International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Significance of Residual Artifacts from Random Access Memory

Sreelakshmi K[1], Princy Sugathan[2]

[1, 2]Cochin University of Science and Technology, College of Engineering Kallooppara, Kerala, India

Abstract: ***Insistent data-oriented approaches in computer forensics face some limitations regarding a number of technological developments, that make an in-time investigation more and more difficult. In order to cope with these issues, security professionals have started to inspect alternative data sources and emphasize the value of volatile system information in RAM more recently. By imaging this part of computer memory and by performing forensics analysis of the data located in RAM, it can be easily concluded that accomplishing RAM imagining and analysis should be one of the essential steps in any forensic investigation. This paper will give a brief introduction to digital forensics and the role of live data forensics. Furthermore, the main goal will be to show and explain the importance of forensics of live machines and artifacts which can be found and are used for extracting and analysing data from RAM.***

Keywords: Digital forensics, RAM, Live Data Forensics, Volatile Data, Memory Acquisition

1. Introduction

1.1 Digital Forensics

Digital forensics is the field of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media. It is a relatively new area which is constantly spreading and progressing quickly. Therefore, it requires continuous monitoring of new technologies in order to be up to date. The development of technologies such as smart phones, tablets as well as the continually changing operating and computer file systems requires an in-depth analysis in order to determine the best way how to get information required in investigations. Furthermore, forensic investigation techniques on existing and current technologies are constantly developing.

When a digital incident occurs, there are commonly two approaches followed by investigators to recognize the incident:

Traditional Forensics: In this approach, an investigator pulls the plug on the machine, and then images (copies) the hard disk, either on site or in a lab. An analyst examines the image in a controlled environment by incessant steps in search of evidence.

Live Forensics: In this case the digital incident has occurred and the computer is still running. It is defined as the techniques of examining volatile or partially volatile computer data i.e. data which disappear when the computer shut down or data that is not insistent – often changed. In digital forensics, the analysis of live data is paramount due to procuring information and evidences which are not reachable otherwise. The analysis of live data involves saving and examining volatile data such as Page file, Hibernation file, Crash Dump files and most importantly RAM - Random Access Memory.

1.2 Random Access Memory – RAM

Computers require that when the computer is in operation, certain amount of computer memory called random access memory be used by the operating system and its applications. The computer employs this RAM to write the current processes it is using as a form of a virtual clipboard. The data is there for immediate reference and use by the process. This type of data is called volatile data since it simply goes away and is irretrievable when the computer is off. In order to log what applications were running on a computer, early practice in incident response includes viewing the monitor and recording the running applications on the desktop. But this practice falls far short of documenting the running system. Noting what information exhibits on the screen or simply „pulling the plug“ does not consider or document all the processes running on a system. while, pulling the plug on a running computer results in the loss of this volatile data, which may contain valuable evidence.

1.3 Information found in RAM

There is a lot of information that can be found by analysing RAM depending on the computer and the operating system used. Most significant being active processes, informations on open files, registry entries, informations on network activities, used drivers, logged users, passwords and cryptographic keys, hidden processes and data, malware, temporary data, portable apps, used dynamic link libraries, open sessions and many other vital informations. Significance of such information are as follows:

1.3.1 Processes

There are several different types of processes that may be found in volatile memory. All currently running processes are stored there and may be recovered from the data structures that house them. In addition, hidden processes can be parsed out of memory. Finally, processes that have been terminated may still be residing in memory because the machine has not been rebooted since they were terminated and the space they reside in has not yet been reallocated. These too may be parsed out and analyzed.

1.3.2 Information on network traffic

Information about network connections, including listening ports, currently established connections, and the local and remote information associated with such connections can be recovered from memory. This is useful because tools that are run on the machine itself, can be trojanized by a malicious intruder or user to provide false information back to the analyst. When pulling the information directly from a memory dump using the data structures themselves, it is much harder for an attacker to hide their listening backdoor, or the connection to their home server from which they are transferring malware and other harmful or illegal files. Information about network connections is the most critical information that can be gathered from a computer which is being investigated, more reliable when it comes from static analysis of a memory dump.

1.3.3 Open files and registry handles

The files that a process has open, or any registry handles being accessed by a process, are also stored in memory. Information about the files that a process is using can be extremely valuable. If the process is a piece of malware, the open files might lead an investigator to discover where the malware is stored on the disk, where it is writing its output, or what previously clean files the malware may have modified to serve its own purposes.

1.3.4 Passwords and cryptographic keys

The main advantage of live data forensics is the possibility to recover passwords and cryptographic keys which were potentially used for decrypting data of interest and user accounts. Passwords and cryptographic keys are generally never stored on the hard disk without additional protection. However, when they are used, they have to be stored in RAM and they remain stored there until they are overwritten with another data or until the computer is shut down. When investigator performs a RAM dump (process of obtaining data form RAM), by reviewing collected data it is also possible to find online account passwords, which can have significant impact on the case itself.

1.3.5 Hidden Data

It is attainable for malicious entities or suspects with data they want to protect to store their data in volatile memory. Because investigators do not inspect volatile memory, it is a safer place to conceal information than on a hard disk. It also makes it easy to destroy sensitive information - Only thing user has to do is pull the plug, and a remote attacker can cause a machine to reboot if desired. Besides hiding files in memory, attackers can also execute malicious code residing in memory instead of storing it on the disk, making it challenging for reverse engineers to attain copies of programs and investigate how they are working and how to lessen the threats they pose. Critical information can be discovered while analysing volatile memory for hidden files and code.

1.3.6 Malicious Code

The attackers run exploits from memory instead of storing malicious code on the hard disk itself. This is to avoid detection, since anti-virus software and other malware detection tools are not currently as good in analyzing volatile memory for malicious code as they are analyzing the hard disk, and some do not have this capability at all. It also benefits attackers by making it harder for analysts to recover. Rootkit is an example that runs in memory and leaves no trace on the affected user's system.

1.3.7 Decrypted content

While recovering keys and passwords can lead investigators to encrypted content, it may be possible to recover data from encrypted files without having the key. When the suspect accesses an encrypted file, the content is unencrypted and loaded into memory. This unencrypted content may remain in memory even after the suspect has closed the file, as long as it is not overwritten by something else. Parsing through volatile memory may reveal fragments of files, or even whole files that would otherwise be unrecoverable if the key or password used to encrypt the data could not be discovered.

1.3.8 Internet data

In this modern times, it is very common for everybody to use the Internet in their daily work or surf the web in their spare time. All research, networking, communication and similar is usually done via Internet. Additionally, it is also very common for people to store their data in the Cloud and not locally on their computers. The data that is being downloaded from the Internet will always pass through RAM. Because of this fact, it is possible to retrieve Gmail or Yahoo emails, Skype conversations and many more. These valuable data would be impossible to recover by "post-mortem" analysis since it is deleted as soon the PC is turned off.

1.3.9 General files

The files that are opened, read and modified on a computer have to pass through RAM. Usually what happens is that the program creates a temporary copy of the file, stores it in the RAM and later when modification is complete, the files is saved on the media. This temporary file can later be recovered in full or just its fragments from the RAM. This is only one of the many possible scenarios but what is important that depending on the RAM size, can in some cases hold large number of files that were opened or used on the computer. Depending on the case, information that a files was used on a certain computer can have big significance. Furthermore, one of the most basic operations done on any given computer is the copy/paste feature. Each time sometime is placed in the clipboard, it is stored in RAM and therefore it is possible to recover it.

2. Proposed System

To retrieve all the information from the ram, have to acquire or take a copy of ram and then analyse it. In order to acquire volatile memory, there are two methods: hardware acquisition, and software acquisition. From a forensics approach, it is preferable to use hardware-based acquisition because it is more reliable and challenging for an attacker to corrupt, but software-based acquisition is more popular method due to its cost-effectiveness and ease of availability.

Software extraction is a much more common way for obtaining data from RAM and it is recommended to perform

it during every computer acquisition in case the computer is active. The main problem of software solutions occurs in case the computer is already compromised, the offender can easily additionally hide his data from such tools or give incorrect data. Another deficiency of software solutions is that, when they are initiated, they themselves are using RAM just like all other programs and thereby they are potentially erasing other, possibly important information. With software tools we need to pay attention that they leave the smallest possible footprint, receptively that they occupy the least possible memory space. Another important fact is that they are operating in the so called "Kernel" mode. This means that the application itself has more rights in the system and that it can reach more information in the system. The main advantage of software tools is that they are free of charge and that they simplify the takeover of RAM so that it can be performed by untrained personnel.

Here proposes a software method for acquiring a forensic copy of a computer"s RAM. It relies on leveraging the \\.\Device\PhysicalMemory section object.

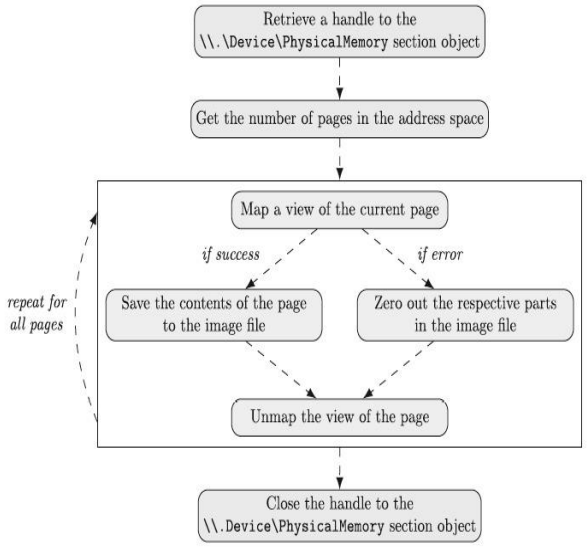

Figure 1: Algorithm for acquiring a forensic copy of memory.

Steps:

1) Calling "ZwOpenSection" function in the first step to retrieve a handle to the \\.\Device\PhysicalMemory object.
2) Portions of RAM may then be read out page wise after determining the actual size of memory, with the help of the "ZwMapViewOfSection" function.
3) A mapped section can be directly written to the image file in kernel space.

After obtaining the raw image of RAM, analysing the result in order to retrieve the important informations such as Processes, Network Informations , Open files, Passwords, cryptographic keys, Hidden data and Malicious codes.

3. Conclusion

Live data forensics should become a part of regular forensic procedures. During every computer analysis ,it is necessary to acquire RAM. The acquisition itself takes much less time than the acquisition of other types of memories and the possibility that it contains information important for the case which would otherwise be unavailable, is very high. Even though the procedure itself, the methodology and analysis are neither sufficiently examined nor documented, the potential results always make up for it. The data that can be found in the RAM can sometimes contain enough evidence to solve the whole case. Here proposes to develop a tool in order to retrieve important informations from the RAM. This will lead to the investigators to collect all the volatile informations without any alterations and this will help them to conclude their investigation successfully without any loss of information.

Acknowledgment

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of college of engineering Kallooppara for their immense support.

References

[1] Ellick M. Chan,"A framework for live forensics", https://www.ideals.illinois.edu/bitstream/handle/2142/24365/Chan_Ellick.pdf?sequence=1, 7.1.2015
[2] Kristine Amari, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory", https://www.sans.org/readingroom/whitepapers/forensics/techniques-toolsrecovering-analyzing-data-volatile-memory-33049, 7.1.2015
[3] Rushita Dave , Nilay R. Mistry , Dr. M. S. Dahiya "Volatile Memory Based Forensic Artifacts & Analysis", http://www.ijraset.com/fileserve.php?FID=162
[4] Gabriela Limon Garcia, "Forensic physical memory analysis: an overview of tools and techniques", http://www.tml.tkk.fi/Publications/C/25/papers/Limongarcia_final.pdf
[5] Timothy Vidas, "The acquisition and analysis of randomaccessmemory",https://pdfs.semanticscholar.org/409a/5f16169bf208d55ca994cdd8638624392faf.pdf
[6] Michael Hale Ligh,Andrew Case,Jamie Levy,AAron Walters,"The art of memory forensics", https://news.asis.io/sites/default/files/The%20Art%20of%20Memory%20Forensics.pdf
[7] "Volatile Memory Based Forensic Artifacts &Analysis" http://www.ijraset.com/fileserve.php?FID=162

Author Profile

Sreelakshmi K obtained the Degree of Bachelor of Technology in Computer Science and Engineering from College of Engineering, Chengannur in 2014. She is now pursuing her master degree in Computer Science with specialization in Cyber Forensics and Information Security at College of Engineering, Kallooppara under Cochin University of Science and Technology.

Princy Sugathan obtained B.Tech in Computer Science and Engineering from College of Engineering Chengannur and M.Tech in Software Engineering from Cochin University. She is currently working as Assistant Professor in College of Engineering, Kallooppara.