ANALYSIS OF THE EFFECT OF VSM ON THE MEMORY ACQUISITION PROCESS USING THE DYNAMIC ANALYSIS METHOD

Sinta Nur Maulina[1*], Niken Dwi Wahyu Cahyani[2], Erwid Musthofa Jadied[3]

1. Sinta Nur Maulina, Jl. Telecommunications No. 1, Sukapura, Kec. Dayeuhkolot, Bandung Regency, West Java 40257
2. Niken Dwi Cahyani, Jl. Telecommunications No. 1, Sukapura, Kec. Dayeuhkolot, Bandung Regency, West Java 40257
3. Erwid Musthofa Jadied, Jl. Telecommunications No. 1, Sukapura, Kec. Dayeuhkolot, Bandung Regency, West Java 40257

Article Info
Keywords: Live Forensics, VSM, Tools, Crash
Article history:

DOI :

E-mail address:
sintanurmaulina@student.telkomuniversity.ac.id[1]
,nikencahyani@telkomuniversity.ac.id[2] ,
jadied@telkomuniversity.ac.id[3]

ABSTRACT
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.

.

I. INTRODUCTION

Digital forensics or forensics is used to examine digital evidence when handling a case that requires the handling and identification of digital goods in forensic science, especially to investigate the discovery of digital device content, and is often associated with crime [1]. Digital investigators use information on an attacker's computer to find clues that can help in proving a case. One aspect is digital evidence that can be retrieved from main memory (RAM), which includes immediate information about the currently running program.

Computer forensics is an investigation and computer analysis technique that involves the stages of identification, preparation, extraction, documentation and interpretation of the origin of the data on the computer to serve as evidence of cybercrime incidents [2]. There is a problem in live forensics, namely some tools crash when the computer is in active VSM (virtual secure mode) using a 64-bit operating system, x64-based processor. This causes the evidence to be taken to be lost. Therefore, it is necessary to find the cause. There are several software-based memory acquisition tools, namely autopsy, isobuster, DumpIt, Magnet RAM Capturer. From the results of the experiments that have been carried out, the tools that have crashed are DumpIt v1.3.2.20110401.

VSM is a Hyper-V container that isolates the lsass.exe process from a running Windows 10 machine. Reduces the risk of credentials from a computer using a tool namely mimikatz, and is used for pass-the-hash attacks. Something worth mentioning is that VSM only protects domain [3] credentials. Each partition contains an operating system environment. If windows based, this environment has this architecture consists of the following parts of Windows i.e. system support processes, services, applications, Windows subsystem, Hardware abstraction layer kernel drivers. Each partition works with its own isolation abuts. The separator boundaries between partitions are created and managed by the hypervisor. Isolation partitioning is implemented so that the hypervisor allocates a separate virtual memory space. The hardware resources for each of these partitions mean that the partition is not accessible to the memory that another partition allocates. In a virtualized environment based on Hyper-V, it is managed using a partition called the root partition. Serves other partitions co-located with it. For example, the root partition hosts virtualization services. Provided by the hypervisor to make this service available on other shared partitions. Also this root partition can host device drivers because it is the only partition that has direct access to hardware resources [4].