Chapter 3
Volatile Memory Collection and Analysis for Windows Mission-Critical Computer Systems

Antonio Savoldi
University of Brescia, Italy

Paolo Gubian
University of Brescia, Italy

ABSTRACT

Most enterprises rely on the continuity of service guaranteed by means of a computer system infrastructure, which can often be based on the Windows operating system family. For such a category of systems, which might be referred to as mission-critical for the relevance of the service supplied, it is indeed fundamental to be able to define which approach could be better to apply when a digital investigation needs to be performed. This is the very goal of this paper: the definition of a forensically sound methodology which can be used to collect the full state of the machine being investigated by avoiding service interruptions. It will be pointed out why the entire volatile memory dump, with the necessary extension which is nowadays missing, is required with the purpose of being able to gather much more evidential data, by illustrating also, at the same time, the limitation and disadvantages of current state of-the-art approaches in performing the collection phase.

INTRODUCTION

We are currently living in the era of information technology which relies heavily on complex computer network infrastructures, with a multitude of services which need to be issued continuously without interruptions. For the sake of clarity, we might define such a category of computer as mission critical, by pointing out that they need to provide continuity of service over a period of time, as can be seen in the case of Web or Email servers. For this specific category of computer systems,

DOI: 10.4018/978-1-60960-515-5.ch003

when a digital investigation will be performed, a live forensic methodology will be needed. This might be obtained by applying a suitable set of techniques which can be helpful in creating a sufficiently detailed representation of the state of the system being observed. For such a purpose, we need to adopt the set of methods and best practices pertaining to the volatile memory forensic discipline. Although it can be considered still in an infancy stage if compared with other branches of digital forensics, this discipline might provide the means of analysis which fit the need of mission critical digital investigations. The ultimate goal for this applied field of the digital forensic science is to collect evidential data from the contents of a computer's volatile memory, by stating which processes were running, when they were started and by whom, what specific activities those processes were doing and the state of active network connections. As a consequence, system memory could provide a great deal of information about the system's runtime state at the time an incident happened. Moreover, it is interesting to point out that state-of-the-art attack techniques have shown a trend towards memory-only modification whenever possible. Thus, traditional post-mortem approaches may fail to find out the existence of intruders (Petroni, Walters, Fraser, & Arbaugh, 2006; Schatz, 2007). One of the main concerns in the volatile memory collection phase, a mandatory step which needs to be performed before the analysis for gathering evidential data, is what should be collected from the system in order to have a detailed view of the inner state of the system. Beside the well known techniques for acquiring the RAM content (Schatz, 2007; Garner, 2008), new approaches are being used for collecting also the page file of a Windows OS based system (Lee, Savoldi, Lee, & Lim, 2007a; Lee, Savoldi, Lee, & Lim, 2007b), which is worthy to be mentioned as an important component of the virtual memory system, containing plentiful of potential evidential data. Once the main memory and the page file have been collected, the analysis part has to be performed. This phase might be carried out both with string matching and virtual memory space reconstruction. For instance, the system being investigated has two encrypted partitions, which can be accessed by means of TrueCrypt tool (Czeskis, Hilaire, Koscher, Gribble, Kohno, & Schneier, 2008). By seizing and analyzing the page file a couple of passwords are found. These pieces of data are confirmed to be digital evidence being able to guarantee the access to the encrypted partitions, as a result of the direct use of them. A further example may involve the analysis of a set of pedo-pornographic images found in the collected page file. Could these pieces of data be considered as strong, effective evidence capable of incriminating the computer's owner? As a matter of fact, these data could come from a malware which might have downloaded such illegal material in the computer's memory. Besides, we must to prove this fact by correlating that page file area, where the images were found, with the related memory process or at least with some other comparable piece of data, which could come from another memory device. As a result, a piece of data within the page file need to be evaluated and verified according to the context and the ability to verify it by external means.

The remaining part of the article has been organized as follows. Initially, the necessary state-of-the-art related to the collection of the volatile memory will be presented discussing also, at the same time, the advantages and disadvantages of such approaches. Therefore, some consideration about the blurriness of the volatile memory, when collected, will be discussed, by illustrating a promising method to reduce the uncertainty in the volatile collection phase. After that, a detailed analysis about how to collect the page file will be outlined, presenting also a tool which can deal with such a task. Hence, a technique for virtual memory process reconstruction will be sketched by pointing out how a page file can be effectively analyzed and used within a digital investigation.