BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sudah tidak dapat terelakkan lagi dengan ditemukannya teknologi-teknologi baru yang sejatinya dimaksudkan untuk membantu manusia dalam hidup kesehariannya. Internet adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputer di seluruh dunia. Sehingga membuat orang dapat bertukar informasi maupun data, banyaknya aktifitas internet membuat pengguna internet rentan terhadap *malware*. Selain dari banyaknya penggunaan internet, m*alware* sudah semakin mudah masuk ke dalam komputer melalui perantara *file*. *Malware* merupakan *software* atau perangkat lunak yang ditulis dengan tujuan jahat dan merugikan karena dapat menggangu kerja sistem dalam komputer. *Malware* masuk ke sistem tanpa izin dan melakukan eksploitasi, misalnya untuk membahayakan data, perangkat atau orang.

Malware diprediksikan akan semakin mutakhir, agresif dan tidak dapat terhindarkan. Oleh karena itu diperlukan teknologi baru yang mampu menganalisis *malware* untuk mengantisipasi masuknya *malware* ke dalam komputer. Oleh karena itu perlu adanya proses analisis *malware* dengan sistem yang canggih, dengan menggunakan beberapa fungsionalitas dalam satu sistem. FAME merupakan salah satu satu *frame work* yang dibuat untuk melakukan analisis *malware* dengan melakukan tugas sebanyak mungkin dan melakukan yang terbaik untuk menentukan modul pemrosesan yang harus dijalankan selama setiap analisis dan melakukan eksekusi modul rantai agar dapat mencapai analisis *end-to-end*.

Saat *malware* dianalisis didapatkan informasi dasar obyek, komponen penyusun dari obyek yang dianalisis dengan berbagai cara, salah satunya adalah dengan melakukan ekstraksi. Ekstraksi adalah blok teks yang menampilkan informasi *file* penyusun dari obyek. Dalam proses ekstraksi inilah bisa mendapatkan informasi tentang *malware*. Dengan ini penulis mencoba membuat sistem untuk analisis *malware* menggunakan FAME, analisis *malware* ini memiliki manfaat untuk menampilkan beberapa informasi. Informasi ini dibutuhkan untuk mempelajari *malware* dan

diharapkan dapat membantu untuk mengetahui *malware* secara lebih detail, sehingga mendapatkan hasil yang bisa diberikan kepada *developer* antivirus sebagai bahan untuk membuat antivirus.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka diambil beberapa rumusan masalah dalam penyusunan Proyek Akhir ini adalah sebagai berikut.

1. Bagaimana cara merancang sistem analisis *malware* dengan FAME ?
2. Bagaimana cara mengaplikasikan FAME untuk analisis *malware* ?

1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam penyusunan Proyek Akhir ini adalah sebagai berikut.

1. Merancang dan membangun sistem analisis *malware* dengan FAME.
2. Melakukan pengujian sistem analisis *malware* dengan FAME.

1.4 Batasan Masalah

Dari beberapa rumusan masalah yang terjadi maka terdapat batasan masalah, untuk membatasi meluasnya bahasan masalah yang akan diteliti, maka dibatasilah masalah yang berkaitan dalam penyusunan Proyek Akhir ini adalah sebagai berikut.

1. Sistem dijalankan pada mesin virtual.
2. Sampel yang digunakan diambil dari internet dan dari komputer pribadi.
3. Sistem ini tidak bisa menghapus *malware.*
4. Tidak menangani hal lebih jauh mengenai pencegahan dan penanganan terhadap *malware*.
5. Tidak dilakukan *forensic* terhadap memori, jaringan.
6. Tidak melakukan analisis *malware* dinamis.
7. Tidak membahas tentang bahasa *Assembly* dan *Disassambly*.
8. Hasil analisis *report* hanya menjelaskan fitur sistem yang telah dibangun dan hasil analisis sampel secara garis besar, tidak terperinci secara spesifik.

1.5 Definisi Operasional

Definisi operasional dimaksudkan untuk menghindari kesalahan pemahaman dan perbedaan penafsiran yang berkaitan dengan istilah-istilah dalam penyusunan Proyek Akhir maka definisi yang perlu dijelaskan adalah sebagai berikut.

1.5.1 Sistem Analisis

Adalah suatu usaha untuk mengamati secara detail sesuatu hal atau benda dengan cara menguraikan komponen-komponen pembentuknya atau penyusunya untuk di kaji lebih lanjut.

1.5.2 Analisis *Malware*

Adalah studi tentang *malware* dengan membedah komponen-komponen yang berbeda dan mempelajari perilakunya untuk mengetahui cara *malware* tersebut bekerja dan mencari celah dalam keamanan. [1]

1.5.3 Malware

Merupakan singkatan dari malicious *software* adalah perangkat lunak yang ditulis dengan tujuan jahat, *malware* masuk ke sistem tanpa izin dan melakukan eksploitasi, misalnya untuk membahayakan data, perangkat atau orang. [2]

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan pada Proyek Akhir ini menggunakan metode waterfall, metode waterfall merupakan metode yang sering digunakan oleh penganalisa sistem pada umumnya. Inti dari metode waterfall adalah pengerjaan dari suatu sistem dilakukan secara berurutan atau secara *linear*. Jadi jika langkah ke-1 belum dikerjakan, maka langkah ke-2 tidak dapat dikerjakan. Jika langkah ke-2 belum dikerjakan maka langkah ke-3 juga tidak dapat dikerjakan, begitu seterusnya. Secara otomatis langkah ke-3 akan dapat dilakukan jika langkah ke-1 dan ke-2 sudah dilakukan.

1 Pengumpulan Kebutuhan

Tahap untuk mengindentifikasi format seluruh perangkat keras (*hardware*) dan perangkat lunak (*software)* yang dibutuhkan secara garis besar dalam membangun sistem yang dibuat.

2 Perancangan sistem

Merancang sistem dilakukan untuk memberi gambaran umum terhadap sistem yang dibuat, dengan membuat perancangan sementara yang berfokus pada penyajian untuk persentasi.

3 Pengujian sistem

Pengujian sistem dilakukan dengan mencoba sistem yang telah dibuat yang diuji dengan parameter-parameter yang telah ditentukan sebagai tolak ukur apakah sistem sudah berjalan dengan baik atau belum.

4 Pembuatan Laporan

Pada tahap ini dilakukan pembuatan laporan terkait aktivitas yang telah dilakukan selama proses percobaan berikut dengan penarikan kesimpulan dan hasil yang didapatkan dalam percobaan.

1.7 Jadwal Pengerjaan

Adapun struktur jadwal pengerjaan yang dilakukan untuk membangun sistem analisis *malware* dengan FAME pada Tabel 1.1.

Tabel 1. 1 Jadwal Pengerjaan Proyek Akhir

No	Kegiatan	Jadwal Pengerjaan 2017/2018																	
		April				Mei				Juni				Juli				Agustus	
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
1.	Pengumpulan kebutuhan.																		
2.	Perancangan sistem.																		
3.	Pengujian sistem.																		
4.	Pembuatan laporan.																		