Forensic Memory Evidence of Windows Application

Funminiyi Olajide,
School of Engineering,
University of Portsmouth,
United Kingdom
funminiyi.olajide@port.ac.uk

Nick Savage,
School of Engineering,
University of Portsmouth,
United Kingdom
nick.savage@port.ac.uk

Galyna Akmayeva,
Infonomic Society,
Republic of Ireland
g.akmayeva@ ieee.org

Richard Trafford,
Business School,
University of Portsmouth,
United Kingdom
richard.trafford@port.ac.uk

Abstract- **In modern digital investigations, forensic sensitive information can be gathered from the physical memory of computer systems. Digital forensic community feels the urge towards accurate data collection, preservation, examination, validation, data analysis and presentation. This investigative process has become an essential part of digital investigation. The extraction of forensically relevant evidence from the physical memory can reveals users' actions. This research will report the amount of evidence that can be extracted and how the evidence changes with the length of time that the system is switched on and the application is still opened. In this experiment, the quantitative assessment of user input on the most commonly used applications will be presented.**

Keywords-Application; time; memory;Windows

I. INTRODUCTION

Digital forensic investigation techniques have focused mostly on evidence contained within hard disks; little has been done on the volatile memory analysis of Windows application. But, recently, there has been a great demand for more tools and techniques to be developed for capturing memory images and analyzing their content [1]**.** In recent time, there has been much progress with regards to forensic evidence gathering, however, little has been done on the research investigation and the analysis of the acquired evidence from RAM of the computer systems. A research work of [2], focused on the dispersal element of sensitive evidence in the memory but, limited efforts have been made into formalizing the forensic time evidence of application level information of Windows application. Application level information is the extracted user input information from the physical memory of the most commonly used Windows applications [3]. Application level information is defined as information which indicates how the user is (or in the case of terminated process, was) using an application.

This research work details the quantitative assessment of the amount of evidence stored on the application memory and how that evidence changes over time while the system remains switched on and images were captured at set interval. The method of capturing memory and the extraction of forensically relevant data will facilitate the investigation of user input stored over time in the physical memory of the applications. These actions will also reveals how user input activities can be recovered and how the forensic time memory evidence of user input can be used to support other related evidence of crime or fraud on computer systems. In this research, some commonly used Windows applications will be identified. The extracted relevant evidence from the physical memory of these applications will be investigated based on various user input activities. The research idea is motivated on the fact that physical memory contents contain information that cannot be found on traditional hard disk forensic investigations. Research investigation into different user input on application and the extraction of forensically relevant evidence relies on the investigator's skill and experience. This approach is essential in determining what information is pertinent and useful to support the crime or fraud cases at hand. The investigators are determined to find out the exact likelihood of users action at particular moment of event, to actualize the cause of the incident. This process of investigations can help the investigators to carry out the analysis of time evidence found in the physical memory of the application. This approach can provide additional relevant evidence when forensically investigating and validating the user input activities on the computer system.

II. RELATED WORK

Digital forensics has become an indispensable tool for information assurance as well as solving crime and tracing fraud, where evidence may reside on a computer system. A method of [4] laid emphasis on the importance of forensic live response and event reconstruction methods. The extension of this work relies on the research of application level evidence from physical memory [5]**.** This approach identified the important aspects of memory analysis and proposed an approach for application level evidence from volatile memory. The method presented in [6] is among the few hardware-based memory acquisition methods that change memory contents as little as possible by using a PCI extension card to dump the memory content to an external device. A range of software-based tools have been recently developed for memory acquisition and memory analysis. A research of [7] focused on memory acquisition, a command line tool that captures and reconstructs the virtual address space of the system process and other processes. A method of [8] is a tool that is capable of revealing hidden and terminated processes and threads whereas, Win32dd or Win64dd [9,7] and Nigilant32 [10]

978-1-908320-08/7/$25.00©2012 IEEE

are tools that can capture the physical memory of computer systems. In addition to these tools, MemParser [11] and the Volatility Framework [12] are examples of other tools that can perform memory analysis. 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 which is a recovery approach that is frequently used during digital investigations. Moreover, it is essential that a new development tools should integrate different approaches. A new model of [14], point towards the graphics extraction that is contained in a memory dump. A recently published paper [15], identified the seven most commonly used application and the aspects of memory analysis on the basis of how much information can be recovered from the memory content of the application. This approach provides prospective evidence regarding the application of time memory analysis.

III. INVESTIGATION PROCESS

A research paper of [15], identified the most commonly used applications. This research work focused on two of the applications, to investigate the forensic time evidence of user input. In order to make our results as applicable as possible we tried to replicate a normal working environment while capturing memory images. As shown in Table, 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 two 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 was run for days until 100 images were captured on each application. The physical memory of the computer was 2 Gigabytes (GB) and this resulted in 200 GB of images being 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 input were made on these applications. This process will identify how the user is using the application over time, when the computer is still switched on.

TABLE I. APPROACH

Applications	User Actions (Open Application)
Excel 2007	List a set of numbers and some data texts, or texts of paragraph only. Draw a graph of the numbers and texts. Input may contain alphanumeric, character 0-9, brackets. Save document
PowerPoint 2007	Write a slide, slides 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. Save document.

The memory content of the applications was investigated and it was discovered that the extracted evidence was stored as dispersed in the physical memory. The initial user input was determined and the time aspect of the information was recorded following the pattern searching techniques that was developed to search through the application memory and then locate where this evidence resided. The pattern searching techniques was developed using a system composition program like python. In this case, an automated executable program was used to perform pattern matching of memdump strings of the applications and to search for memory evidence. As the initial user input was determined, pattern matching techniques was used to find out the forensically relevant evidence of user input on each application. The extracted evidence reveals what the user was doing on the application, what the user has been doing and what the user was using the application. The temporal analysis of user input can be useful to forensic investigators to uncover how sensitive information is stored over time in the memory. This approach can lead to further investigation, while analyzing the user input on the basis of other forensic questions of who, how, when and where.

IV. QUANTITATIVE ASSESSMENT

In this section, the quantitative assessment of forensically relevant data from the physical memory content of Excel 2007and PowerPoint was analysed. The investigation identified how evidence was stored over time in the physical memory of these applications. Table II describe the percentage amount of user input found in the memory allocated to these applications. The mean percentage of evidence found shows how much of the original user input has been identified in the memory dump that was extracted.

TABLE II. QUANTITATIVE ASSESSMENT

Sample Application	Mean % of Evidence found
Excel	44
PowerPoint	96

Large amount of evidence was stored over time on PowerPoint applications. This series of experiment was run for days and as investigated, it was discovered that the forensically relevant was stored as dispersed in the physical memory. It can be said that the evidence found can be reconstructed for evidential purposes based on user action on this application. This relevant information can be led to further investigations of user input on the basis of forensic questions of who, how, when, where and why. However, all the user input information was recovered as stored over time in the application memory. There is 96% of forensic evidence found in the memory. In this experiment, the user data input contained only the data text of paragraphs and alphanumeric characters with bracket, semi-colon, full stop, question mark and currency sign. It was evident that large percentage amount of evidence was found and as stored over time in the memory content of

this application. In some cases, all the relevant evidence of user input was recoverable by the pattern searching technique. This information may be useful to forensic investigators when determining the user input made on this application, and how the amount of user input stored over time in the physical memory. On excel application, it was found out that least amount of relevant user input can be recovered over time from the memory. The percentage amount of evidence found in Excel was 44% as calculated. This is because it was very difficult to reconstruct the numeric format of information stored on Excel application. The forensic evidence found on Excel, scattered throughout the extracted memory. The user input was traced mostly to be the numeric data entered by the user but there are more of the numeric system in-built defined data that was found. In some other experiments, it was discovered that user input contains only the text data while in some days, it was just the numerical data that was entered on Excel application. In the series of experiments that was carried out, it was discovered that all of text data of user input can be recovered over time as it was assessed, whereas the extraction of numeric data was very difficult as was found scattered in the physical memory.

As shown in Table II, this finding is interesting because the percentage amount of forensically relevant evidence that was stored over time in the memory of Excel application was revealed. The percentage amount found was calculated, being the least amount of relevant data, when compared to the percentage amount of user input recovered from other application like PowerPoint. This is because there are more numeric system defined data that was found on the memory. This information indicated that there are more numerical data that was stored in the memory than the actual text data of user input made on this application.

Moreover, it was found out that the time aspect of evidence stored by an application is useful to determine the amount of information recovered. This information may be useful to forensic investigators in digital investigation.

V. 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, only in Excel application that the least amount of data stored over time, as it was recorded. However, the least amount of data recovered was only on the numeric data type while in other experiment for example, in PowerPoint, large amount of evidence was found stored in the memory. This is only possible on the user data input specific to data texts. The series of experiment carried out have helped to determine the percentage of evidence stored over time in the memory of the application. For example in PowerPoint applications, large amount of data was recovered only because the user's data input were data texts strings whereas, least amount of user input was recovered from Excel application memory because more of numeric data was found to be part of the system defined data, that is, the in-built system defined information that are resided in the memory of Excel application. Further investigation revealed that the amount of user input found on Excel application have the least percentage of evidence even when the user input made on this application contains the mixtures of data texts, numeric data, graphs and tables. In this perspective, it can be said that both the text strings and numeric information can be traced, but the percentage amount of user input stored over time may differs. This information may be useful to forensic investigators, from the perspective of forensically relevant data that was found in the memory content of Excel application. 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 on physical memory and how the evidence is dispersed over time. Consequently, data evidence gained in each application is relevant towards what the user is doing, what they have been doing and what they have been using the application for. This information may be useful to forensic investigators while determining the integrity, completeness and authenticity of evidence stored in the physical memory of applications.

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. This research uncovers the amount of evidence stored over time in the memory.

VI. CONCLUSION

In this research, the quantitative assessment of user input was discussed based on a model of how much relevant data can be recovered, and as stored over time in the physical memory of the two most commonly used Windows applications. Specifically, we have laid emphasis on the amount of data evidence stored on each application. This model has been used to describe the process of securing digital evidence and analysing the forensically relevant data, to support the case at hand, as related to computer crimes or fraud investigation. This experiment involves memory dumping, extraction of relevant data and strings conversion of evidence. This also include the searching and finding the percentage description of relevant evidence of user input on the application memory, when images were captured at set interval and the validation process for data presentation in the court of law. This approach has become part of forensic analysis in digital investigation. The quantitative assessment of evidence found reveals the key questions of forensic based on what the user was doing on the application, what the user has been doing and what the user has been using the application for.

VII. FUTURE WORK

In the future, forensic investigation and more practical experiments on these applications will be performed and the qualitative assessment of user input activities will be fully explored.

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] 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.

[5] 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.

[6] 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.

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

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

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

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

[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] 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.

[15] 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.