BAB III
ANALISIS SISTEM

3.1. Analisis Sistem

3.1.1. Menyiapkan dan Melakukan Instalasi Sistem Operasi

Sistem operasi untuk proses analisis tidak dilakukan pada sistem operasi utama karena *malware* bisa saja merusak file – file sistem jika sedang dijalankan atau sedang di analisis. Maka dari itu analisis akan dilakukan pada komputer *virtual* menggunakan bantuan *software virual machine*. Sistem operasi yang digunakan memiliki spesifikasi sebagai berikut :

1. Sistem operasi windows xp3
2. Windows x86 (32-bit)

3.1.2. Melakukan Instalasi Tools untuk Proses Analisis

Untuk melakukan analisis malware dibutuhkan *tools* sebagai berikut :

1. IDA-PRO Disassembler

   Tool untuk melakukan *disassembly* dan *debugging*.

2. Reg Shot

Tool untuk melakukan perbandingan pada *registry windows* sebelum dan sesudah proses eksekusi program.

3. Proses Monitor

   Tool yang digunakan untuk melakukan monitoring pada proses yang berjalan di *memory*.

4. Wireshark

   Tool yang digunakan untuk menangkap paket pada lalu lintas jaringan.

5. md5Sum

   Tool yang digunakan untuk melakukan validasi file.

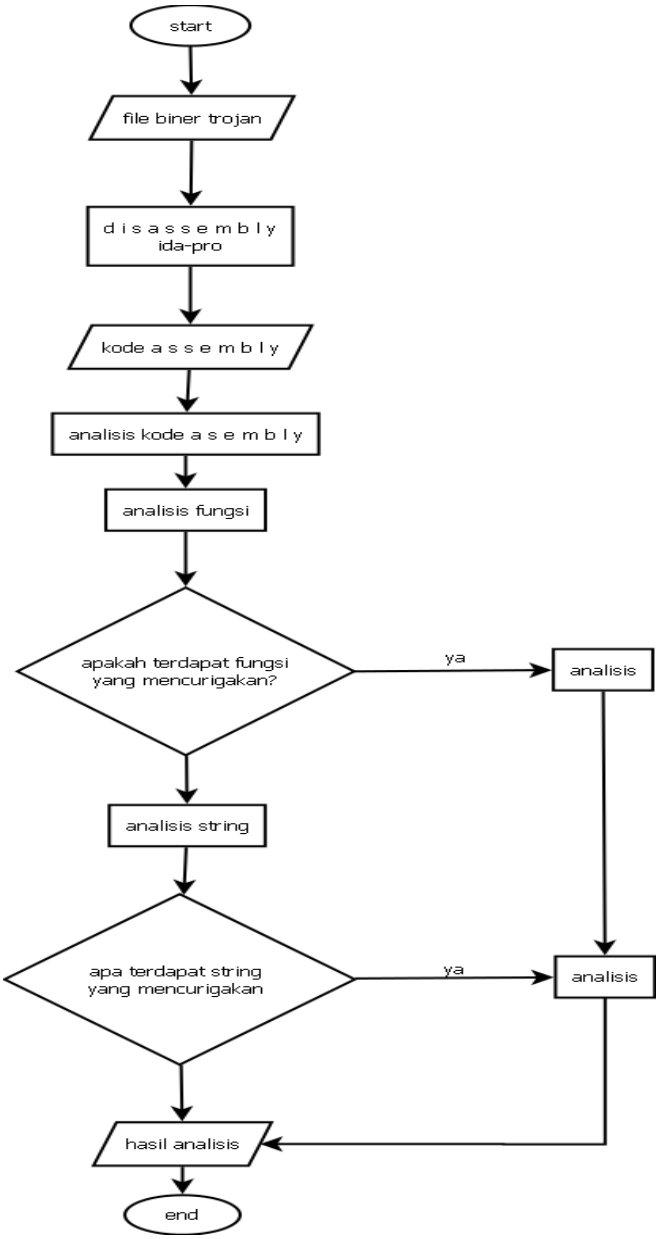
3.1.3. **Melakukan Analisis Statis *(static analysis)***

Analisis statis *(static analysis)* terhadap malware *trojan* meliputi tahapan – tahapan sebagai berikut :

1. Melakukan proses *disassembly* terhadap file biner

3.1.3.1 **Proses Disassembly Terhadap File Biner Trojan**

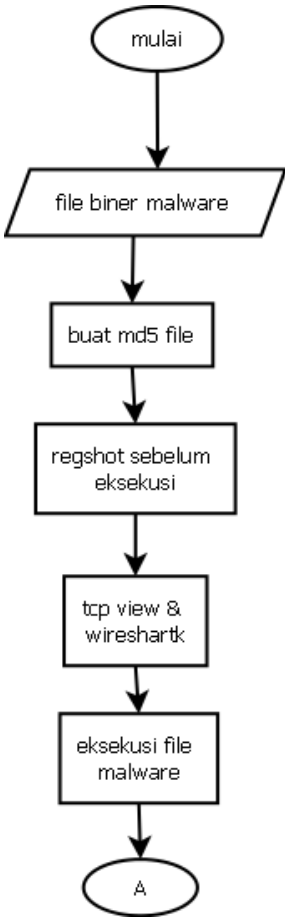
Proses *disassembly* terhadap file biner dilakukan mengikuti langkah – langkah yang ditunjukkan pada gambar 3.1.



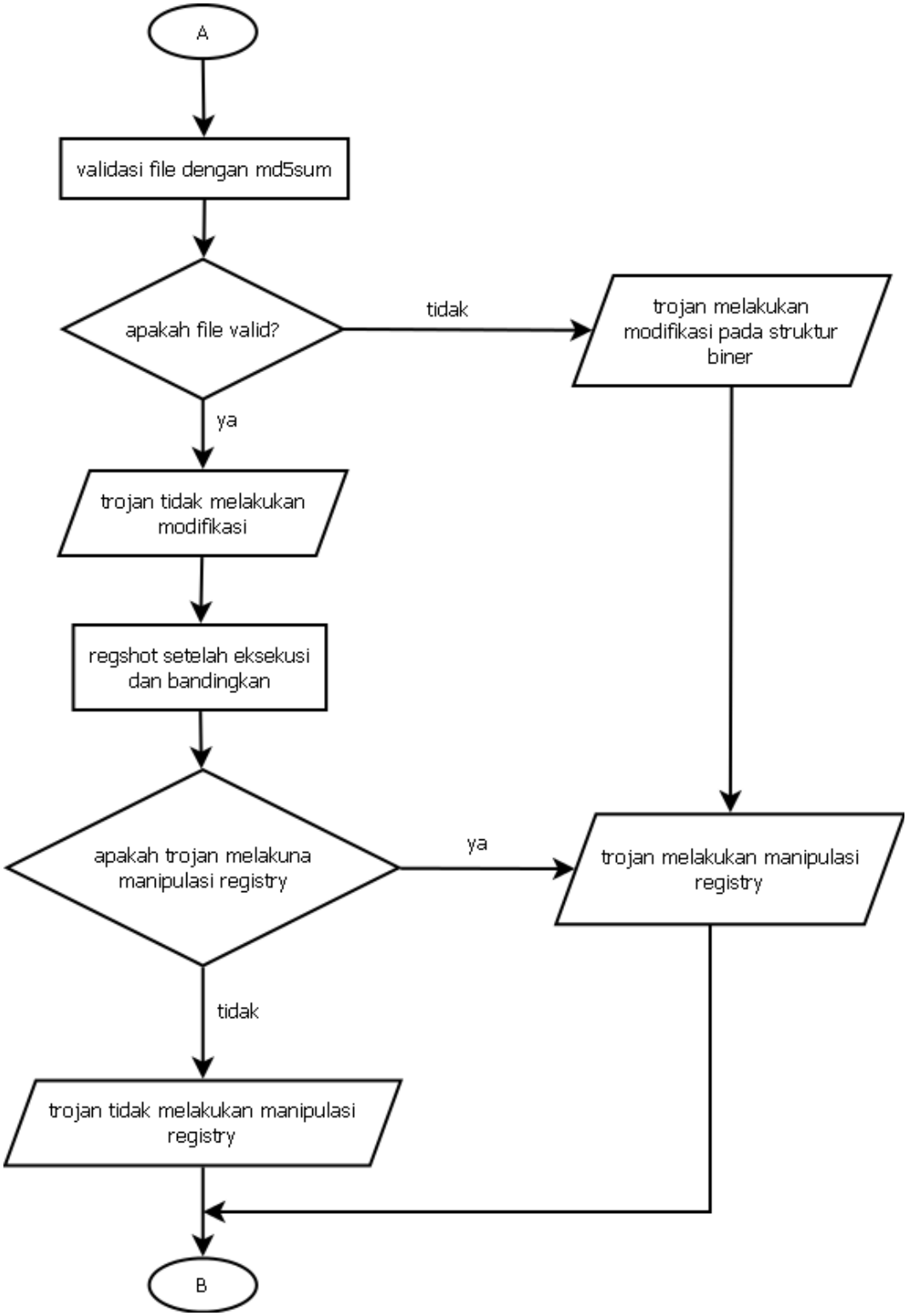
Gambar 3.1 Flowchart Proses disassembly

3.1.4. **Melakukan Analisis Dinamis *(dynamic analysis)***

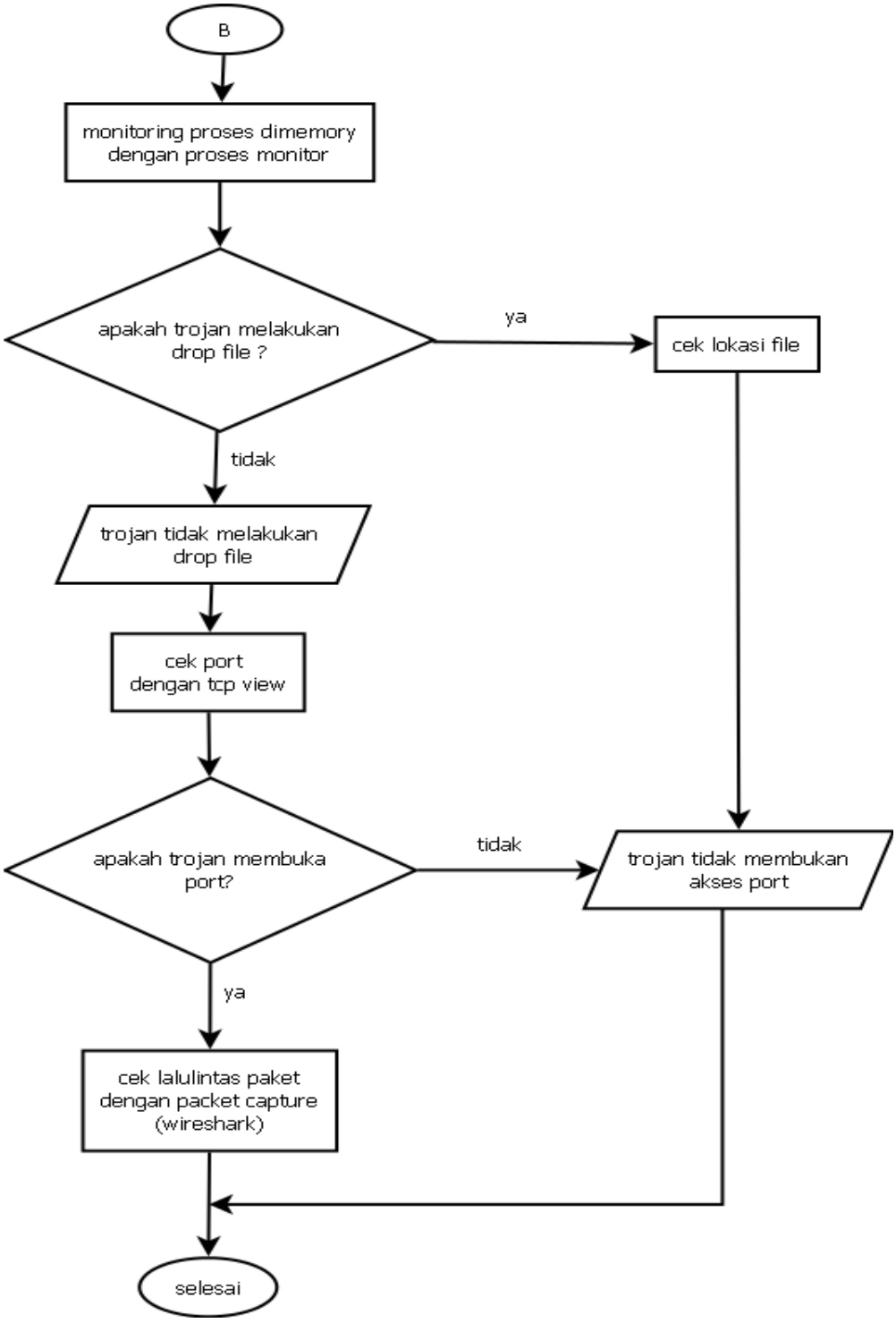
proses analisis dinamis *(dynamic analysis)* terhadap file biner dilakukan mengikuti langkah – langkah yang ditunjukkan pada gambar 3.4, 3.5, 3.6.



Gambar 3.4 Flowchart Proses analisis dinamis



Gambar 3.5 *flowchart* A proses analisis dinamis



Gambar 3.6 *flowchart* B proses analisis dinamis