Analisis Pengaruh VSM Terhadap Proses *Akuisisi* Memori Menggunakan Metode Analisis *Dinamis*

Sinta Nur Maulina[1], Niken Dwi Wahyu Cahyani, Ph.D[2], Erwid Musthofa Jadied, S.T.,M.T.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[4]Divisi Digital Service PT Telekomunikasi Indonesia
[1]sintanurmaulina@student.telkomuniversity.ac.id, [2]nikencahyani@telkomuniversity.ac.id,
[3]jadied@telkomuniversity.ac.id

Abstrak

Awal mulanya forensik hanya difokuskan pada analisis data yang berada pada *harddisk* dalam sebuah sistem. Tetapi dengan semakin berkembangnya kapasitas penyimpanan serta enkripsi data, menyebabkan penggunaan teknik digital forensik tradisional mengalami kendala. Maka yang lebih poly serta proses yang tidak memakan waktu lama dalam membuat prosesnya, sebagai akibatnya dikembangkan teknik *memory forensics* atau biasa diklaim live *forensics*. Kondisi ini membutuhkan *volatile memory forensic* atau biasa disebut *live forensic*. Terdapat permasalahan pada *live forensic* yaitu pada beberapa *tools* mengalami *crash* pada saat komputer dengan kondisi VSM (Virtual Secure Mode) aktif. Hal ini menyebabkan bukti yang ingin diambil menjadi hilang. Oleh karena itu, diperlukan untuk mencari penyebabnya. Terdapat beberapa tools akuisisi memori berbasis perangkat lunak yaitu *autopsy, isobuster, DumpIt, Magnet RAM Capturer*. Dari hasil percobaan yang telah dilakukan, tools yang mengalami crash yaitu DumpIt v1.3.2.20110401. Metode penelitian yang dipakai untuk melakukan analisis pengaruh VSM pada tool akuisisi memori adalah analis kode dinamis yang menggunakan *WindBg* sebagai alat bantuannya. Tujuan dari penelitian ini yaitu menemukan terjadinya *crash* pada beberapa *tools forensic* sehingga sangat membantu para ahli forensic ketika melakukan penyelidikan.

Kata kunci: live forensics, VSM, tools, crash

At first, forensics was restricted to studying data that was stored on a system's hard disk. However, as storage capacity and data encryption increased, applying conventional digital forensic procedures became more challenging. As a result, memory forensics techniques are developed, or are frequently referred to as live forensics, because the process is quicker and more sophisticated. Volatile memory forensics, often known as live forensics, are necessary for this condition. Live forensics has flaws, specifically that some programs can fail when the computer is in active VSM (virtual secure mode). This results in the retrievable evidence being lost. Therefore, determining the cause is essential. The software-based memory acquisition tools Autopsy, Isobuster, DumpIt, and Magnet RAM Capturer are just a few examples. According to the findings of the experiments, the tools that have crashed include DumpIt v1.3.2.20110401. A dynamic code analysis using WindBg as a tool was utilized to study the impact of VSM on the memory acquisition tool. This study's goal is to identify the instances of crashes in various forensic instruments, which will be highly useful for forensic experts performing investigations.

Keywords: live forensics, VSM, tools, crash

1. Pendahuluan

1.1 Latar Belakang

Forensik, khususnya forensik digital, digunakan untuk memverifikasi bukti digital dalam kasus membutuhkan penanganan dan identifikasi barang digital. Ini sering dikaitkan dengan kejahatan [1]. Penyelidik digital memanfaatkan informasi di komputer penyerang untuk menemukan petunjuk yang dapat membantu dalam membuktikan suatu kasus. Salah satu aspeknya adalah bukti digital yang dapat diambil dari memori utama (RAM), yang mencakup informasi langsung tentang program yang sedang berjalan.

Forensik komputer melibatkan identifikasi, persiapan, ekstraksi, pendokumentasian, dan interpretasi data komputer untuk membuktikan kejahatan dunia maya orang dalam [2]. Terdapat permasalahan yang disebabkan oleh *live forensic* yaitu pada beberapa tools mengalami *crash* pada saat komputer dengan