan ekstensi (.doc) yang akan berkerja ketika file tersebut dibuka oleh pengguna.

3.2.2. Studi Literatur

Setelah melakukan identifikasi masalah, pada tahap ini melakukan pencarian referensi terkait informasi cara kerja *malware* dan metode yang digunakan pada penelitian ini.

3.3. *Malware Analysis*

Tahapan ini merupakan implementasi dari tahap awal penelitian terkait metode penelitian yang digunakan pada penelitian *malware.* Ada 8 (delapan) alur dalam tahap ini, yaitu:

3.3.1. *Static Analysis*

Static Analysis atau analisa statis dilakukan untuk mengetahui informasi awal dari *malware AQUVAPRN.exe* dengan tahapan sebagai berikut:

1. Mengambil *Sample Malware*

   Malware yang digunakan pada penelitian ini diambil dari *website* https://any.run/ yang dilanjutkan dengan analisa awal yang akan dijelaskan secara rinci pada bab selanjutnya.

2. Analisa Jumlah *Hash Malware*

   Tahapan ini *malware* akan di indentifikasi menggunakan *tools HashCalc* untuk mendapatkan informasi terkait nilai MD5 (*Message-Digest Algorihm 5*).

3.3.2. *Dynamic Analysis*

Dynamic Analysis atau analisa dinamis dilakukan dengan media *virtual* yang bertujuan agar *malware* tidak menginfeksi sistem utama pada saat pelacakan fungsi, informasi, dan cara kerja dari *malware AQUVAPRN.exe*. Tahapan yang dilakukan adalah:

1. *Setting Up Virtual Machine*

   Ruang lingkup yang digunakan pada penelitian ini menggunakan *virtual* karena dinilai lebih aman dalam melakukan pengujian sample *malware* yang diteliti untuk mencegah *malware* menginfeksi sistem fisik yang digunakan.

2. *Setting Up Virtual Network*

   Tahap ini menggunakan *tools ApateDNS* yang memiliki fungsi untuk merespon *DNS* pada alamat *IP* yang di tuju oleh *malware* pada komputer lokal.

3. *Starting Process Explorer*

   Tahap ini memilki tujuan untuk menampilkan informasi proses yang berjalan pada latar belakang sistem operasi. *Tools* yang digunakan adalah Process Monitor versi 3.89.

4. *Running Malware*

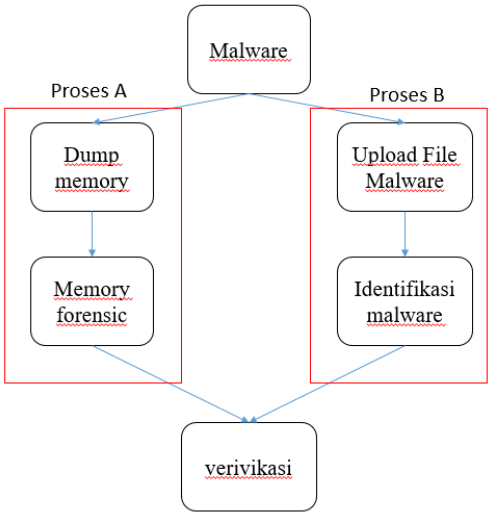
   Proses ini bertujuan untuk melihat perilaku malware saat dijalankan pada sistem. Pengujian ini dilaksanakan menggunakan ruang *virtual* untuk mencegah *malware* menginfeksi komputer fisik.

3.3.3. *Reverse Engineering*

Tahapan ini menggunakan *tools IDA Pro* dalam melakukan proses *disassembler* pada *malware AQUVAPRN.exe*. *Tools* ini menerjemahkan bahasa mesin menjadi bahasa manusia yang akan diubah dalam proses analisis *command* yang digunakan oleh *malware AQUVAPRN.exe*.

3.3.4. *Memory Forensics*

Alur analisis ini menggunakan *tools volatility* yang selanjutnya akan dibagi menjadi dua proses yang dapat dilihat pada Gambar 3.2.



***GAMBAR 3.2 ALUR METODE* MEMORY FORENSICS**