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].

Hypercalls implements the services that the hypervisor displays to partitions. It involves critical system services enabling the operation of virtual systems, namely memory management services. Each Hyper-V hypercall can be uniquely identified by an identification number, which is referred to as a dialing code. An important prerequisite for a Hyper-V hypercall to be called is the existence of the hypercall page in the context of the partition. The hypercall page is a memory page that stores code to invoke a hypercall according to the Hyper-V specification. This page is exposed by the hypervisor to every partition. The Windows hypervisor is the bridge through which Hyper-V communicates with the hardware. Of course, the hardware is designed and certified to run on the Windows Server operating system. Hyper-V manages virtual machines with hardware partitions. Called a virtual partition. A virtual partition consists of a parent partition and child partitions. Partition for where Windows Server resides. Meanwhile, sub-partitions can be shared with other operating systems can be seen in figure 1.

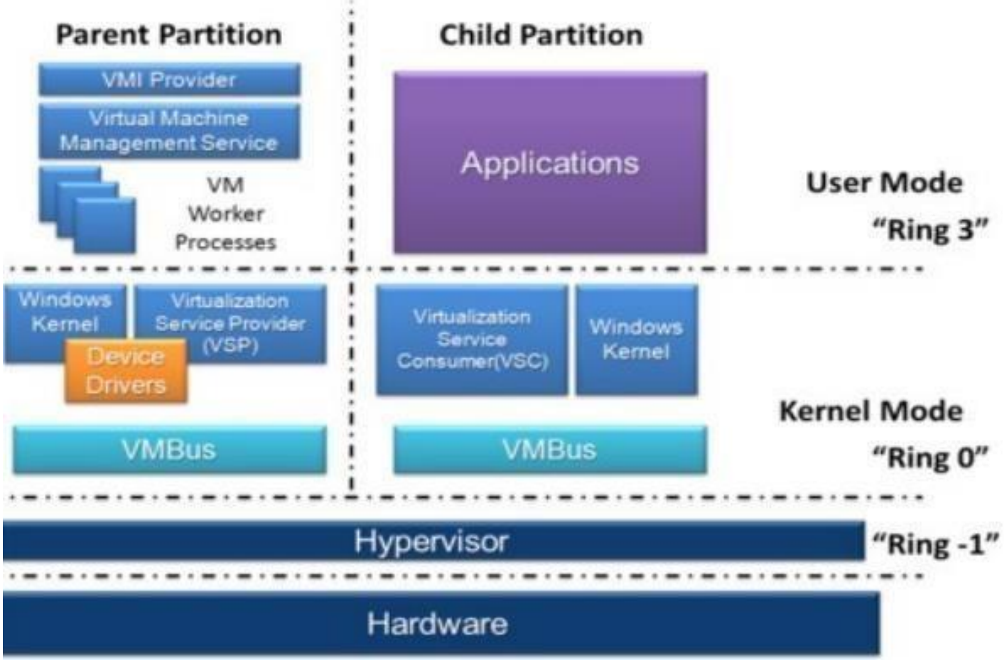

Figure 1 : Hyper-v architecture

WinDbg is a multipurpose debugger for the Microsoft Windows computer operating system, distributed by Microsoft. Debugging is the process of finding and resolving errors in a system in computing that also includes exploring the internal operations of software as an aid to development. It can be used to debug user mode applications, device drivers, and the operating system itself in kernel mode. This type of archive includes a minimum amount of information. It contains only the BSOD error message, information about the driver, the processes that were active at the time of the crash, and which kernel process or thread caused the crash in the generally small kernel memory dump, 1/3 the amount of physical memory. Kernel memory dumps are more specific than minidumps. It contains kernel mode drivers and programs, including memory allocated to the Windows kernel and hardware abstraction layers, and memory allocated to other kernel mode drivers and events. Complete memory dump. largest size and requires memory equivalent to your system RAM plus the 1 MB required by Windows to build this file. Automatic memory dump. sync with kernel memory dumps in case of issues. These differ only in how much space is used to form the dump file. This archive type does not exist in Windows 7. It was added in Windows 8. The memory disposal area is active. This type of filter element cannot determine the cause of the system failure. Windbg is the most powerful debugging and reverse engineering tool on the Windows platform. Windbg, namely X-ray plus MRI plus CT scan of programs running on the Windows operating system, including the operating system itself. It finds the cause of complex problems with programs running in Windows (OS) and programs running in Windows (OS)[5].

Dumplt is a collection of two tools, namely win32dd and win64dd, combined as an executable used to acquire physical memory. Dumplt is designed to be administered to non-technical users using a removable USB drive. Dumplt will take a snapshot from physical memory and save it to the folder[6]. Memory Dump is carried out for the purpose of memory acquisition which has two approaches for performing memory acquisition, namely hardware-based and software-based. There are so many software available to get memory privately. This software software can capture RAM privately. DumpIt is a compact portable software that makes it easy to store the contents of physical memory[7].

Memory acquisition is the process of acquiring volatile memory (RAM) to non-volatile storage (files on disk)[8].

live forensics is a way in a forensic process where the system is still running, this is done because if the system dies then there will be lost data or information[9]. The live forensic method is usually used for cases where there is volatile data where the data will be lost if the power source dies, volatile data is usually stored in temporary media, namely RAM. Meanwhile, live forensics is used to collect data when the affected system is still alive[10]. Virtual forensic investigations mainly rely on data stored on storage media along with primary storage. Volatile memory or random access memory can store information i.e. running processes, incognito browsing sessions, clipboard statistics, information stored in plain text reports.

This study aims to analyze the effect of VSM on the live memory acquisition process using the dynamic method using the windBg method. The Windows Debugger (WinDbg) can be used to debug kernel mode and user mode code, analyze crash dumps, and inspect CPU registers while code is running[11].

II. RESEARCH METHOD

A. Problem Solving Systematics

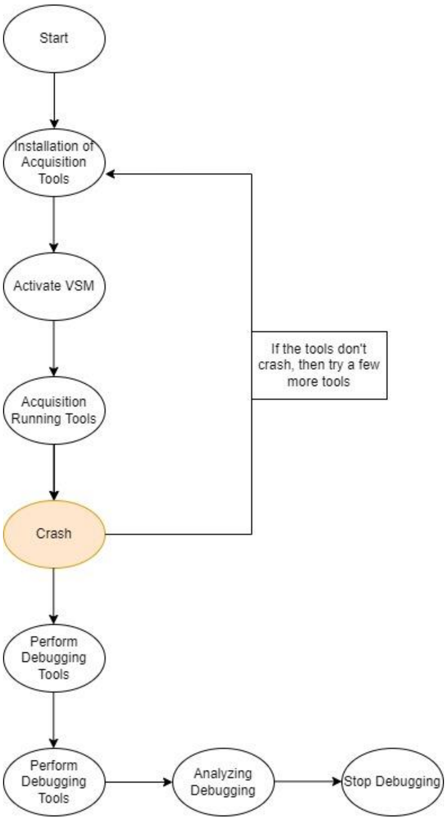
Start
Installation of Acquisition Tools
Activate VSM
Acquisition Running Tools
Crash
If the tools don't crash, then try a few more tools
Perform Debugging Tools
Perform Debugging Tools
Analyzing Debugging
Stop Debugging

Figure 2 : Flowchart Overview of system design

In figure 2, the stages of research in the systematics of solving this problem use qualitative methods, namely literature studies which aim to collect more specific information related to the problem being studied, then this information will of course be utilized if it has something to do with the research being carried out which is shown by the theories relevant theory.

In this research, the method used to analyze the effect of VSM on the memory acquisition tool is dynamic code using WindBg as its auxiliary tool. Software-based memory acquisition tools, namely autopsy, isobuster, DumpIt, Magnet RAM Capturer. However, using this tool on a system with active VSM mode causes a system crash known as a blue screen on death (BSoD). The following is proof that VSM is active by looking for "Task Manager" and checking whether "Secure System" is running or not can be seen in figure 3.