Indian Journal of Science and Technology, Vol 9(25), DOI: 10.17485/ijst/2016/v9i25/95211, July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Forensic Investigation and Analysis of User Input Information in Business Application

Funminiyi Olajide* and Sanjay Misra

Department of Computer and Information Sciences, Covenant University, Ota, Nigeria;
funminiyi.olajide@cu.edu.ng, sanjay.misra@covenantuniversity.edu.ng

Abstract

Objectives: This paper investigates the amount of user input that can be recovered from the volatile memory of Windows computer systems while an application is still running. Additionally, an investigation into temporal, functional analysis and event reconstruction of user input activities in business application is discussed and reported upon. **Methods/Analysis**: Forensically, relevant user information is suitable for an evidentiary purpose. Therefore, the qualitative assessment of user input on commonly used windows-based applications is presented. **Findings**: In this research, detailed emphasis has been laid on the quality of evidence recovered from the allocated line numbers of the application memory. This approach describes the process of securing digital evidence for investigators. The research uncovers the process of analysing the forensically relevant data recovered from Windows applications. The investigation comprises of the following; dumping of memory, data extraction, strings evidence strings conversion, result finding of the evidence and also, reconstructing the extracted evidence of user information. **Applications/Improvement**: This research focuses on digital forensic investigation of digital images captured and the memory analysis of user information on using some very popular windows-based applications. It is aimed that this may become part of forensic analysis in digital investigations.

Keywords: Application, Forensic, Fraud Information, Investigation, User-Input

1. Introduction

In today's digital world, the use of information devices has been very popular and active amongst users. ICT performance and capacity on a computer is determined by settings based on date-time-stamp information and this is vital in digital evidence analysis[1]. It can be said that when an application is running from a particular location for the very first time, Windows creates a prefetch file. However, for Investigation purposes, this file contains some valuable information on users as they interacts with business application to determine history on computer systems. Prefetch files can speed up the loading of applications as evidence of program execution can be valuable resources for forensic investigators. The information contain in the history can prove user input specific information or ran a particular program to cover up any potential wrongdoing. For example, if any user input information on a business application has been deleted or cleaned up for an intended purposes, a prefetch file of such information may still exist on the computer system to provide evidence of program execution. This paper uncovers a commonly used business application that was investigated to determine and analyse user input activities such as what the user is typing on the application. Further investigation was achieved by combining some basic timeline analysis to assist the investigation, resulting in the identification of additional information on user activity on Windows application. With the additional information, the root cause of an incident on user input information on this commonly used business application was revealed.

However, necessary tools and techniques are required to capture digital image of an incident on business application for forensic investigation. Recently, the in the digital forensic research community, there have been calls for additional tools and techniques to help capture mem-

*Author for correspondence

ory images and analyse the memory content of the user information[2]. Recently, much progress is being made in respect of forensic evidence gathering from volatile memory for Windows, Mac, Linux and UNIX systems.

In time past, digital investigation concentrated mostly on evidence obtained hard disks. However, only little research has been carried out on the analysis of the acquired evidence of user information from the volatile memory of Windows applications. According to[3], digital Forensics is described as a branch of forensic science that is concerned with legal evidence found on computer systems and other digital storage media[4]. During the investigation, investigators require acquisition of digital evidence from business application in computers, laptops, USB, and other electronic digital devices. While analysing the digital evidence, the memory content of an application can record accurate time of when information is hidden but if not properly preserved, user input information may be deleted or wipe off. A research paper of[5] provided vital information on tools to use as well as steps to take in acquiring and analyzing data from the volatile memory of Android Smartphones and revealed important process to gain root privileges to execute forensically relevant information[6].

There are lot of research goals to generate specific user information on business application and for forensic investigators; certain methods must be adopted to uncover user intended purposes on this application. Digital forensic using two steps inject methods by[3] discusses advantages of this methods in a way that system working in secret to prevent the loss of digital evidence by suspects or third party. A paper of[5] moved a step forward on the forensic examination and analysis of the prefectch files on specific cybercrime issues, a Trojan malware incident on banking application. This papers shows how the prefectch files contain valuable evidential data which covers forensic questions of how, what and when the banking Trojan malware can infects the system and gives answers on Prefetch files of data remnants of the malware incidents.

In[4], discussed the quantity of sensitive evidence that was dispersed in the application memory. It was discovered that little has been achieved in respect of using the time aspect of application level information stored in windows-based application memory. But, the forensic approach of investigating Windows computing devices includes mobile technology for memory imaging, memory dumping and the extraction of forensically relevant data can be useful during digital investigations. The forensic investigator can determine the date-time-stamp of user activities on the basis of the quality of information stored in applications. This information can be recovered as stored on the volatile memory of Windows application. Event reconstruction of user input can then be performed. This process of reconstructing the event of user input can reveal certain amount of relevant information which can be validated and used as evidence against perpetrators. Information about how a user is using an application is referred to as application level information. This research work focused on qualitative assessment of user information stored on the application memory and how that evidence can be reconstructed to determine the memory aspect of relevant information stored on Windows application[7].

This research reveals temporal, functional analysis of user input when the computer system remains switched on. By reconstructing the event of user information while the application is remains open with images captured at intervals for relational analysis of user input. This forensically relevant information can be used to determine the input of a user, who the user is, when the user last accessed the application and what the user has been doing on the application while interacting with the application. Thus, the memory analysis of this information can uncover forensically relevant information for investigators. This evidence can provide information assurance for the audit trail analysis of user information, as well as the related system log file that was useful when investigating the malicious code of cybercrime attacks[8]. Related evidence of user actions can be found while tracing fraud on computer-based systems or digital mobile devices, such as the new emerging mobile technology.

Some commonly used Windows applications were used for this research. The user information was extracted from the volatile memory of the windows-based applications. Techniques adopted as described in[9], facilitated the investigation and analysis of user input activities on business applications on Windows-based computer systems. This research is built upon this technique and with combination of prefetch files that contain history of the computer systems where the user input information of the application was stored. The research reveal a forensically relevant data of user input on a commonly business application. Recovered user input information uncovers details of all user activities on the application.

Memory forensics is the forensic acquisition and analysis of volatile data in system Random Access Memory (RAM). In[10] examined the forensic resilience of simple memory acquisition techniques by testing current commercial and free open source tools. The memory acquisition techniques did not however, rely on operating system facilities but were based on direct manipulation of page table as well as PCI hardware. The research concentrates more on information systems analysis of data and cyber warfare principles based on the perception of South African usage of internet and the effect of cybercrime on business. But for example, in the UK, cyber fraud costs small firms £22bn a year[11] and therefore, memory imaging analysis is of significant research interest in digital forensics. A paper on forensically robust method for acquisition of iCloud data in[12] was reviewed to determine effective means of original file data and metadata. Further investigation is required to determine if the original harsh file and file metadata with data-time-stamps are altered[13]. Schuster in[14], indicated that there has been much attention to the acquisition of physical memory and stated that the information contained in Windows operating systems is vast. This includes physical memory address spaces for processes (both user and kernel processes), cached file system blocks and free pages that are not currently allocated to any process[15]. Kurt Oestreicher in[12] investigated on iCloud data with relevant evidence of extracted information from physical memory of an application. Memory evidence recovered can be used to support forensically relevant evidence in the court. For example, in cybercrime investigations the investigators are required to find out the exact likelihood of users actions. This information can be reconstructed to further investigate the various events of user input within the applications. In addition, a priori knowledge of user information was used to determine the causes of cybercrime based on user input information on business application. But, for evidence to be acceptable in the court of law, the evidence must be tested and forensically sound. Also, the evidence must be validated to be accepted for presentation and can be used for evidential purposes against perpetrators in a court of law

Volatile memory analysis is an important field in computer forensics investigation and a paper of[16] presented ranking algorithms for digital forensic string search hits that contained therein, the relevancy string search output queries in digital forensics. This research is similar to the web browsing application using a valuable analytical technique of text string searching[17]. Textual evidence is regarded as important in digital forensic investigation on a common fact of user input activities on application like PowerPoint application, which is one of the most commonly used Windows business application. According to[11], evidence extraction must be validated to be accepted for presentation and may be used as evidential purposes against perpetrators in the court[18]. In[18], pointed out that there a lot of work that has been done on the analysis aspect of memory forensics but the acquisition and image generation process of cyber fraud in business application is still at its infancy. In particular, the quality and quantity of information recovered from Windows mobile application has not been adequately assessed[5]. Whereas, the research of[9], investigated the type of repeated evidence stored on the application memory as well as the percentage of evidence found on the application when the computer systems is actively running and the user is still interacting with the application.

In[19], presented a paper on the extracted hidden messages in steganographic images, exposing an inherent vulnerability in the embedded algorithms of actual message. This approach revealed the message bits and the research works by finding modified pixels or residuals as an artefact of the embedding process. In[17] emphasised the importance of forensic live response and event reconstruction methods. The authors in[20] further extended this work by focusing on the application level evidence.

In[13], presented a hardware-based memory acquisition technique which described how data changes over time in the memory contents of an application[9]. In[2], addressed the importance of more tools such data carving, for use in physical memory acquisition and analysis. Moreover, it is essential that new development tools be integrated into different approaches[22] of forensic investigation. The Volatility Framework is more extensive[12].

Memory analysis of Windows systems provides a means of examining the system artefact during malware analysis. In[20], analysis of memory images to determine the rootkit hook and code of the operating system was carried out while[15] broadly discussed the forensic process in terms of availability and usefulness of evidence. Therefore, modern tools for the extraction of user input information are capable of detecting rootkits and other malware infecting the host as well as analysing the malicious software that can infect the Windows application. In[23], gave an indication of the analytical capability of memory imaging, memory dumping and the extraction of forensically relevant data that can be useful during a

digital investigation. In[9] presented paper that the forensic investigator can determine the quality of information stored with date-time-stamp of user activities as stored and recovered from volatile memory of Windows applications. In[19] discussed on the native actors of how to scale network forensic and a VAST technique was designed by presenting a distributed database to support interactive network forensics of VAST, the Visibility Across Space and Time[16]. This technique enhances forensic investigations in the memory analysis of voluminous data associated with incidents investigations.

2. Forensic Investigation Approach

To investigate the forensic user input information on business application, a time memory aspect of user input on Windows applications is determined. Table 1 shows that the computer would be turned on and off in a given working day in a business organization.

The computer was first switched on, followed by the application to be used by the user. As the user interacts with the application, user information is captured based on set time intervals. Several tests were carried out for several days until big data analytical images were captured on the application. Upon completion of the volatile imaging, copies of the captured images were made in order to preserve them. The memory dump of the extracted user input information was reconstructed using pattern searching techniques, and Natural Language Processing. An example of the algorithm used for the extraction of user input activities is shown in the Table 2. The recovered user input information reported exactly what user has been doing on the application. The information found was dispersed throughout the allocated memory of these applications. In this experiment, the methodology approach of user input information was reconstructed using some commonly used English word.

This research work determines how a user interacts with a computer application by analysing the user input and activity. This process identifies how the user interacts with the application and what the user has been doing by reconstructing the user input events. This is achieved by carrying out analysis of the memory allocated to each of the applications while the system remained on. It was discovered upon investigation of the memory content of the applications, that the acquired evidence stored in the physical memory is dispersed. Using pattern searching techniques, user information was extracted and converted into strings. The forensic investigation approach on a sample Power Point application, include a user opening the application to create a slide of texts with commas, semi-colon, brackets and full stop. This user input contained alphanumeric characters including the brackets.

Table1. Algorithm summary of experiment on windows computer system

Algorithm Summary of experiment on Windows Computer Systems	Stages of Experiment	
	1.	Experiment focused on Windows 7 systems was switched on
	2.	A typical day-to-day business environment was demonstrated on user input information was repeated on two most commonly used business applications on the Windows Computer Systems
	3.	Various user input actions that were made on each of the application at set period of time

Table 2. Algorithm summary of automated program for evidence extraction

Algorithm Summary of automated program for the memdump extraction of Evidence	Stages of Experiment for the Evidence Extraction	
	1.	Run automated program written in python to dump memory
	2.	Run automated program written in python to extract strings processes for evidence searching
	3.	Run automated program written in python for pattern evidence matching using some commonly used English words
	4	Run automated executable code to construct a database the results.

The system composition program which is similar to python was used to develop pattern searching techniques on the memdump strings of the applications. The evidence was reconstructed to determine the time memory aspect of the forensically relevant data, based on the activity of the user. This approach can reveal the sensitive information pertinent to user activities on the application memory. By reconstructing this evidence, this approach can lead to further investigation, when forensic investigators are analysing the user input on the basis of other forensic questions of why, who, how, when and where the user input are stored in the memory.

3. Qualitative Result and Assessment

This section presents the qualitative assessment of data obtained from the physical memory of a Power Point application that is relevant for forensics purpose. This investigation describes how evidence was stored gradually in the volatile memory of the applications. As can be seen from Figure 1, the evidence stored in memory appeared dispersed. The line number was allocated to the evidence found on this application, and as extracted from the physical memory.

In some instances, there exists occurrences of consistent repetition of evidences varying locations in memory and this can be traced with the line numbers allocated. The extracted memdump strings of user input on these applications have been reconstructed for evidential purposes. There are partial fragments of the evidence and also, in some cases, whole fragments of evidence were discovered in continuous blocks of the application memory. Figure 1, describes the reconstructed application level information from the PowerPoint applications. In this experiment, the case was reversible; because the user input stored on this application was found dispersed more in whole fragments than the partial evidence information that was recovered. Although, the relevant evidence was extracted from the memdump strings, and more of the evidence information was recovered in continuous blocks of the application memory. Moreover, the evidence information that was dispersed in the memory content of this application can be reconstructed as partial or whole fragment of user input.

By reconstructing the user input extracted from Power Point Application more evidence information was revealed, for example, the partial fragment of information was found stored in line number "4010" and also, in line number "4049". While reconstructing the two line numbers, revealed that the evidence stored in line number "7899" can be termed as the whole fragment of user input found in continuous block of evidence. This information represents the full sentence of forensically relevant data with full stops and commas. However, the partial fragment of evidence information was found stored in line numbers "4010", "4049", "4050", "4051", "4052", and "4053" respectively.

As shown in Figure 1, the user input evidence can be reconstructed to determine the user activity. As illustrated in the figure above, this research experiment clarifies the important aspect of user input activities on some commonly used Windows applications.

PowerPoint Application - Evidence Extracted From MEMDUMP STRINGS
Partial Fragment with Line Numbers / Whole Fragment with Line Numbers.
[Reconstructing by Pattern matching Evidence]

```
4010
Inter are unmoved by Roman intrigue  ANY
Manchester United fans crying foul at Chelsea
4049
s 2-0 win at deadly rivals Liverpool on Sunday
should spare a thought for Serie A title chasers
Roma. Inter Milan were forced to play down the
controversy which followed their win over Lazio
in the Italian capital on Sunday. The 2-0
victory saw then establish a tow point lead at
the top of Serie A
4050
at the expense of Lazio
4051
s city rivals Roma.
4052
Inter are unmoved by Roman intrigue
4053
ANY Manchester United fans crying foul at
Chelsea
7899
Inter are unmoved by Roman intrigue, Manchester
United fans crying foul at Chelsea's 2-0 win at
deadly rivals Liverpool on Sunday should spare a
thought for Serie A title chasers Roma. Inter
Milan were forced to play down the controversy
which followed their win over Lazio in the
Italian capital on Sunday. The 2-0 victory saw
then establish a tow point lead at the top of
Serie A at the expense of Lazio.
```

Figure 1. The reconstructed evidence of powerpoint application.

4. Result Analysis

The purpose of this experiment was to determine what data in the physical memory will be relevant for forensic purpose and how this evidence can be assessed based on the quality of user input that has been reconstructed. Images were captured at some set time intervals. Pattern matching technique was used to investigate the user input. This information is crucial to forensic investigators and can be used to augment the qualitative assessment of user input stored over time in the physical memory. The evidence recovered can be used for forensic analysis purposes.

Also, the extracted user input can be reconstructed to further investigate other forensic questions of what, who, when, where and how. For example, the question of *"what"* the user was doing on the application, can be traced to different allocated numbers of the reconstructed evidence in Figure 1. Also, the questions of "*who*" can be described as the identity of the user that entered information on this application. The questions of *"where"* can be termed as where user input was made. In this experiment, it can be said that the user input was made on Power Point applications and as extracted for event reconstruction purposes. This is the application that the user was using to input data. It can be said that the question *of "when"* can be answered during the investigation of process listings and scanning of the applications while using the Volatility tools. The question of *"how"* can be answered based on the way the user input information was stored partially and in whole fragment of information on this application. Therefore, it can be said that the user input found on the allocated memory of the application was dispersed and as stored over time with the allocated line numbers.

5. Conclusion

This research work considered the qualitative assessment of user input incommonly used Windows-based applications. Detailed emphasis has been laid on the quality of evidence recovered from the allocated line numbers of the application memory. This approach describes the process of securing digital evidence for investigators. The research uncovers the process of analysing the forensically relevant data recovered from Windows applications. The focus of this work is finding and reconstructing user information at the application level. The process involves memory dumping, extraction of relevant data as well as string conversion. This approach may be included as part of analysis phase of digital investigations.

6. Future Work

It possible to carry out more practical work on other windows-based applications apart from the ones considered in this work. The research may explore both quantitative and qualitative assessment of user input will be explored on the assumptions of how user input information can be reconstructed from the application memory, to form a continuous block chain of evidence.

7. References

1. Lee S, Sunghyuck H. Analysis of time records on digital forensics. Indian Journal of Science and Technology. 2015; 8(7):365–72.
2. Kleiman D, Carvey H. Windows forensic analysis. Incident Response and Cybercrime Investigation Secrets. Burlington: Syngress Publishing; 2007.
3. Syambas NR, El Farisi. Development of digital evidence collection methods in case of digital forensic using two step inject methods. JICT Res Appl ITB. 2015; 8(2):141–56.
4. Olajide F, Savage N. Dispersal of time sensitive evidence in windows physical memory. Cyberforensics, International Conference on Cybercrime, Security and Digital Forensic; Glasgow, UK: The University of Strathclyde. 2011. p. 27–9.
5. Heriyanto, AP. Procedures and tools for acquisition and analysis of volatile memory on android smartphones. 11th Australian Digitl Forensics Conference; Perth, Western Australia: Security Research Institute, Edith Cowan University. 2013.
6. Russinovich ME, Solomon DA. Microsoft Windows internal covering Windows server 2008 and Windows Vista. 5th ed. Washington: Microsoft Press; 2009.
7. Systems, volatile. The volatility framework: Volatlile memory artifact extraction utility framework. 2009 Apr; Available from: http://www.volatilesystems.com/default/volatility
8. Msuiche.Msuiche.net at: Capture memory under win2k3 or vista with win32dd. 2008 Mar; Available from: http://www.msuiche.net/2008/06/14/capture-memory-under-win2k3-orvista-with-win32dd
9. Olajide F, Savage N. A study of application level information from the volatile memory of windows computer systemns [PhD thesis]. Portsmouth, UK: University of Portsmouth; 2011.
10. Stuttgen J, Cohen M. Anti-forensic resilient memory acquisition. Digital Investigation. 2013; 10:105–15.
11. Kornblum J. Identifying almost identical files using context triggered piecewise hashing. Digital Investigation. 2006; 3:1–7.
12. Kurt O. A forensically robust method for acquisition of iCloud data. Digital Forensics Research Workshop, Digital Investigation; Magnolia, Denver: Elsevier. 2014. p. 106–13.
13. Garcia, GL. Forensic physical memory analysis:An overview of tools and techniques. Seminar on Network Security; Helsinki, Finland. 2007.
14. Schuster A. Searching for processes and threads in microsoft windows memory dumps. Digital Forensic Research Workshop (DFRWS); 2006.
15. Harris R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem.

Digital Investigation Proceedings of the 6th Annual Digital Forensic Research Workshops; 2006. p. 4–9.
16. Beebe NL, Liu L. Ranking algorithms for digital forensic string search hits. Digital Forensic Research Workshop (DFRWS), Digital Investigation; Denver. 2014. p. 124–32.
17. Olajide S. Application level evidence from volatile memory. Journal of Computing in Systems and Engineering. 2010 Dec; 2:40–8.
18. Vomel S, Stuttgen J. An evaluation platform for forensic memory acquisition software. Digital Investigation. 2013; 10:30–40.
19. Wählisch MV, Charousset D, Schmidt TC, Paxson V, Matthias. Native actors: How to scale network forensics. ACM SIGCOMM' 14 Computer Communication Review; Chicago, IIIinois. 2014.
20. Florio E. When malware meets rootkits. Virus Bulletin; 2005.
21. Savage N, Olajide F. Forensic live response and events reconstruction methods in linux systems. PGNET The Convergence of Telecommunications Networking and Broadcasting; Liverpool. 2009. p. 141–7.
22. Home Office, UK. News UK Politics. UK cyber crime costs £27bn a year-government report. 2011; Available from: http://www.bbc.com/news/uk-politics-12492309
23. Cohen F. Challenges to digital forensic evidence. Cybercrime Summit 06 Digital Investigation; Washington. 2006. Available from: http://all.net/Talks