BAB III
METODE PENELITIAN

3.1 Langkah Penelitian

3.1.1 Alur Penelitian Cuckoo Sandbox

Pada penelitian menggunakan tools Cuckoo Sandbox ini, langkah pertama yang harus dilakukan adalah membangun lingkungan penelitian. Lingkungan penelitian ini menggunakan mesin Linux yaitu Ubuntu 16.04. agar simulasi dan analisis dapat dilakukan, mesin linux harus diatur agar dapat menjalankan simulasi dengan cara menginstall virtualbox pada mesin linux tempat simulasi dan analisis yang akan dijalankan. Virtualbox adalah software virtualisasi untuk memasang sebuah sistem operasi, dimana Virtualbox akan diinstal sistem operasi Ubuntu 16.04.

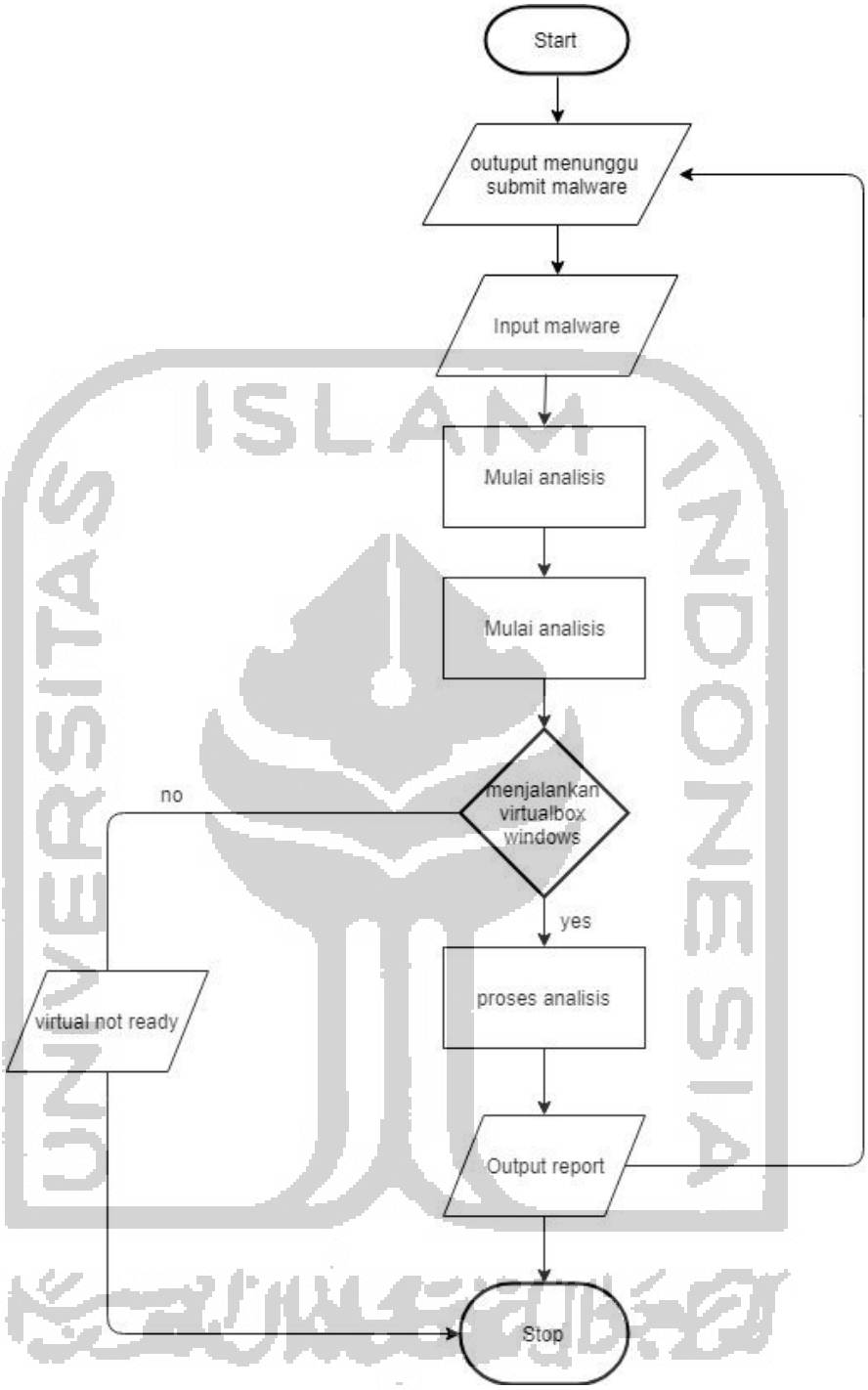
Langkah selanjutnya adalah melakukan instalasi Cuckoo Sandbox dari repository github milik Cuckoo di sistem operasi Linux 16.04. seperti yang kita ketahui cuckoo sandbox adalah ekstensi dari cuckoo yang khusus untuk menganalisis *Ransomware*.

Setelah Cuckoo Sandbox telah dipasang, langkah selanjutnya adalah melakukan konfigurasi terhadap beberapa file di dalam direktori Cuckoo Sandbox. Konfigurasi yang dilakukan terdiri dari nama mesin, sistem operasi yang digunakan, database yang digunakan, tools analisis lain yang digunakan seperti analisis jaringan, dan lain-lain.

Hal yang perlu dipersiapkan selanjutnya adalah Agent.py. pada penelitian ini, Agent.py adalah file ekstensi python yang nantinya akan digunakan dalam proses pengolahan malware.

Cuckoo Sandbox memerlukan beberapa tools tambahan untuk menunjang analisis yang akan dilakukan, beberapa tools berupa modul Python yang dapat dipasang menggunakan PIP (Python Install Packages), namun ada juga yang dapat dipasang menggunakan perintah apt-get *install*.

Alur kerja Cuckoo saat melakukan analisis sampel *Ransomware* dapat dilihat pada gambar 3.1



Gambar 3. 1 Alur analisis Cuckoo Sandbox

Setelah Cuckoo berhasil dijalankan, kita dapat melakukan submit *Ransomware* melalui *web browser* dengan mengakses halaman web milik Cuckoo sandbox. Setelah *submit*, Cuckoo akan mulai melakukan analisis, setrlah analisis selesai, hasil analisis dapat dilihat pada bagian *result*.

3.2 Studi Pustaka

Studi pustaka dilakukan dengan mengumplulkan dan mempelajari refrensi berupa paper, literature, makalah, presentasi, dokumentasi tentang sandboxing, instalasi CuckooSandbox, implementasi dan eksekusi *malware,* memetakan dan klasifikasi evolusi dari malware. Hal ini dilakukan untuk memahami tool yang digunakan, serta informasi yang berkaitan dengan penelitian, serta error-error yang mungkin terjadi selama proses penelitian.

3.3 Analisi Kebutuhan Sistem

Analisis kebutuhan dalam penyelesaian penelitian analisis *malware* ini didasarkan pada kebutuhan sistem untuk menjalankan tools dan analisis *malware* tersebut. Hasil dari analisis kebutuhan ini adalah:

3.3.1 Analisis Kebutuhan Perangkat Keras

a. Laptop

Laptop yang digunakan pada penelitian ini adalah laptop HP 14-BW015AU dengan spesifikasi prosesor AMD A9-9420 Radeon R5, 3.00 Ghz dengan RAM 4GB menggunakan sistem operasi Ubuntu 16.04 untuk melakukan simulasi dan analsisi *malware* dan Windows 10 64bit untuk proses penulisan laporan.

3.3.2 Analisis Kebutuhan Perangkat Lunak

a. Python 2.7

Python adalah Bahasa pemrograman yang dapat melakukan eksekusi sejumlah instruksi multiguna secara langsung (interpretative) dengan metode orientasi objek (Object Oriented Programming) serta menggunakan semantic dinamis untuk memberikan tingkat keterbacaan syntax (Advernesia,2018). Python yang digunakan adalah python dengan versi 2.7 dan diinstal pada system operasi Ubuntu.

b. CuckooSandbox

CuckooSandbox adalah tools yamg digunakan untuk menganalisis malware yang akan di eksekusi pada sistem operasi yang telah di injeksikan malware.

c. Volatility

Volatility Framework adalah kumpulan tools yamg diimplementasikan dengan python dibawah lisensi public GNU, untuk ekstraksi artefak digital dari sampel volatile memori (RAM). Teknik ekstraksi dilakukan sepenuhnya independen dari sistem yang sedang tetepi menawarkan visibilitas ke status runtime sistem. Framework ini dimaksudkan untuk

memperkenalkan orang kepada teknik dan kompleksitas yang terkait dengan ekstraksi artefak digital dari sample memori yang mudah menguap dan menyediakan platform untuk bidang penelitian ini di masa depan.

d. Virtualbox

Virtualbox adalah software gratis milik Oracle yang fungsi utamanya adalah mem-visualisasi-kan sebuah atau banyak Sistem Operasi (OS) di dalam Sistem Operasi utama kita.

e. MongoDB

MongoDB adalah salah satu produk database noSQL Open Source yang menggunakan struktur data JSON untuk menyimpan datanya. MongoDB adalah merupakan database noSQL yang paling populer di internet. MongoDB sering dipakai untuk aplikasi berbasis Cloud, Grid Computing, atau Big Data.

f. Cacti

Cacti adalah salah satu software yang digunakan untuk keperluan monitoring yang banyak digunakan saat ini. Cacti menyimpan semua data atau informasi yang diperlukan untuk membuat grafik dan mengumpulkannya dengan database MySQL. Untuk menjalankan Cacti diperlukan software pendukung seperti MySQL, PHP, RRDTool, net-snmp, dan sebuah webserver yang support PHP seperti Apache atau IIS.

Cacti merupakan sebuah software MRTG (Multi Router Traffic Grapher) web based yang menjadi solusi komplit untuk network graphing yang memanfaatkan penyimpanan data RRDTool dan fungsi grafik. Pada umumnya Cacti digunakan untuk menampilkan graph dari suatu jaringan kebanyakan parameter bandwitdh used yang di-graph. Tak hanya itu Cacti juga bisa menampilkan parameter *ping*, uptime dari sebuah hardware misalnya server, router, access point.

3.3.3 Analisis Kebutuhan Lainnya

a. Analisis Kebutuhan Masukan atau *Input*

Kebutuhan input dalam proses simulasi dan analisis ini adalah *malware* yang bekerja pada perangkat Windows. Beberapa sampel *malware* sengaja disediakan oleh developer melalui Github untuk orang-orang yang ingin menggunakannya untuk tujuan akademis. *Malware* yang sama juga diinjeksikan pada Windows untuk mengetahui aktifitas *maware* tersebut.

b. Analisis Kebutuhan Proses

Proses yang dibutuhkan dalam proses analisis pada sistem Cuckoo Sandbox adalah sistem melakukan dynamic analisis terhadap malware yang telah diunggah ke dalam sistem. Serangkan proses memetakan dan klasifikasi malware menggunakan diagram yang memetakan dan klasifikasi karakteristik malware

c. Analisis Kebutuhan Keluaran atau Output

Keluaran akhir yang dihasilkan oleh analisis menggunakan Cuckoo Sandbox adalah informasi dari malware didalam localhost sistem. Sedangkan keluaran akhir dari memetakan evolusi malware adalah berupa diagram dimana bagian tersebut adalah representasi dari *class* dan *object* property yang telah dibuat.

3.3.4 Analisis kebutuhan proses

Pada saat melakukan penelitian analisis *Ransomware* menggunakan Cuckoo Sandbox, terdapat beberapa proses yang terjadi. Proses berawal dari mengunduh sampel *Ransomware* dari repository Github. Kemudian sampel *Ransomware* yang telah diunduh tadi di *submit* kepada Cuckoo Sandbox. Setelah proses *submit* selesai, selanjutnya Cuckoo Sandbox akan menjalankan Virtualbox untuk melakukan proses analisis. Setelah analisis selesai dilakukan, Cuckoo Sandbox akan memproses hasil analisis yang telah didapatkan akan di tampilkan ke dalam *report* melalui halaman website.

Kemudian, proses untuk melakukan analisis *Ransomware* pada file dengan membuka *result* pada website Cuckoo Sandbox, setelah itu akan ditampilkan halaman *report* pada website. Setelah itu dapat masuk navigasi bar *behavorial analisys,* dan disitu dapat dilihat kebiasaan dari *Ransomware* yang telah kita analisis.

3.4 *Ransomware* Analisys

Tujuan dari penelitian ini adalah untuk membuktikan apakah *Ransomware* dapat mengakses file atau tidak. Maka, langkah awal dari penelitian ini adalah melakukan eksekusi file.exe yang diduga sebagai *Ransomware* ke dalam Cuckoo Sandbox. *Ransomware* yang sama juga dapat dieksekusi pada sisi mesin virtual. Awal eksekusi pada Cuckoo Sandbox adalah dengan melakukan *submit* pada website Cuckoo, kemudian Cuckoo Sandbox akan mengeksekusi dan melakukan analisis secara otomatis. Laporan dari hasil analisis Cuckoo Sandbox dapat dilihat dalam halaman website.

Untuk analisis pada sisi virtual diawali dengan perangkat yang sudah diinjeksi *Ransomware*. setelah file.exe dijalankan pada Virtualbox yang sudah diinstal sistem operasi, akan dianalisis monitoring Cacti. Cara melakukan analisis dengan Cacti adalah dengan melihat *live report* dari proses berjalannya program dalam CPU.

Hasil akhir dari rencana analisis ini adalah diharapkan dapat menemukan dan membuktikan adanya *Ransomware* mengakses file pada sisi Virtualbox, serta memetakan evolusi *Ransomware* dari hasil beberapa *Ransomware* yang telah dijalankan pada Cuckoo Sandbox.