A Volatile Memory Analysis Tool for Retrieval of Social Media Evidence in Windows 10 OS based Workstations

Ranul Thantilage
School of Computing
Asia Pacific Institute of Information Technology
Colombo, Sri Lanka
ranulthantilage@gmail.com

Neera Jeyamohan
School of Computing
Asia Pacific Institute of Information Technology
Colombo, Sri Lanka
neera@apiit.lk

Abstract— **Crimes are rapidly increasing, and criminals today use digital devices to facilitate criminal activities. The majority of individuals now own at least a Personal Computer (PC). This has in turn led to Social Media being used as a key medium for information gathering and exchange. Criminals tend to search through social media platforms and extract data which will facilitate them. Additionally, social media platforms such as Facebook, Viber, Skype are used to exchange information about criminal activities. Such information relating to social media can be highly critical evidence at a forensic investigation. A variety of different tools have been necessary for forensics investigators to extract evidence from computers. The main focus on capturing traces left behind after crimes has been the data stored in hard drives. Yet, a significant amount of data is stored in volatile memory as well, and these traces might be very important evidence in solving a case. But the volatile memory is mostly not looked at. All such information exchanged through such applications has to pass through the volatile memory of the system at some point. Even though many applications tend to provide end-to-end encryption, research on volatile memory forensics shows that applications yet write unencrypted data to the RAM (Random Access Memory). This has led to a new area of research towards patterns in how data are written in the volatile memory. This will be a next step in digital forensics, which would assist in recovering evidence that would otherwise get completely lost.**

Keywords—Volatile Memory, Digital Forensics, Social Media, Evidence

I. Introduction

In the last decade, more and more users have started using digital devices to carry out their day to day activities. Because of the increasing demand, vendors also have started announcing new cutting-edge devices. The introduction of new devices has also introduced a variety of problems to forensic investigators, and they need beneficial applications to detect and prevent numerous malicious attacks. Applications built for specific purposes use the volatile memory to store data temporarily for further processing. Therefore, volatile memory becomes a valuable source for evidence acquisition during an investigation. On the other hand, when it comes to retrieving evidence from the volatile memory of a system there are very few options available at a forensic investigator's disposal.

Another technological advancement that has developed over the course of time is the amount of data that has been exchanged using social media platforms. Therefore, social media platforms have become a preferred method for information storage, sharing and processing. Extracting evidence stored from such applications can be a huge benefit for an investigation. This research paper concentrates on identifying the challenges related to extracting evidence from social media applications and challenges related to volatile memory analysis and discusses a method that can be used to extract volatile memory based evidence.

II. Background

"Computer systems are windows to the past" [4]. A computer stores a considerably large amount of data and one should be able to draw out a complete timeline of events that has happened in the user's life by analyzing the pattern. Criminals often tend to leave traces of evidence in digital devices and such evidence might help the investigators to relate the evidence they collect physically and digitally, and thus it will ultimately shed light on the investigation.

Volatile memory is a sector that is mostly not looked upon during data analysis. Volatile Memory refers to the RAM, cache or any temporary storage medium which is used to store the data for future processing and the data is lost if the power is disconnected. [5] stated that any data "travelling" through a computer, should pass through the RAM at some given point. Whatever the type of process it is, temporary data should be recorded on memory blocks in the RAM. Volatile forensics is also referred to as Live Data Forensics [5] due to the nature of evidence acquisition and analysis.

According to [7] volatile memory analysis faces three types of challenges such as hardware issues, software issues and legal issues. According to [2], while conducting volatile forensic investigations, there are steps that should be followed by the first responders and crime scene investigators. These include:

- The system should not be restarted until all data from volatile media are retrieved.

978-1-5386-2425-8/17/$31.00 ©2017 IEEE

- Keep a record of system date and time and other command history.
- Consider all applications are compromised on the system and work accordingly by not running any programs requesting administrative privileges.

III. Framework Design

This section of the report consists of a detailed description of the proposed framework and the design. The framework consists of three main components, namely memory acquisition, memory analysis and report generation.

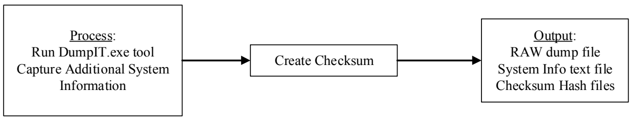

Fig 1. Memory Acquisition Process

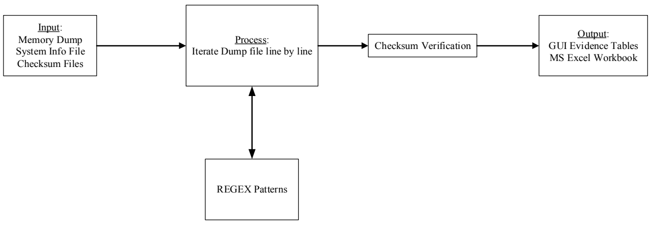

Fig 2. Memory Analysis Process

A. Memory Acquisition

Memory Acquisition is considered as the initial step of the solution proposed. A separate portable tool is implemented for the process of acquiring volatile memory from a workstation based on Windows 10 operating systems. This tool could run from a portable USB storage device and does not have any dependencies. Therefore, the portable tool can be used in any workstation with a USB port. This portable tool runs ‘DumpIT’ by MoonSols, a tool widely used to create memory dumps. Additionally, several other system information such as list of running processes and network details are extracted from the system. Created memory dump and the system information text file is named using the name of the system followed by the acquisition time which gives reference to when the dump is acquired from the system. After successfully acquiring he memory dump, a SHA-512 hash is created for both files and is stored in a .chk file which can be used later to verify the integrity of the data acquired.

B. Memory Analysis

Memory analysis is considered as the key role in the proposed framework. To commence memory analysis the acquired memory dump is needed to be loaded as the primary input. The text file that contains information related to the system and the .chk file generated should also be available in the same directory as the memory dump. Upon completion of the analysis cycle, the evidence retrieved will be organized into several different tables in a tabular format. This would allow the user to easily differentiate and go through the evidence. This process of memory analysis takes place in a sequential manner and the memory dump is read by using a Scanner class which minimizes the usage of memory and allows large files to be read in an effective manner. Sequential reading can be time consuming but it allows larger memory dumps even up to 20GB to be read by the tool. The technique used for building the evidence database is known as String Search, which is used to identify the evidence through pattern matching. Since these data storage patterns are similar in any workstations based in windows 10, they can be used to search for evidence in any given RAW memory dump.

C. Report Generation

The user could export the retrieved evidence into an MS Excel workbook so that it can be submitted to either court of law or any commissions which require digital evidence for their investigation. The MS Excel report generated would be split into different sheets in an equivalent manner to the tabular format within the GUI.

IV. Implementation

As an extensible framework, the ultimate indicator of this tool’s usefulness is the quality of the components that have been integrated into it. The application is developed based on string search as the key method to extract evidence from a volatile memory dump. But memory analysis can be conducted using four methods such as string search, process-object searching, file signature search and file carving.

A. String Search

String Search can be considered as an important method that can be used in volatile memory analysis [3]. Any required information to the investigation can be used as a simple search string to search the memory dump for relevant results. Search patterns are similar patterns of characters that are formed in order to store information in the memory. These characters can be alphabetical, numerical or symbolic or they can even be non-printable characters. For example, one such pattern such as “\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b” can be used to find email addresses in a given dump. This simplifies searching and aids in analyzing large data sources such as memory dumps.

B. Process Object Searching

A process object search refers to the Windows process analysis as stated by [3]. Each process has a ‘EPROCESS’ structure that is associated with it. In the same way, an ‘ETHREAD’ structure is associated with each Windows thread. This technique also can be used for malware analysis in an infectious system [3]. A thread should mostly belong to some process of an application. Therefore, if any threads that do not match with or belong to any process are found, they can be considered suspicious and belonging to a malicious program. [3] also mentions that the size of the structures and values changes depending on the operating system and the version of its service pack. Identifying the exact structure is therefore needed for the process and thread analysis.

C. File Signature Searching

This technique of volatile memory analysis is quite less reliable as stated [1]. There are unique patterns for each file type and these are referred to as the signature. Searching for these signatures in a memory dump can allow the investigator to figure out if such files have been running in the system during the time of memory acquisition.

D. File Carving

File Carving is a technique used in recovering files without file system metadata as stated by [8]. It can be also known as using RAW data to extract structured data files, which is done based on specific characteristics present for each file format [6]. There are three most common general file carving techniques that are used to recover files. One such method is called Header and Footer based carving. This method refers to the recovering of files based on headers and footers that are known to file types. In instances where the footer is not available the maximum known file size is taken into consideration [6]. The starting bytes of each file are identified using the header and the last bytes of the files are identified using the footer and this allows the file start and end location to be identified within the memory dump. The other method of file-carving is the file structure based carving where it is carried out by using the header and footer but also the internal layout including size and identifier strings [6]. For this method, the internal structure of the file should be known. Microsoft Word (.doc), Microsoft PowerPoint (.ppt) and other compound document files, zip files and video files are mostly recovered using this file carving method [9]. The third method is called content based carving and it is based on the content characteristics of files [6]. Such characteristics include; character count, white and black data listing, entropy of information, recognition of text or language and other statistical attributes.

V. Evaluation

The table below shows the comparison between availability of implemented evidence retrieval functionality in other digital forensic tools and the proposed framework. The proposed framework was compared with Volatility framework which is a well-known volatile memory analysis open source tool and Encase Forensic which is an, other commercial tool used widely by forensic investigators.

TABLE I. Comparison of Volatile Memory Analysis Frameworks

Retrieved Evidence Type	Developed Application	Volatility Framework	EnCase Forensic
Google Search History	✓	✗	✗
Facebook Information	✓	✗	✗
Facebook Messenger Chat	✓	✗	✗
Skype Chat	✓	✗	✗
Twitter	✓	✗	✗
Email	✓	✓	✓
Viber (PC)	✓	✗	✗
WhatsApp (PC)	✓	✗	✗
URL s	✓	✓	✓
IPv4 Info	✓	✗	✗
Facebook password	✓	✗	✗
Integrity Verification	✓	✓	✓
Users Logged in Remotely	✓	✓	✗
Users Logged in Locally	✓	✓	✗
Active Processes	✓	✓	✗
Routing Table	✓	✓	✗
Socket and Network Information	✓	✓	✗

VI. Conclusion

An exhaustive research was done to gain knowledge to develop this volatile memory analysis framework. The research mainly concentrated on three key areas such as volatile memory management, volatile memory dump acquisition and retrieval of evidence from volatile memory. As an outcome, it was evident that most of the social media related evidence does get stored temporarily on volatile memory such as RAM for further processing. In cases where volatile memory analysis is possible it is necessary that first respondents collect the dump without losing any data. This will ensure the admissibility of evidence in a court of law, and it will also aid investigators during their investigation process. The proposed framework can be one of the tools the investigator uses to retrieve evidences from volatile memory as part of their digital forensic methodology.

References

[1] Amari, K. (2009). Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. [Online]. Available from: https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049.

[2] Dhanunjaya, V. (2016). Collecting Volatile and Non-volatile Data. [Online]. 2016. Available from: https://www.linkedin.com/pulse/collecting-volatile-non-volatile-data-vuppala-dhanunjaya. [Accessed: 14 October 2016].

[3] Garcia, G.L. (2007). Forensic physical memory analysis: an overview of tools and techniques. [Online]. Helsinki. Available from: http://www.tml.tkk.fi/Publications/C/25/papers/Limongarcia_final.pdf.

[4] Garfinkel, S.L. (2013). Digital Forensics: Modern crime often leaves an electronic trail. Finding and preserving that evidence requires careful methods as well as technical skill. American Scientist. [Online]. 101 (5). p.p. 370. Available from: http://www.americanscientist.org/issues/pub/digital-forensics

[5] Hausknecht, K., Foit, D. & Burić, J. (2015). RAM data significance in digital forensics. 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings. (May). p.pp. 1372–1375.

[6] Kloet, B. (2010). Advanced File Carving. [Online]. (September). p.pp. 1–36. Available from: papers2://publication/uuid/E68694F9-0DB3-4154-B81C-3E9E31642A00.

[7] Narayanan, S. (2015). Emerging Challenges in Digital Forensics. Forensic Magazine. (December). p.pp. 26–27.

[8] Pal, A. & Memon, N. (2009). The evolution of file carving. IEEE Signal Processing Magazine. 26 (2). p.pp. 59–71.

[9] Povar, D. & Bhadran, V.K. (2011). Forensic data carving. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. 53. p.pp. 137–148.