INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES
ISSN: 2322-0821(O) ISSN: 2394-9910(P)
VOLUME 10 ISSUE 4
Oct 2022 - Dec 2022
www.irjeas.org

Original Article

Live Memory Forensic for Windows

*Priya Parameswarappa [1]

[1]*Research Scholar, School of Information Technology, University of the Cumberland's, Kentucky, USA*
pparameswarappa69940@ucumberlands.edu https://orcid.org/0000-0003-2059-6043

**Corresponding Author – pparameswarappa69940@ucumberlands.edu*

DOI - https://doi.org/10.55083/irjeas.2022.v10i04002

Received: 21 August 2022; Accepted: 17 October 2022

Abstract: This work describes a functional, generic, broad-scoped investigative methodology for Windows memory analysis. The methodology applies equally to functional and damaged, or corrupted memory images and relies on Volatility. It is based on the author's various memory analysis case studies. Summing it up succinctly, the methodology aids the forensic practitioner in squeezing the maximum amount of possible evidence from a memory image. The proposed methodology is suitable for analysts at all levels of investigative capability. It provides guidance in extracting maximum evidence using simple, commonplace tools and techniques familiar to digital forensic practitioners. As with all methodologies, nothing is written in stone; the forensic practitioner must be flexible and agile in responding to ever-changing investigative requirements. To assess the performance of various tools for gaining, analysing, and improving criminal evidence from volatile memory. A comparison of several tools is offered in order to provide a better understanding of the tools used.

Keywords: Cyber security, Memory analysis, Memory forensic, Windows

1. INTRODUCTION

Memory analysis can be complex and time consuming, particularly when done manually using command line driven analysis frameworks (e.g., Volatility, Rekall). This is in contrast to automated or semi-automated frameworks that remove the investigator or analyst as much as possible (e.g., CounterTack ResponderPro, Mandiant Redline). Which to choose is a matter of needs vs. available resources. In situations where ample resources are available, manual analysis is an excellent manner for investigators and analysts to maintain and sharpen their skills.

Either way, there is an overreliance on automated tools. This leads to situations where investigators and analysts cannot explain the production of certain results. While such frameworks and tools certainly speed up triaging and analysis, they are unlikely to catch highly complex or stealthy malware; this has been corroborated using ResponderPro, although mileage may vary with other similar frameworks. In such cases, only a manual analysis conducted by a competent investigator can find evidence or indications of its presence.

Various memory analysis frameworks exist, including, but not limited to, free and open source software (FOSS) solutions (e.g., Volatility, Rekall.) There also exist various commercial frameworks. The primary difference between these paradigms is that the FOSS solutions usually allow an investigator or analyst to modify plugins or write new ones using

high-level languages, to modify or improve their capabilities[1-2].

As there is no one-size-fits-all approach, investigators must be versatile in memory forensics, so that, when necessary, deviation from the proposed methodology will not result in the loss of analytical focus or capability. This paper attempts to combine these various case studies into a more formalized methodology although it remains qualitative in nature. Although it places much emphasis on identifying and extracting malware-specific evidence, it is sufficiently generic to allow for extracting much additional information and evidence. While it makes avid use of Volatility and its myriad plugins, broader analysis will typically maximize evidentiary extraction to better fill gaps in the investigation [3].

2. BACKGROUND

The author's initial Windows-specific investigative methodology was first proposed in the Zeus report [4]. It was later refined in Prolaco & SpyEye [5] and then further clarified in Stuxnet [7] and Tigger [8]. These early models were a first step towards a generic analytical approach. Since then, it has been vastly improved, tested and generalized. Additional revisions improved its focus for handling the complexities of malware memory investigations. However, it does not discuss Law Enforcement specific techniques or methodology. Instead, it provides a clear approach for conducting generic investigations for non-reverse engineers, computer forensic investigators and analysts [6].

Various steps are proposed in this methodology. Some are mandatory, others optional. It is broken down into ten specific steps, most of which provide an opportunity to cease the investigation and conduct a wrap-up. These steps can be readily rearranged or altered to suit the reader's needs as hey meant to be fluid. Additional processing can be applied wherever necessary. While it is aptly suited to malware, it is entirely appropriate for non-malware investigations too[7-12].

The tools and techniques described in the methodology are familiar to forensic practitioners at both ends of the knowledge/capability spectrum. Often taken for granted, they can be readily used in extended memory analysis.

3. METHODOLOGY

The process of memory forensic is majorly categorized in three distinguished processes.

- Memory Procurement
- Data Analytics
- Evidence Recuperating.

3.1 Memory Procurement

It's not straightforward to extract the "memory image" from a live memory. Because the data we're getting is from main memory, we must be cautious because even little relocation can result in heap de-regimentation [13]. For Windows, there are a variety of tools and strategies for acquiring volatile memory and extracting harmful applications from it. Used tools are simple and can yield intriguing results.

3.1.1 Live RAM Capturer by Belkasoft

Figure 1 portrays Belkasoft's Live RAM Capturer, a free unpredictable memory measurable instrument that is utilized to catch fundamental RAM [14]. It accompanies both 32-cycle and 64-digit bit drivers, letting it to run in the most favoured portion mode. The memory dump will be saved with the mem expansion, and it will be analyzed later with the Belkasoft proof focus apparatus [15].

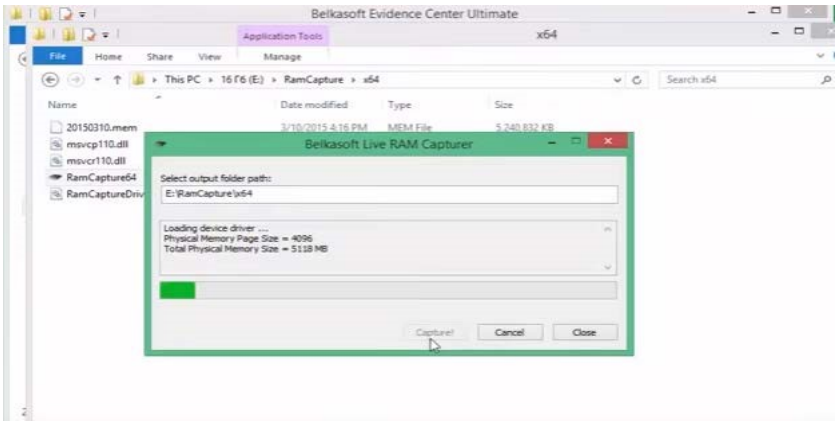

Figure 1- Procurement of Memory

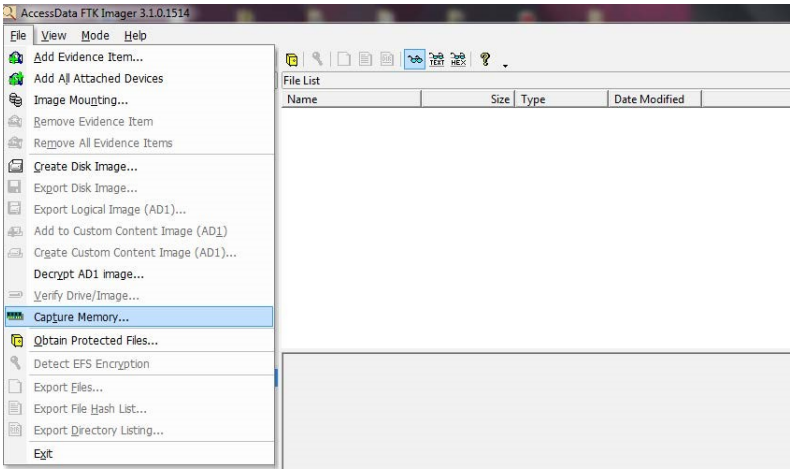

Figure 2- Choose the "Capture memory"

3.1.2 Ftk Imager

The Ftk Imager22 produces a bit-by-bit image with unused and slack space. As seen in Figure 2, it assists in the capture of active RAM, but it is unable to inspect the memory dump obtained. It stores the memory dump as memextentions (as seen in Figure 3), which may then be analysed using the wxHexEditor tool or another tool [16].

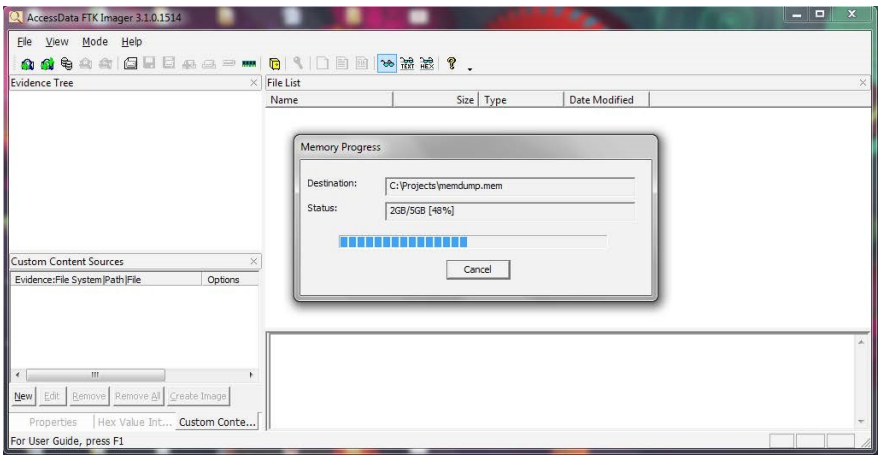

Figure 3- FtkImager Tool for procurement of memory

3.1.3 Madiant Memoryze

MadiantMemoryz23 is a free memory forensics tool that helps first responders find evil in real-time memory. It has the ability to both acquire and analyse memories. As seen in Figure 4, this programme can capture all processes that are in running condition, all drivers, and the entire memory image dependent system [17].

3.1.4 DumpIt

It's a fascinating tool which provides the facility to the people wishing to record the RAM of a suspicious or under surveillance individual [18-20]. The live RAM may be acquired in less than a minute with this utility, which can be stored on a pen drive. Just an affirmation question (i.e., asking yes or no) is provoked when the pen drive is joined and DumpIt24 is run on that individual's PC, as displayed in Figure 5, and a mem document of that individual's live RAM is put away on the pen drive.

3.2 Acquired Memory Dump Analysis

Following the obtaining of the memory picture, the memory picture will be surveyed. The evidences must be thoroughly examined during this step.

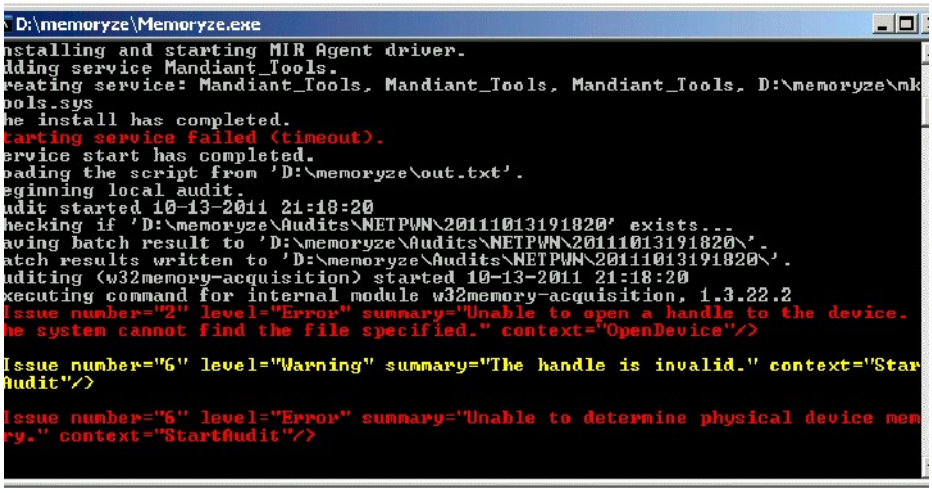

Figure 4- Mediant Memoryze Tool Demonstration

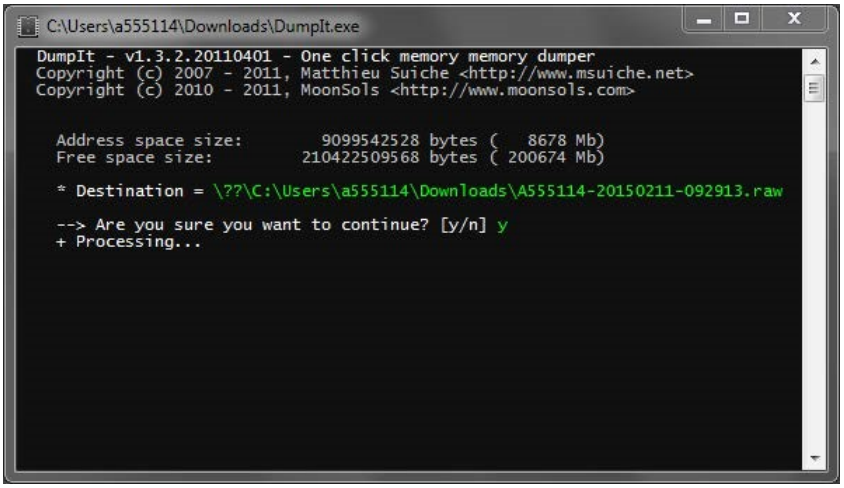

Figure 5- DumpIT memory procurement

3.2.1 Evidence Centre at Belkasoft

Belkasoft21 is highest intriguing applications available today. This application reads the mem file created by the Belkasoft LIVE Ram capturer, which allows it to swiftly analyse the memory dump. It's simple to understand and use, and it doesn't require any special understanding to use [21]. The technique for presenting the gathered memory file connected to photographs from Belkasoft live RAM capturer is shown in Figure 6. Figure 7 illustrates how to import the necessary data sources for carving. Finally, as shown in Figure 8, the carved data of the acquired memory image is analysed [22].

3.2.2 wxHexEditor

wxHexEditor25 can be used to examine the memory dump captured by the FtkImager. It's a free programme that analyses memory dumps. It is divided into two sections: right side and the left side. The information string values are displayed on the right side, while the string hex values are displayed on the left side. Figure 9 shows the FtkImager-captured memory image being loaded into wxHexEditor for processing.

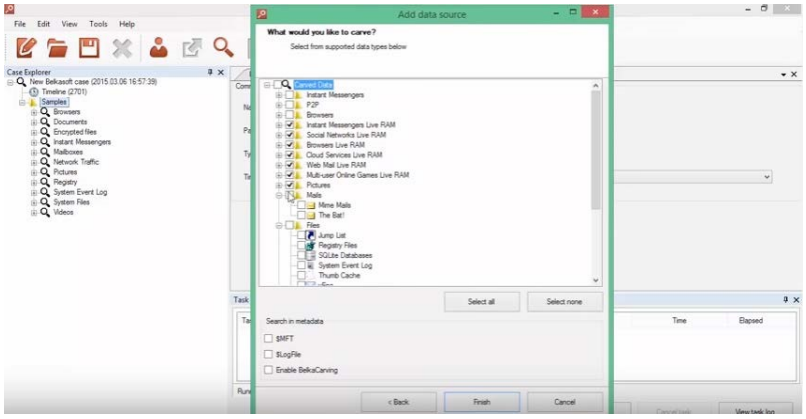

Figure 6- Access of Procured Memory with Belkasoft

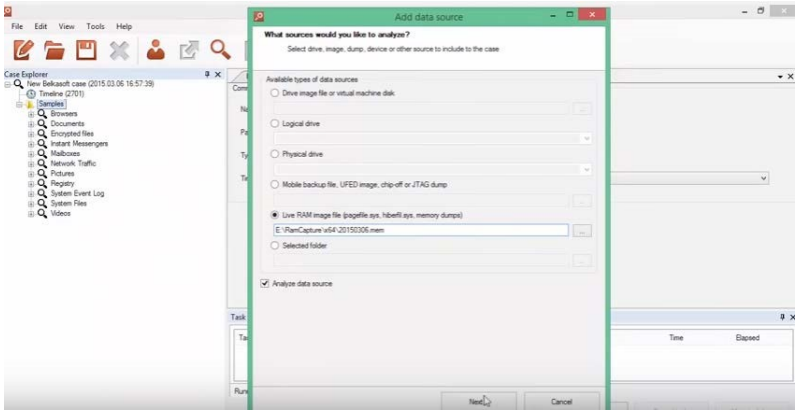

Figure 7- Updation of Data Source

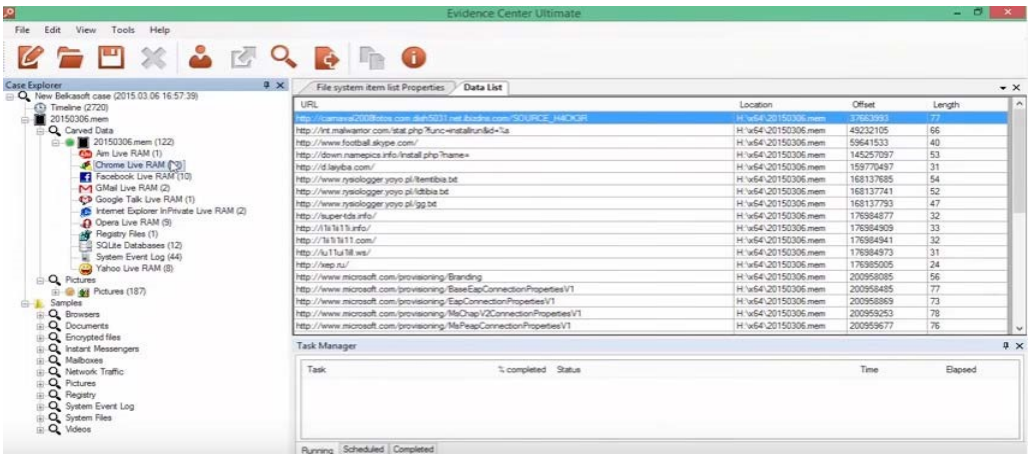

Figure 8- Data Analytics from Procured Memory

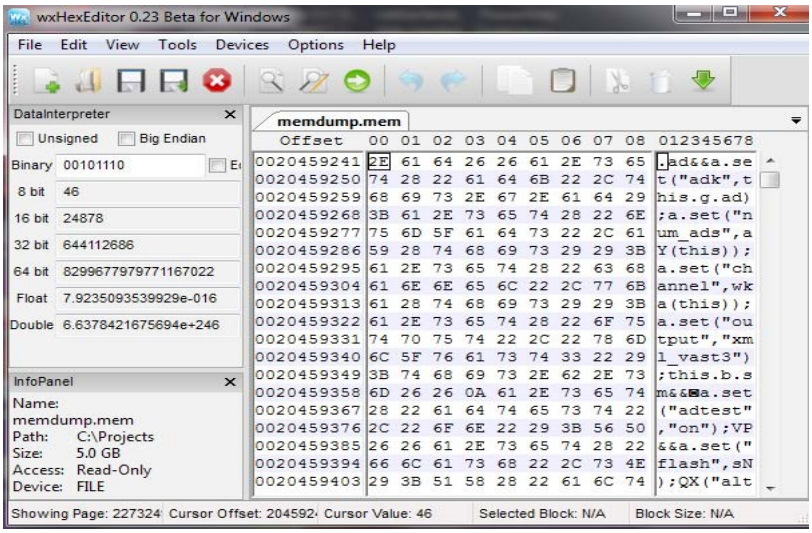

Figure 9- FtkImager Screenshot with procured memory

This tool allows you to look for a pattern by typing some words into the search box. Figure 10 depicts the results of a search for the term "gmail." Figure 11 shows the result of enquiring for the word gmail. The terms that match "gmail" will be shown as shown in Fig. 11 and can then be evaluated. As demonstrated in Figure 12, the wxHexEditor can be used to extract users and passwords.

3.3.3 Autopsy

Autopsy26 is a free utility that analyses the RAM that has been recorded. It's used to examine disc images and do in-depth file system analysis. Figure 13 depicts the Autopsy tool in action.

3.4 Recovering Data using FtkImager

In order to protect the system, the attacker may remove some sensitive information or photos. However, data that has been deleted can be recovered. Although it is a taxing process that needs complete concentration, the outcomes are occasionally fascinating. Assume the attacker utilised a puppy image and then erased it from the machine. The image can now be retrieved using FtkImager22, as illustrated in the screenshots in Figures 14, 15, 16 and 17. The assailant stores the photograph before deleting it from the file as well as the recycle bin. The FtkImager application is launched, and deleted files are searched in the unallocated region. Because FtkImager does not include a searching tool, each file must be opened individually.

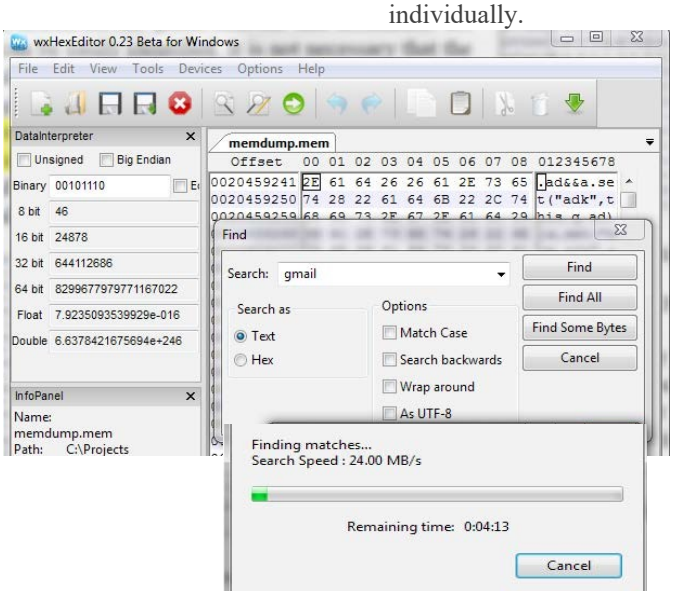

Figure 10- Evidence-based procured memory analytics

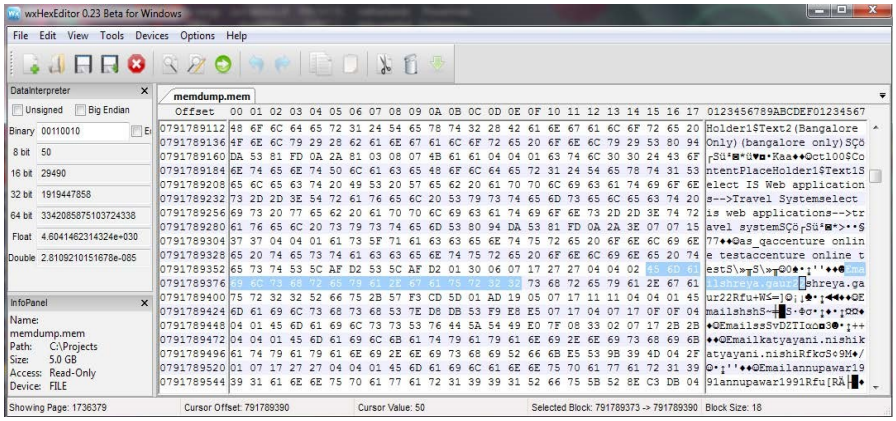

Figure 11- Analytics of Procured Gmail Details

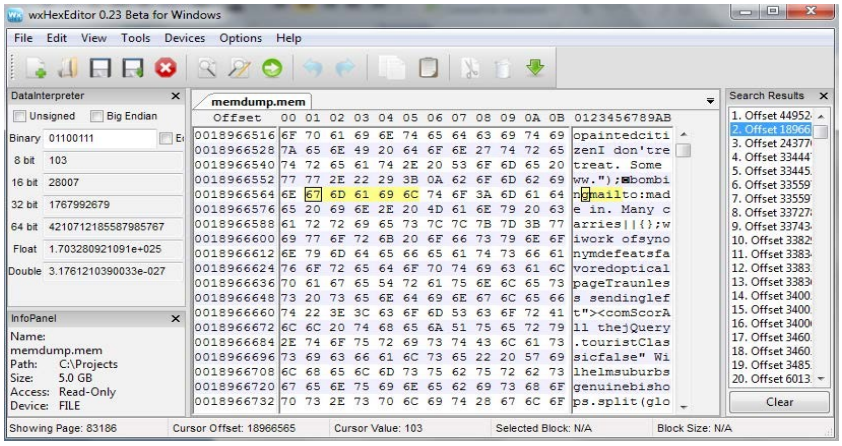

Figure 12- Retrieval of Credentials

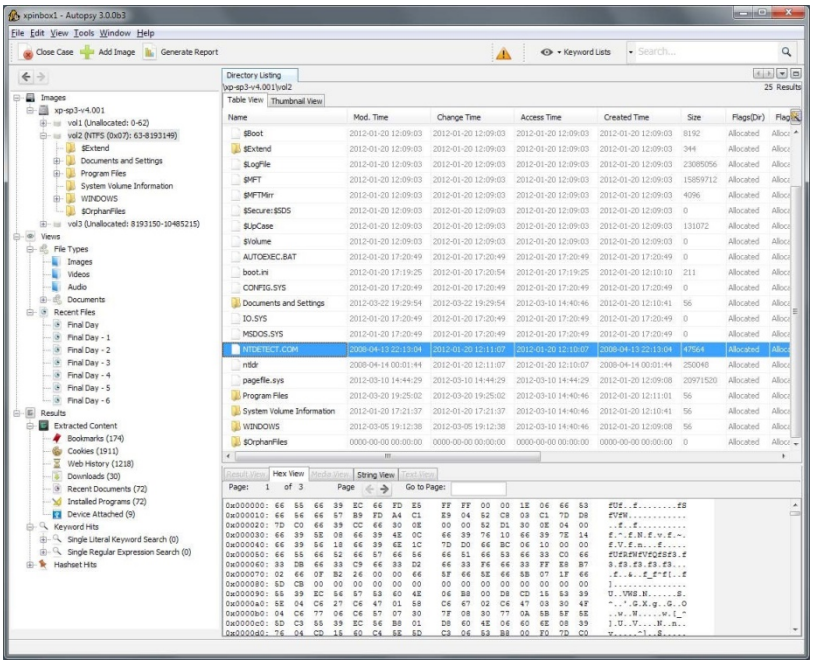

Figure 13- Evidence Finding using Image Analytics

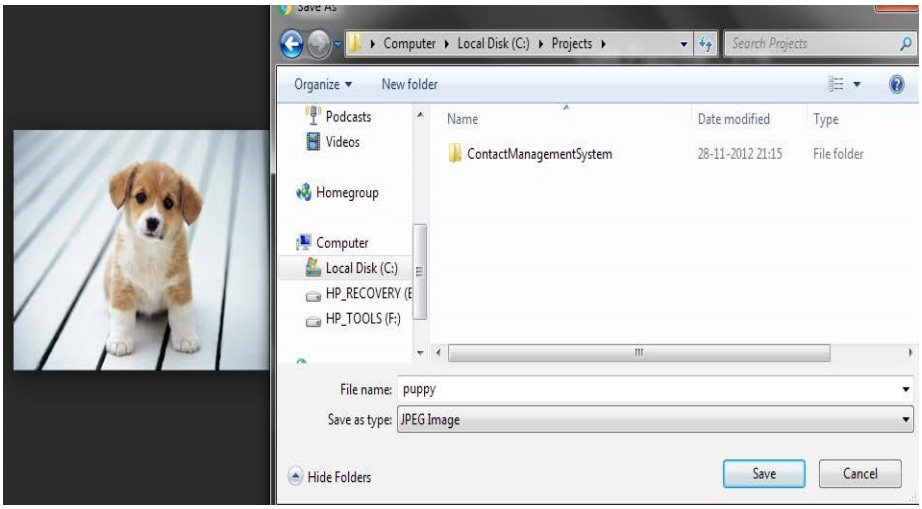

Figure 14- Store the Image

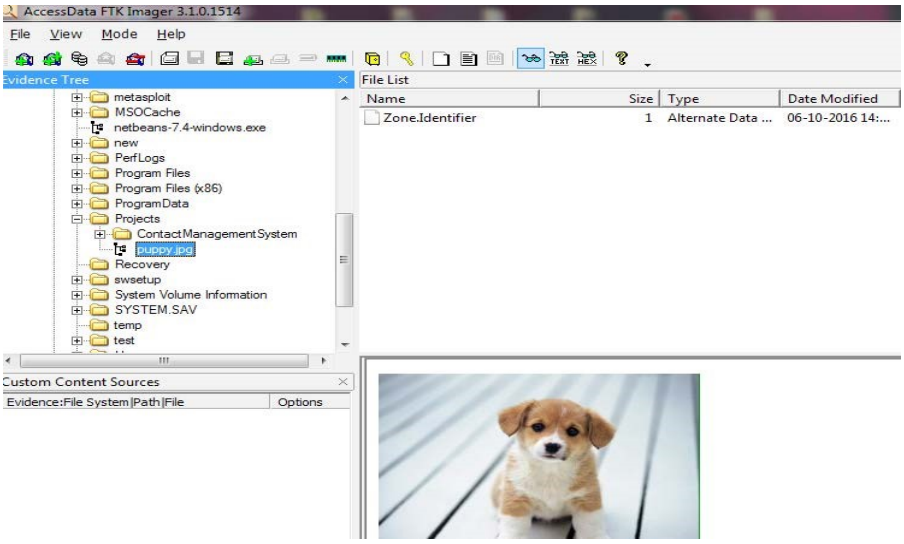

Figure 15- FtKImager based image

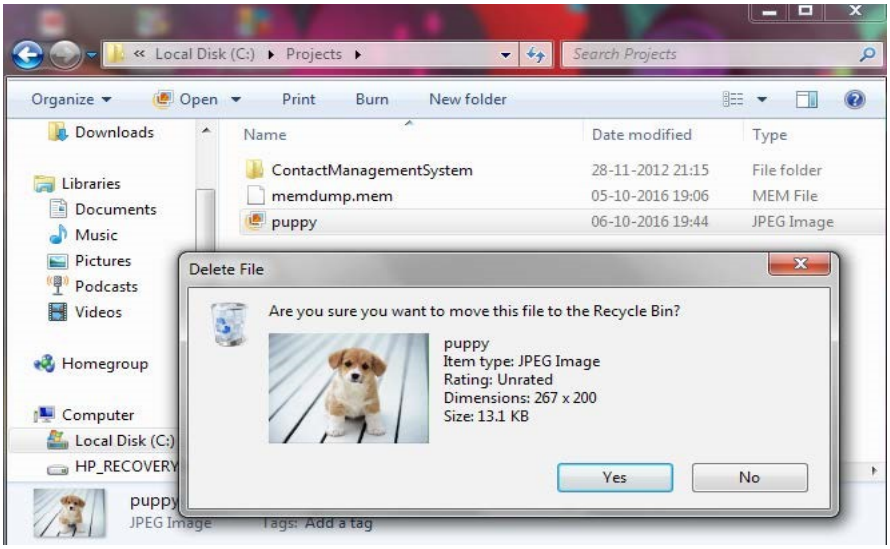

Figure 16- Destroy the Image

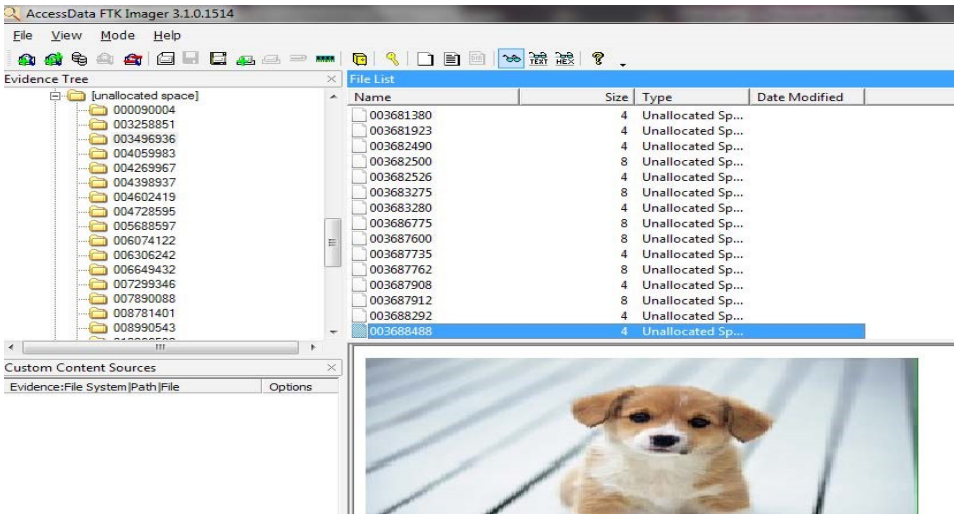

Figure 17- Recovery of Deleted File

4. DISCUSSION

Memory forensics is a large field with a lot of work done so far. Researchers used to focus on hardware acquisition although software acquisition has become increasingly prominent in the recent decade, while unstable memory legal sciences are still in its outset. Despite the fact that there are various free devices accessible to support the examination of impermanent memory, there are as yet a couple of holes that should be filled. Looking at the information recovered turns into a troublesome and tedious methodology since the information to be broke down is seen as a tree with many branches in FtkImager and Belkasofttools. It also does not guarantee hundred percent successes, which can result in fruitless searches. The tools examined in this study are solely designed to locate a specific piece of evidence, not to aid in the inquiry; as a result, the investigation takes a long time to complete. This essentially means that the investigator must use his or her brains to locate evidence, as the technology does not supply intelligent data. Another key issue in the field of forensics is that numerous tools are required to obtain results, and one instrument is insufficient throughout the entire process. The instruments take a long time to retrieve and restore information that is sensitive, which may result in excessive harm, and critical evidence could be destroyed because information does not last long in memory.

5. CONCLUSION

A very new discipline that has a lot of promise emerged as a Memory forensics. Although different technologies exist to tackle cybercrime, their efficacy and effectiveness are insufficient to deal with the tremendous increase in cybercrime. Regardless of the explosive growth of digital forensics over the last decade, this field has a promising future. The increased attention on memory forensics is a significant step in quickly combating cybercrime. There are lot of tools available for volatile memory. Some of them have been discussed in this study. The limitations and benefits of tools for executing the three key memory forensics activities of acquisition, analysis, and recovery have been examined. There is a lot of future potential in the field of memory forensics. Some tools provide a tree-like structure that can be adjusted to save time and offer improved results. Additionally, the focus should be on developing a single tool capable of acquiring and analysing memory.

REFERENCES

[1] Reith M, Carr C, Gunsch G. An examination of Digital Forensics Models. International Journal of Digital Evidence. 2002; 1(3):1–12.

[2] Hay B, Nance K, Bishop M. Live analysis: Progress and Challenges. IEEE Security and Privacy. 2009:7(2):30–7.

[3] Wang L, Zhang R, Zhang S. A model of computer live forensics based on physical memory analysis. Proceedings of 1st IEEE International Conference on Information Science and Engineering (ICISE). 2009. p. 4647–9.

[4] Aljaedi A, Lindskog D, Zavarsky P, Ruhl R, Almari F. Comparative Analysis of Volatile Memory Forensics: Live Response vs. Memory Imaging. Proceedings of 3rd IEEE International

Conference on Privacy, Security, Risk and Trust. 2011.p. 1253–8.

[5] Petroni NL,Walters A, Fraser T, Arbaugh WA. FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory. Digital Investigation. 2006;3(4): 197–210.

[6] Gianni F, Solinas F. Live Digital Forensics: Windows XP vs Windows 7. Proceedings of 2nd IEEE International Conference on Informatics and Applications (ICIA). 2013. p. 1–6.

[7] Balogh S, Pondelik M. Capturing encryption keys for digital analysis. Proceedings of 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). 2011. 2, p. 759–63.

[8] Savold A, Gubian P. Towards the virtual memory space reconstruction for windows live forensic purposes, Proceedings of 3rd IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. 2008. p. 15–22.

[9] Carrier BD. Risks of live digital forensic analysis. Communications of the ACM. 2006; 49(2): 56–61.

[10] Meera V, Isaac MM, Balan C. Forensic acquisition and analysis of VMware virtual machine artifacts. Proceedings of IEEE Automation, Computing, Communication, Control and Compressed Sensing (iMac4s). 2013. p. 255–9.

[11] Chhikara RR, Sharma P, Singh L. A hybrid feature selection approach based on improved PSO and filter approaches for image steganalysis. International Journal of Machine Learning and Cybernetics. 2015; 7(6):1195–206.

[12] Shenbagarajan A, Ramalingam V, Balasubramanian C, Palanivel S. Tumor diagnosis in MRI brain image using ACM Segmentation and ANN-LM classification techniques, Indian Journal of Science and Technology. 2016 Jan; 9(1): 1–12.

[13] Sajana T, Sheela Rani CM, Narayana KV. A Survey on clustering techniques for Big Data mining. Indian Journal of Science and Technology. 2016 Jan; 9(3):

[14] Hamid HM S, Shafie AL M, Yahaya C, Muhammad A S. An appraisal of meta-heuristic resource allocation techniques for IaaS Cloud. Indian Journal of Science and Technology.

[15] Deevi R. R, Sk. Nazma S, Pasala L. S. Challenges of Digital Forensics in Cloud Computing Environment, Indian Journal of Science and Technology. 2016 May; 9(17):1–7.

[16] Sungjin L, Sunghyuck H. Analysis of Time Records on Digital forensics. Indian Journal of Science and Technology. 2022 Apr; 8(S7):365–72.

[17] Belkasoft tool. 2022March 03. Available from: https:// belkasoft.com/ec.

[18] Ftkimager tool. 2022March 24. Available from: https://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.2.0.

[19] Memoryze tool. 2022March17. Available from: https:// www.fireeye.com/services/freeware/memoryze.html.

[20] Dumpit tool.2022April 27. Available from: http://qpdownload.com/dumpit.

[21] Wxhexeditor tool.2022March 25. Available from: https:// sourceforge.net/projects/wxhexeditor/.

[22] Autopsy tool. 2022March 25. Available from: http://www.sleuthkit.org/autopsy/download.php.

Conflict of Interest Statement: *The author declares that there is no conflict of interest regarding the publication of this paper.*