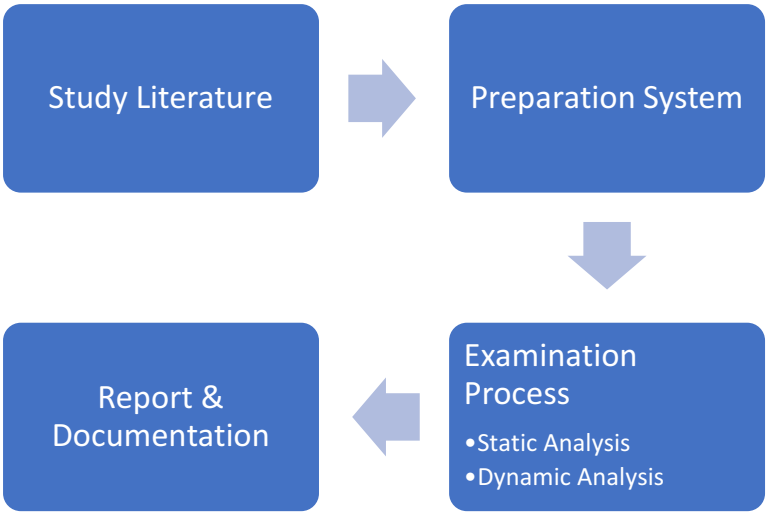
# BAB III

# METODOLOGI PENELITIAN

Penelitian ini melakukan studi literatur selain melakukan uji coba langsung untuk melakukan analisis *malware*. Tahapan pada penelitian ditunjukkan pada gambar 3.1.




Gambar 3.1 Tahapan Penelitian

## 3.1 *Study Literature*

*Study Literature* dilakukan dengan cara mengumpulkan data dan informasi dari buku, media, jurnal, pakar ataupun hasil penelitian orang lain yang bertujuan untuk menyusun dasar teori yang digunakan dalam melakukan penelitian. Buku dan jurnal referensi dapat berisi uraian singkat atau penjelasan secara menyeluruh mengenai analisis *malware*.

## 3.2 *Preparation System*

Preparation System adalah proses mempersiapkan segala kebutuhan yang diperlukan untuk melakukan analisis malware. Persiapan yang dilakukan diantaranya adalah memasang sistem operasi pada mesin virtual, memasang tools dan mengunduh sample malware.

## 3.3 *Examination Process*

### 3.3.1 *Static Analysis*

Proses *static analysis* menggunakan beberapa teknik untuk mendapatkan informasi pada *malware redline stealer*. Penjelasan teknik yang dilakukan sebagai berikut:

a. *Fingerprint Malware*

*Fingerprint Malware* yang dimaksud pada penelitian ini adalah menghitung nilai *Hash Sample Malware*. Nilai *hash* tersebut akan dibandingkan dengan nilai *hash* yang didapat dari sumber *malware*.

b. Identifikasi Jenis File

Identifikasi jenis file malware dilakukan untuk mencari signature file menggunakan tool Hex Editor. Tahapan ini bertujuan untuk mengidentifikasi sistem operasi dan arsitektur yang menjadi target malware Redline Stealer

c. *Strings extract*

*Strings extract malware* dilakukan menggunakan *tool Strings*.

d. *Decompile*

*Decompile sample malware* dilakukan menggunakan *tool Dnspy.*

e. *Obfuscation Detect*

*Obfuscation Detect* dilakukan menggunakan *tool de4dot*. *Tool de4dot* juga digunakan untuk proses *deobfuscate* jika *sample malware* terdeteksi menggunakan *obfuscation*.

### 3.3.2 *Dynamic Analysis*

*Dynamic Analysis* dilakukan dengan cara *sample malware Redline Stealer* dijalankan dan dipantau. Proses pemantauan ini dilakukan dengan 2 teknik yaitu *Process Monitoring* dan *Network Monitoring.* Penjelasan mengenai teknik yang dilakukan pada *dynamic analysis* sebagai berikut:

a. *Process Monitoring*

*Sample malware* dijalankan dan dilihat proses apa saja yang dibuat oleh *sample malware Redline Stealer* saat dijalankan. *Process Monitoring* dilakukan dengan menggunakan *tool Procmon.*

b. *Network Monitoring*

*Network Monitoring* dilakukan menggunakan aplikasi *Wireshark*. *Wireshark* akan merekam semua lalu lintas data yang dilakukan *sample malware Redline Stealer* saat dijalankan.

### 3.4 *Report & Documentation*

Tahapan terakhir adalah dokumentasi untuk menyimpan hasil data yang diperoleh dari proses analisis *malware* dengan menggunakan metode *static analysis* dan *dynamic analysis*. Dokumentasi tersebut berupa keluaran data dari video, gambar ataupun hasil keluaran data dan informasi dari *tools* analisis, yang kemudian dituangkan pada laporan penelitian.