BAB III

METODOLOGI PENELITIAN

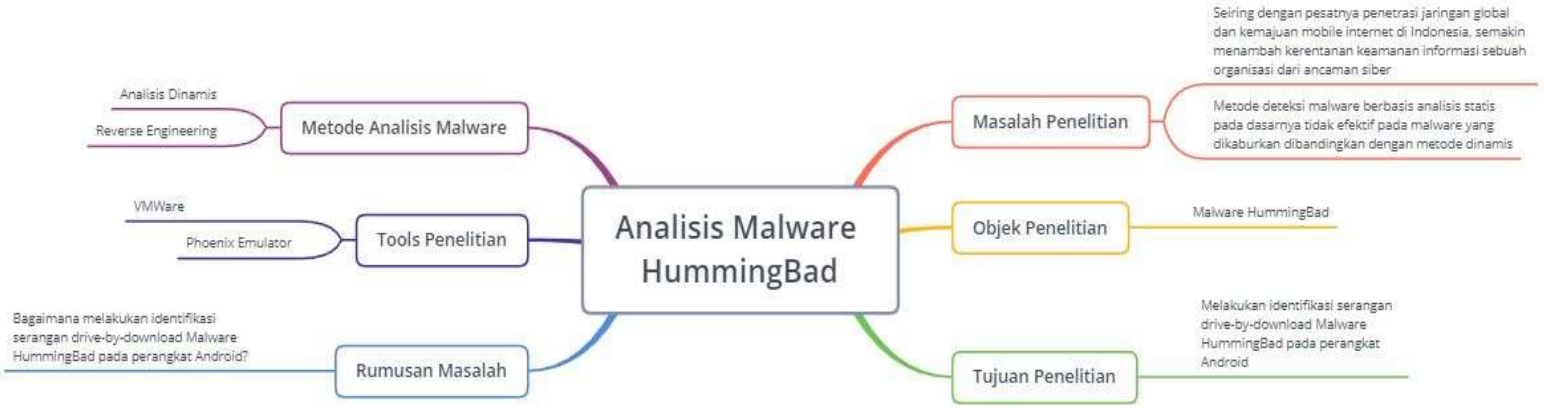
3.1 Metodologi Penelitian

Metodologi penelitian diartikan sebagai memberikan sebuah ide yang jelas tentang metode apa atau akan memproses dengan cara bagaimana di dalam penelitiannya agar dapat mencapai tujuan penelitian. Proses pemilihan metode penelitian adalah bagian yang sangat penting di alam proses penelitian (Industrial, 2010).

3.2 *Mind Map* Penelitian

Gambar 3.2 merupakan *Mind Map* Penelitian dimana analisis malware hummingbade dilakukan karena Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber Metode deteksi malware berbasis analisis statis pada dasarnya tidak efektif pada malware yang dikaburkan dibandingkan dengan metode dinamis. Dimana objek penelitian ini adalah *malware humingbad*. penelitian ini bertujuan untuk Melakukan identifikasi serangan drive-by-download Malware HummingBad pada perangkat Android.

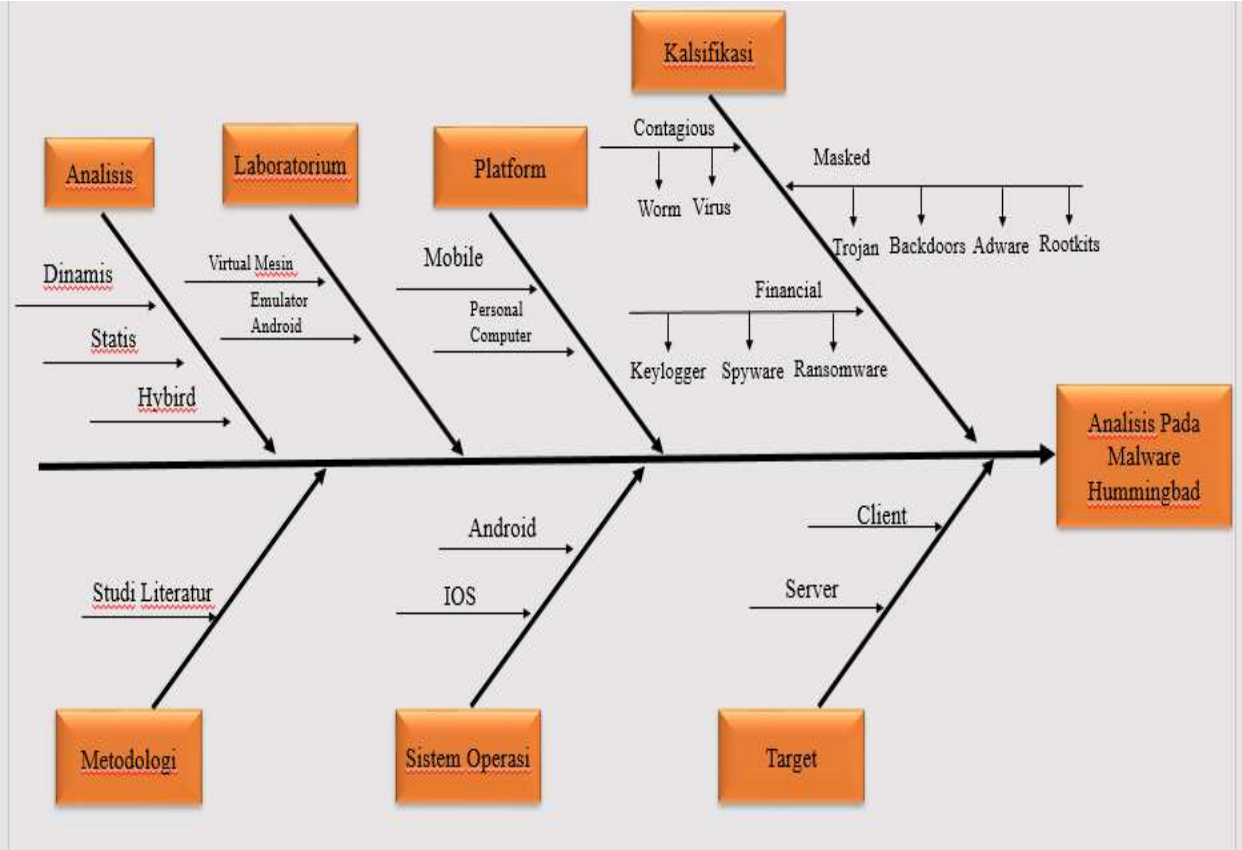
Penelitian ini juga mengetahui bagaimana melakukan identifikasi serangan drive-by-download Malware HummingBad pada perangkat Android dengan metode yang digunakan adalah dengan analisis dinamis dan *reverse engineering*, yang menggunakan tools phone emulator.



Gambar 3.2 *Mind Map*

3.3 Diagram *Fishbone*

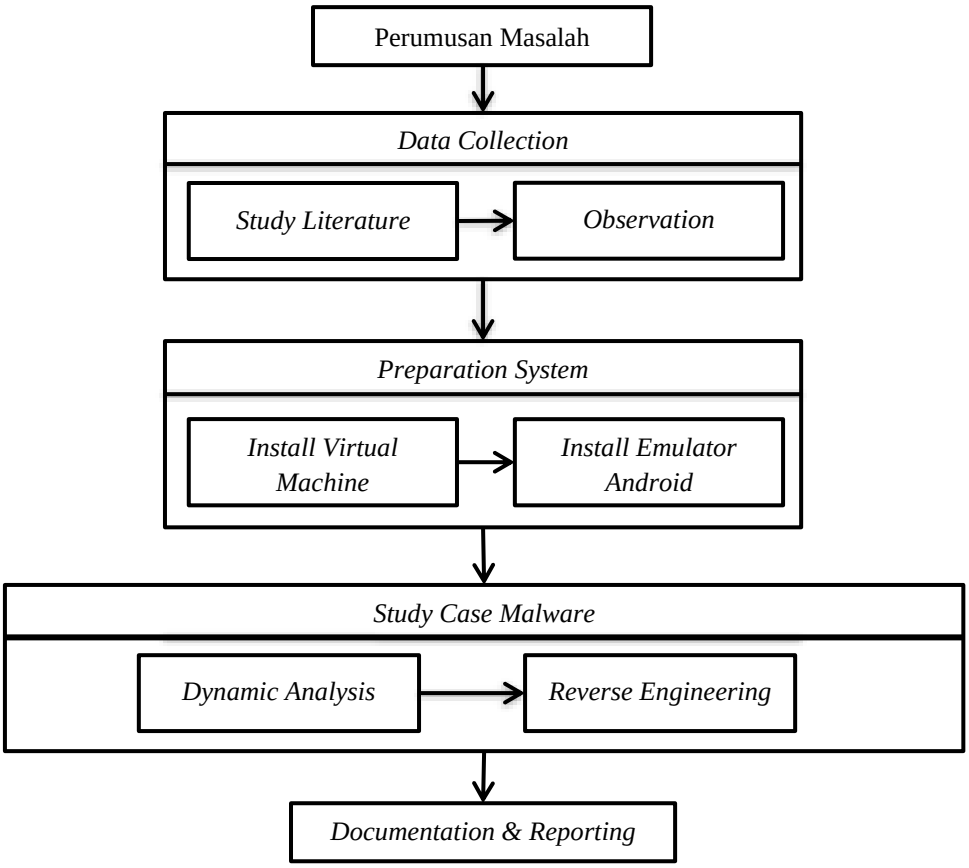
Gambar 3.3 menunjukkan diagram *fishbone* penelitian, diagram ini menggambarkan hal-hal yang berkaitan dengan penelitian yang akan dilakukan dan rencana penelitian. *Malware* yang akan di teliti adalah *Troja`n*. *Sample malware* yang didapat, *malware* melakukan serangan pada *target* posisi sebagai *client*, *platform* yang diserang adalah *smartphone*. Laboratorium untuk melakukan analisis *malware* ini menggunakan *virtual* mesin. Analisis *malware* menggunakan analisis dinamis. Penelitian ini menggunakan metodologi *kualitatif*, sedangkan untuk sistem operasi yang diserang adalah *Android*.



Gambar 3.3 Diagram *Fishbone*

3.4 Tahapan Penelitian

Penelitian ini menggunakan metodologi deskriptif seperti ditunjukan pada gambar 3.4 sebagai berikut:



Gambar 3.4 Alur Penelitian

Penelitian ini menggunakan metode deskriptif yang menurut Punaji (2010) metode deskriptif adalah penelitian yang memiliki tujuan untuk menjelaskan atau mendeskripsikan suatu peristiwa, keadaan, objek apakah orang, atau segala sesuatu yang terkait dengan variabel-variabel yang bisa dijelaskan baik menggunakan angka-angka maupun kata-kata. Metode deskriptif kebanyakan tidak dimaksudkan untuk menguji hipotesis tertentu, melainkan lebih untuk menggambarkan apa adanya suatu variabel, gejala, atau keadaan.

3.4.1 Perumusan Masalah

Langkah awal untuk memulai penelitian adalah proses merumuskan masalah yang akan diteliti. Tahap ini merupakan tahap yang paling penting dalam penelitian karena semua jalannya penelitian akan dituntun oleh perumusan masalah.

Langkah selanjutnya menetapkan berbagai aspek masalah yang dihadapi. Informasi mengenai masalah disusun sedemikian rupa untuk dijawab menjadi suatu perumusan masalah. Tujuan penelitian harus dirumuskan dengan jelas serta mencakup pernyataan tentang mengapa penelitian dilakukan, sasaran penelitian, maupun pikiran penggunaan dan dampak hasil penelitian.

Penelitian ini adalah sebuah upaya untuk memberikan gambaran solusi dalam penanganan atas serangan *malware* dengan cara melakukan analisa terhadap *malware* yang telah berhasil melakukan eksploitasi serangan.

Penelitian ini dilakukan analisis terhadap *malware* dengan nama *Malware HummingBad.* Jenis *malware* ini ditemukan pada tahun 2016. Ditemukannya jenis *malware* tersebut maka hal berikutnya yang harus diungkap adalah bagaimana serangan dari *malware* tersebut. Analisis dari *malware Hummingbad* tersebut dilakukan dengan cara analisis dinamis dan *reverse engineering*.

3.4.2 *Data Collection*

Data Collection merupakan tahap kedua dari penelitian ini. Permasalahan yang sebelumnya dirumuskan, kemudian dicari solusi pemecahan masalahnya. Langkah awal pada tahap *Data Collection* adalah *Study literature* (kajian pustaka) yang merupakan penelusuran

literatur yang bersumber dari buku, media, jurnal, pakar ataupun dari hasil penelitian orang lain yang berkaitan dengan proses analisis *malware* dengan berbagai metode yang ada. Proses tersebut bertujuan untuk menyusun dasar teori yang berguna sebagai penunjang penelitian.

Penunjuk informasi dalam menelusuri bahan bacaan adalah dengan menggunakan buku referensi. Buku-buku dan jurnal referensi ini dapat berisi uraian singkat atau penunjukan nama dari bacaan tertentu. Bahan dari jurnal dan buku referensi tidaklah untuk dibaca dari halaman pertama sampai tamat, hanya bagian yang penting dan yang diinginkan saja. Bahan acuan yang digunakan adalah jurnal-jurnal dan buku mengenai analisis *malware.*

Data penyelesaian yang telah dikumpulkan, selanjutnya dilakukan proses pencocokan dengan praktik di lapangan apakah memang dapat diimplementasikan dan menghasilkan output yang baik atau tidak. Pengguna ponsel *android* harus semakin waspada, sebab telah ditemukan *malware* baru yang sukses menginfeksi 85 juta perangkat sistem operasi tersebut, *malware HummingBad* dapat menghasilkan kerugian US$300.000 atau Rp3,93 miliar per bulan setiap bulan dari iklan penipuan yang dibuat oleh si pelaku. Cara kerja *malware HummingBad* yaitu dilakukan untuk mendapatkan *root access* dari perangkat *android* dan memicu kerentanan, jika ini berhasil maka *malware* ini bakal mendapat akses penuh dari perangkat tersebut namun jika tahap mendapatkan akses ini gagal, maka *malware* bakal membuat notifikasi *update* yang palsu, sehingga

memungkinkan pengguna untuk mengijinkan akses keamanan perangkat ketika *root* telah ditembus *HummingBad* bakal mengunduh aplikasi palsu sebanyak mungkin untuk memudahkan kerjanya.

3.4.3 *System Preparation*

Sistem ini harus disiapkan terlebih dahulu agar nantinya dapat dilakukan analisis terhadap *malware HummingBad*. Mesin virtual dipilih sebagai sistem pengganti dari sistem yang asli agar proses analisis dinamis terhadap *malware HummingBad* dapat dilakukan secara aman sehingga tidak menginfeksi perangkat yang asli. Mesin virtual yang dipilih adalah *android studio*.

HummingBad merupakan *malware* yang menginfeksi perangkat Android, maka dari itu diperlukan emulator Android yang sudah terpasang pada mesin virtual sehingga perilaku dan aktivitas *malware HummingBad* dapat diamati untuk kemudian dilakukan analisis dinamis.

3.4.4 *Study Case Malware HummingBad*

HummingBad versi sekarang beroperasi sebagai *dropper* yang digunakan untuk mengunduh dan menjalankan aplikasi tambahan, mirip dengan taktik yang digunakan oleh *HummingBad* versi sebelumnya. *HummingBad* versi sekarang menggunakan *plugin Android* yang disebut *DroidPlugin*, yang awalnya dikembangkan oleh Qihoo 360, untuk mengunggah aplikasi palsu di mesin virtual.

Pertama, server *Command and Control (C&C)* menyediakan iklan dan aplikasi palsu untuk *malware* yang diinstal kemudian

menyajikannya kepada pengguna, setelah pengguna mencoba menutup iklan, aplikasi yang sudah diunduh oleh *malware* diunggah ke mesin virtual dan dijalankan seolah-olah itu adalah perangkat nyata. Tindakan tersebut menghasilkan ID pengarah palsu, yang digunakan *malware* untuk menghasilkan pendapatan bagi para pelaku. Implikasi dari proses tersebut mengakibatkan:

1. *Malware* dapat menginstal aplikasi tanpa mendapatkan izin terlebih dahulu.
2. Aktivitas jahat yang tersamarkan sehingga memungkinkan adalah penyusup ke Google Play.
3. *Malware* dapat melepaskan *rootkit* yang tertanam karena dapat mencapai efek yang sama bahkan tanpa itu.

3.4.5 *Analisis Dinamis*

Tahap ini melakukan analisis secara dinamis terhadap *malware HummingBad*. *Malware* dijalankan dengan menggunakan emulator Android Phoenix yang diinstal pada mesin virtual. Hasil analisis kemudian didokumentasikan dan dibuatkan laporannya.

3.4.6 *Reverse Engineering*

Tahap ini melakukan pembongkaran *source code* dari *malware HummingBad* dengan menggunakan *tools* javadecompilers . *Source code* yang ada dianalisis untuk menentukan bagian dari *source code* mana yang dampaknya sangat besar sehingga menimbulkan perangkat Android terinfeksi *malware*.

3.4.7 *Documentation & Reporting*

Tahapan terakhir adalah *Documentation & Reporting* dimana pada tahap ini proses analisis yang telah dilakukan kemudian didokumentasikan untuk disimpan dan diterapkan pada laporan penelitian di bab 4.