FALI: Time Memory Information of Windows Computer Systems

Funminiyi Olajide
Institute of Criminal Justice Studies
University of Portsmouth
United Kingdom

Richard Trafford
Business School
University of Portsmouth
United Kingdom

Abstract

In today digital investigation, forensic application level information (FALI) has become an important part of digital forensic research. In this research, information stored on Windows computer systems was analysed. The user input gathered from the volatile memory (RAM) of Windows applications has been described as the most important aspect of digital forensic investigation. User input is made at set interval when the application is still opened. This research will report the quantitative assessment of forensically relevant information on Windows application.

1. Introduction

The digital forensic research workshop [1] demand for more tools and techniques to be developed for capturing volatile images and analyzing the memory content of user input on Windows applications**.** As a result, there has been much progress with regards to forensic evidence stored on volatile memory (RAM) of Windows. Little effort has been done on the analysis of the user input recovered from the physical memory contents of Windows application.

A research work of [2], discusses the amount of sensitive evidence that are dispersed in the application memory. Again, limited research work has been made into the formalization of the application level information stored in Windows memory.

Application level information is the extracted user input information from the physical memory content of the most commonly used Windows applications [3]. Application level information can be defined as information which indicates how the user is (or in the case of terminated process, was) using an application.

This research work details a qualitative assessment of evidence stored on some of the commonly used applications. In this experiment, the forensically user input information was extracted and analyzed when the application is still active. Volatile images were captured at set interval hence, the system remains switched on.

The approach of memory imaging and the extraction of forensic application level information (FALI) can be useful during digital investigation of cyber fraud on digital devices. This information can be presented as evidence in the court of law. It is essential that forensic investigator determines the quantity of user input information stored on volatile memory (RAM) of an application.

Forensic application level information (FALI) can be used for information assurance when investigating computer crime or any related cybercrime issues that are committed using digital devices. Investigation into this computer-based systems fraud can reveal user actions. These actions will reveal the quantity of user input, the events of activities on this application. For the purpose of this research some commonly used Windows applications was identified.

The extracted forensic application level information (FALI) from the volatile memory of an application was investigated to reveals various user's actions. The stage of investigations relies on investigator's skills and experience. The approach taken is pertinent towards the demand of digital forensic community research and the trends of cybercrime issues all around the world.

2. Related work

A research of [4] focused on memory acquisition. This is a command line tool that captures and reconstructs the virtual address space of the system process and other processes. The research method in [5] presented the hardware-based memory acquisition. This approach change memory contents as little as possible by using a PCI extension card to dump the memory content to an external device.

A method of [6] laid emphasis on the importance of forensic live response and event reconstruction methods. The extension of this research work in [7] focused on the application level evidence**.** This approach identified the important aspects of memory analysis and proposed an approach for the volatile memory analysis.

There are open source software-based tools that have been developed recently for memory acquisition and for memory analysis. A method of [8] is a tool that is capable of revealing hidden and terminated processes and threads whereas, Nigilant32 [9] are tools that can capture the physical memory contents of computer systems.

In recent time Win32dd and Win64dd [10,4] have also been used to capture memory and perform memory analysis. In addition, MemParser [11] and the Volatility Framework [12] are examples of other tools that can perform full memory analysis on Windows application. Of these two, the Volatility Framework is more extensive.

This tool is capable of performing the analysis on a variety of memory image formats such as DD format, crash dump and Hibernate Dumps. Volatility is able to list OS kernel modules, drivers, open network socket, loaded DLL modules, heaps, stacks and open files.

The research work of [13] addresses the need for more sophisticated tools on physical memory acquisition and analysis. This is data carving method of research that can be used for a recovery purpose. This approach is frequently used during digital investigations. A paper [14], identified the most commonly used application. This approach provides prospective evidence regarding the application of memory analysis on Windows computer systems.

Moreover, it is essential that a new development tools should be integrated on other different approaches. Therefore, a research model of [15], presented the graphics extraction that is contained in a memory dump.

3. Approach taken

A normal working environment was replicated for capturing volatile memory images. As shown in Table 1, the computer would be turned on at the start of the day and then turned off at the end of the day. When the computer is first turned on, the applications will be opened and the user will interact with the applications and images will be captured at set interval of 30 minutes. Series of tests will be carried out for days until 100 images were captured on each application.

The physical memory in the computer was 2 Gigabytes (GB) and this resulted in 200 GB of images captured. After volatile imaging, copies of the images captured were made for preservation purposes.

The aim of this research is to determine how a user is interacting with the computer systems when user input were made on these applications. This process will identify how user is using the application while reconstructing the event of user input stored on the memory allocated to these applications when the computer is still switched on.

In this experiment, the volatile memory content of FALI was investigated and it was discovered that the extracted evidence that was stored in the volatile memory are dispersed. By pattern searching techniques that was developed, relevant user input of FALI was extracted and converted into strings. User input of FALI was searched through the application memory and the extracted FALI evidence was matched with the original user input.

The pattern searching techniques was developed using the system composition program like python. In this case, an automated executable program was used to perform pattern matching of memdump strings of the extracted FALI. This information was used to search for memory evidence.

Table 1. Approach

Application	User Input (Open Application)
Outlook Email	Write a note of texts with commas, semi-colon, brackets, full stop. User input may contain or type alphanumeric, character 0-9, brackets close or open. . Long sentences or short sentences. Send and receive emails or do nothing. Save document or do not save.

Evidence of FALI was reconstructed based on what the user was doing on the application, what the user has been doing and what the user was using the application for. This approach reveals sensitive information of FALI.

4. Quantitative assessment

In this section, the quantitative assessment of FALI data from the volatile memory content of Outlook Email 2007 was analysed. The investigation identified the mean percentage of FALI evidence stored in the application memory. Table 2 describe the percentage amount of user input found in the Outlook Email memory.

The mean percentage of evidence found shows how much of the original user input in the memory dump that was extracted from Windows computer systems.

Table 2. Quantitative assessment

Sample Application	Mean % of Evidence found
Outlook Email	98

Large amount of evidence was extracted from Outlook Email. This series of experiment was run for days. As investigated, it was discovered that the forensically relevant data was stored in the volatile memory. This evidence information was reconstructed to ascertain the quantity of FALI based on what the user was doing on the application.

Further investigation on what the user has been doing on the application and what the user was using the application for was also investigated and analysed. However, all the FALI information were recovered and analysed as stored over time in the application memory. There is 98% of forensic evidence found in the memory. In this experiment, the FALI contained only the data text of paragraphs and alphanumeric characters with bracket, semi-colon, full stop, question mark and

currency sign. All the relevant evidence of FALI was recoverable by the pattern searching technique. This information may be useful to forensic investigators when determining the user input made on this application.

As shown in Table 2, this finding is interesting because the percentage amount of forensically relevant evidence that was stored over time in the memory of Outlook Email application was revealed.

The percentage amount found was calculated, being the amount of relevant data. This information indicated that there are more relevant data of FALI that was stored in the memory for a longer period of time in the application memory. This information can be described as the original and actual text data of user input made on this application.

Moreover, it was found out that the percentage amount of FALI information resided in the application memory can be useful to determine the various user input activities on Windows computer systems. This information may be useful to forensic investigators in digital investigation.

5. Analysis

This research uncovers the amount of data that can be stored in the memory based on the series of experiments carried out. As investigated, Outlook Email, contain large amount of evidence that was found stored in the memory. This is only possible based on the user input specific to data texts of relevant information extracted from FALI. The series of experiment carried out have helped to determine the percentage of evidence stored over time in the memory of the application.

Large amount of data was recovered because the user's input contains only the data texts strings. This research is in line with the long term of evidence preservation and the investigations carried out, uncovers the amount of evidence data stored over time in the memory. The purpose of this research experiments is to found out the forensically relevant data of FALI on volatile memory based on what the user is typing, what the user has been doing and what the user was using the application for. This information may be useful to forensic investigators while determining the integrity, completeness and authenticity of evidence stored in the volatile memory of this application.

As a practice in memory analysis, evidence is often saved in the memory for later use in the belief that it can be accessed anytime in the future. It is evident that this research of FALI uncovers the amount of evidence stored over time in the memory application of Windows computer systems.

6. Conclusion

In this research, the quantitative assessment of user input was discussed based on a model of FALI extracted from the Windows computer systems. The quantity amount and the analysis of FALI evidence was achieved based on what the user is typing, what the user has been doing and what the user was using the application for. One of the most commonly used Windows applications was investigated. Specific research experiment has been performed. Emphasis was laid based on the mean percentage of information that was calculated for FALI evidence as stored on the application memory.

This model has been used to describe the process of securing digital evidence and analysing the forensically relevant data. This research will be useful to support evidence on computer crimes or fraud investigation in the court of law. This experiment involves memory dumping, extraction of relevant data and strings conversion of evidence. This also includes the searching and finding the percentage descriptions of relevant FALI evidence on the application memory, when user input information and images were captured at set interval. Validation process of FALI evidence was achieved for presentation purposes in the court of law. This approach has become part of forensic analysis in digital forensic investigation of FALI.

7. Future work

In the future, digital investigation of FALI based on other most commonly used application will be investigated and analyzed.

8. References

[1] Digital Forensic Research Workshop, DFRWS. (2007) http://www.dfrws.org/2007/challenge/index.shtml. [Online].

[2] F. Olajide. N. Savage, "Dispersal of Time Sensitive Evidence in Windows Physical Memory C, , June 2011.," in *yberforensics, International Conference on Cybercrime, Security & Digital Forensic*, The University of Strathclyde, Glasgow, UK, 2011, p. 27–29.

[3] F.Olajide, "A Study of Application Level Information From The Volatile Memory of Windows Computer Systemns ," PhD Thesis, University of Portsmouth, Portsmouth, UK, 2011.

[4] Msuiche. (Accessed 2008) Msuiche.net at:, [Online]. http://www.msuiche.net/2008/06/14/capture-memory-under-win2k3-orvista-with-win32dd.

[5] G. L. Garcia, "Forensic Physical Memory Analysis: an overview of tools and techniques," in TKK T-110.5290 Seminar on Network Security, Helsinki, Finland, 2007.

[6] F. Olajide. N. Savage, "Forensic Live Response and Events Reconstruction Methods in Linux Systems," in PGNET The Convergence of Telecommunications Networking and Broadcasting, Liverpool, Dec. 2009, pp. 141-147.

[7] F. Olajide. N. Savage, "Application Level Evidence From Volatile Memory," Journal of Computing in Systems and Engineering, vol. II, no. 3, pp. 40-48, Jan. 2010.

[8] ManTech. Memory. (2010) Memory dd. [Online]. http://www.mantech.com/msma/MDD.asp

[9] Nigilant32, Agile Risk Management. (2006.) Agile . [Online]. http://agilerm.net/publications.4.html

[10] F. Cohen, "Challenges to digital forensic evidence.," in Cybercrime Summit 06. Retrieved from: http://all.net/Talks, Washington, 2006.

[11] C. Betz, "Mempaser analysis tool.," in DFRWS 2005 Forensic Challenge: http://www.dfrws.org/2005/challenge/memparser.shtml, MA, 2005, pp. 100-115.

[12] Volatile. Systems. (2009) The Volatility framework: volatlile

mwmory artifact extraction utility framework. . [Online]. http://www.volatilesystems.com/default/volatility

[13] D. Kleiman H. Carvey, "Windows Forensic Analysis Incident Response and Cybercrime Investigation Secrets," 1st ed. Syngress Publishing; , Jul. 2007.

[14] F. Olajide. N. Savage, "On the extraction of forensically relevant information from physical memory," in World Congress on Internet Security (WORLDCIS-2011), Technically Co-Sponsored by IEEE UK/RI Computer Chapter, London, 2011.

[15] T. Hoppe, J. Dittmann. S. Kiltz, "A New Forensic Model and ITS Application To The Collection, Extraction And Long Term OF Screen Content OFF A Memory Dump," in 16th International Conference on Digital Signal Processing (DSP), Aegean island of Santorini, Greece, 2009.

