BAB I
PENDAHULUAN

1.1 Latar Belakang

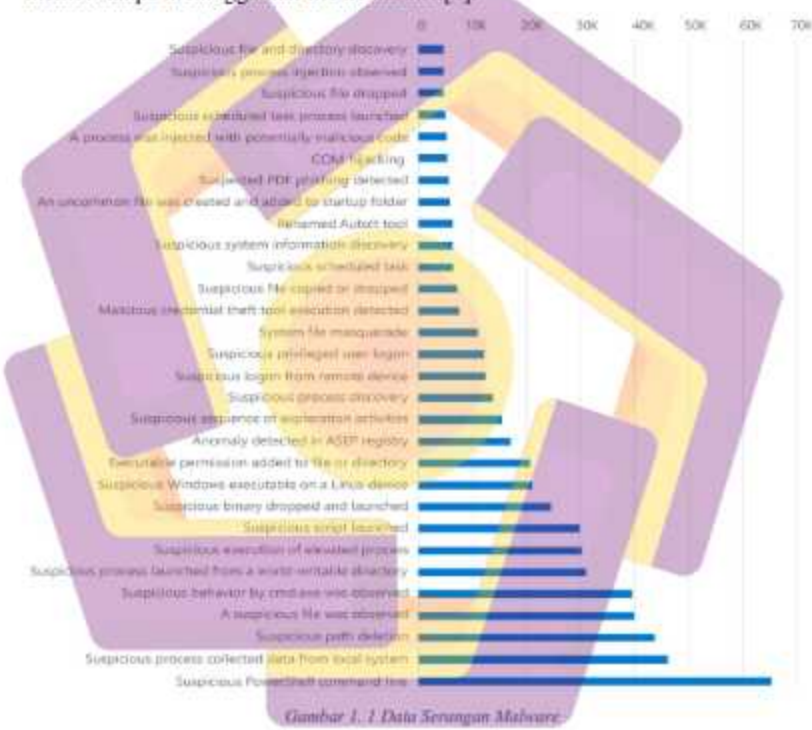
Kejahatan dunia maya telah mengancam keamanan nasional yang menargetkan semua sektor infrastruktur penting, termasuk layanan kesehatan masyarakat, teknologi informasi, jasa keuangan dan sektor energi[1]. Indonesia mendeteksi serangan siber dalam rentang waktu Januari 2020 sampai Desember 2020 sebanyak 316,167,753 serangan dimana sumber serangan tertinggi berasal dari India sebanyak 15,91% total serangan di urutan kedua berasal dari Indonesia sebanyak 12,26% total serangan[2].

Tabel 1 Sumber Serangan dari Berbagai Negara

	Negara	%
1	India	15,91
2	Indonesia	12,26
3	Irlandia	11,31
4	Vietnam	8,14
5	Rusia	5,91
6	Pakistan	5,82
7	Cina	3,96
8	Bangladesh	3,70
9	Amerika Serikat	2,66
10	Venezuela	2,44
11	Other	27,89

Fileless malware merupakan *malware* yang sebagian besar memiliki komponen yang sah di dalam perangkat target, yang sulit untuk dideteksi karena tidak meninggalkan file pada komputer target, hal tersebut yang membedakan antara *fileless malware* dengan *file-based malware* yang meinggalakan file ke

komputer target[3]. Microsoft Digital Defense mendeteksi 24 triliun sinyal serangan per hari sejak pertengahan 2020 sampai Juni 2021. Lebih dari 60 ribu *Powershell Command Line* yang mencurigakan yang telah terdeteksi oleh Microsoft sejak Mei-Juni 2021[1]. Antivirus yang didesain oleh *developer* untuk mendeteksi dan mencegah adanya file *malware* menjadi sangat sulit untuk mendeteksi jenis *fileless malware* karena *fileless malware* di jalankan langsung ke memori tanpa meninggalkan file ke hardisk[4].



Gambar 1. 1 Data Serangan Malware

Teknik analisis *malware* dengan metode statis dan dinamis sudah umum digunakan[5]. Analisis statis merupakan teknik analisis suatu file tanpa menjalankan nya. Sedangkan analisis dinamis teknik analisis dengan menjalankan sampel *malware* kemudian dilakukan pemantauan aktivitas. Forensik memori merupakan teknik untuk mencari dan mengekstrak artefak dari memori komputer (RAM). Analisis *malware* menggunakan metode memori forensik sangat berguna

untuk menemukan komponen yang berbahaya karena di dalam memori (RAM) menyimpan banyak informasi seperti aplikasi yang sedang berjalan, objek yang diakses (file, *registry*), koneksi jaringan yang aktif, *modules*, *kernel drivers*, dan informasi lain[6].

1.2 Perumusan masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan sebuah permasalahan untuk penelitian yang akan dilakukan adalah sebagai berikut.

1. Bagaimana teknik melakukan akuisisi RAM pada perangkat windows yang dijalankan pada VirtualBox?
2. Bagaimana cara melakukan analisis terhadap RAM perangkat windows yang telah diakuisisi?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1. Mengimplementasikan teknik akuisisi RAM menggunakan VBoxManage debugvm yang ada pada VirtualBox.
2. Melakukan analisis terhadap RAM yang telah diakuisisi menggunakan Volatrik automation Volatitlity Framework.

1.4 Batasan Masalah

Dari uraian rumusan masalah di atas, peneliti menetapkan batasan pada masalah tersebut adalah sebagai berikut.

1. Sistem operasi yang diujikan untuk menjalankan *malware* adalah windows 10.
2. Mesin virtual yang digunakan untuk menjalankan sistem operasi windows 10 adalah VirtualBox.
3. *Malware* yang digunakan adalah sebuah *script* yang dijalankan melalui *Powershell*.
4. Alat digunakan untuk melakukan akuisisi RAM adalah VBoxManage debugvm dari VirtualBox.

1.5 Manfaat Penelitian

Manfaat dari peneilitian ini adalah sebagai berikut.

1. Mengetahui cara kerja dan aktivitas *fileless malware*.
2. Berkontribusi dalam bidang penelitian forensik dengan membangun sebuah *automation tools* dari *volatility framework* yaitu Volatrik.