RAM DUMP COLLECTION TOOL

Sanjay Kumar P[1], Ajay Kumar C[2], Gokul Krishna C[3], Arun Karthik R[4],
sanjaykumar.it20@bitsathy.ac.in, ajaykumar.it20@bitsathy.ac.in,
gokulkrishna.it20@bitsathy.ac.in, arunkarthik.it20@bitsathy.ac.in

[1]*Student, Information Technology, Bannari Amman Institute of Technology, Tamil Nadu, India*
[2]*Student, Information Technology, Bannari Amman Institute of Technology, Tamil Nadu, India*
[3]*Student, Information Technology, Bannari Amman Institute of Technology, Tamil Nadu, India*
[4]*Student, Information Technology, Bannari Amman Institute of Technology, Tamil Nadu, India*

ABSTRACT

The field of digital forensics is dependent on the accurate collection and examination of volatile memory contents, where RAM dump collecting tools play a crucial role. This in-depth study offers a perceptive examination of RAM dump collecting methods, outlining their functions, prowess, and applicability to the field of digital forensics. The essay emphasizes the crucial role that RAM dump collection plays in forensic investigations because of the richness of important data stored in volatile memory. This survey's main focus is on the complex technological difficulties associated with memory acquisition. The meticulous research covers a wide range of topics, including the tough memory protection techniques used by contemporary operating systems. The report also emphasizes how important it is to use forensically sound acquisition procedures to maintain the integrity of the evidence throughout collection. The investigation is completed by illuminating the RAM dump collecting tool landscape and identifying their various characteristics and suitability for addressing the dynamic field of digital forensics. This review converges on the complicated interaction between encryption keys, volatile memory, and their resonance within digital forensics in the goal of a comprehensive knowledge of RAM dump collecting technologies. In conclusion, this investigation broadens our understanding of the usefulness of RAM dump gathering tools in modern investigative techniques.

Keyword: - *RAM dumps, examination of volatile memory, digital forensics, and encryption keys*

1. INTODUCTION

The discipline of digital forensics requires specific tools that allow investigators to acquire and examine computer systems' volatile memory, or RAM dumps. Volatile memory, often known as RAM (Random Access Memory), holds important details about the present state of a system, such as active processes, network connections, open files, and encryption keys. Forensic experts might find important evidence and acquire insights into the activity that took place on a computer at a certain moment by obtaining and examining RAM dumps.The main goal of RAM dump collecting tools is to record the information in volatile memory of a system and save it to a storage device for subsequent examination. These programmes make use of a variety of methods to obtain memory dumps, such as software-based methods utilising kernel-level drivers.Both open-source and for-profit versions of RAM dump gathering programmes are available, and each has a unique set of features and functionalities. Open-source solutions offer flexibility and customizability choices, enabling users to extend and adapt their functionality in accordance with their own needs. On the other hand, commercial programmes frequently include user-friendly interfaces, thorough support, and extra features designed for certain forensic purposes. These tools make it easier to analyse the memory image that was obtained after a RAM dump has been acquired .To help investigators spot patterns, spot criminal activity, and reconstruct human behaviours, some systems also include sophisticated memory analysis techniques and heuristics. As computer architectures, operating systems, and digital forensic techniques evolve, so does the field of RAM dump gathering tools. These tools are updated to support the most recent operating systems, hardware setups, and memory protection techniques when new technologies are developed. In order to increase efficiency and decrease the amount of human work necessary, there is also an increasing focus on automating the analysis process and including memory analysis frameworks into these tools.

2. LITERATURE SURVEY

Significant authors independently provide their perspectives on the difficulties with data security, the advantages of the Ram dump collection tool, and the value of analyzing the dump files. They provide a springboard for more investigation and bolster the significance and applicability of the ongoing study. In their papers,[2] Vivek Ravindra, H.K. Khanuja ,Studied Memory imaging approach of RAM analysis is used to find out the malicious processes using the GUI based tool that can analyze the volatile memory artifacts that are affected by malwares,[3] Mifraz Murthaja ,Benjamine,Diluxana Uthayakumar. Investigated the four predominant domains of registry, DLL, API calls and network connections in memory forensics to implement the system `Malfore,' which helps automate the entire process of memory forensics.analyze malware samples and to obtain memory dumps and volatility frameworks to extract artifacts from the memory dump, [7]Arash Habibi Lashkari; Beiqi Li; Tristan Lucas Carrier, Introduces VolMemLyzer, Developed python-based tool to excerpt the most critical characterization feature set from the memory dumps taken during live malware infection,[10] Stuart Laing, Robert Ludwiniak ,analyzed the forensic viability of a RAM analysis method for Hadoop based investigations and compared it against targeted process data dumping through the Java heap information. The RAM analysis was done through string searching and the use of the RAM analysis tool Volatility.

3. PROPOSED METHODOLOGY

There are several crucial elements in the suggested process for creating RAM dump gathering tools. The first step is to do a thorough literature review to grasp the current tools, strategies, and processes. The requirements and goals of the tool are specified in light of the gaps and restrictions that have been found. The tool's features, such as live memory acquisition or physical memory acquisition, are chosen, along with the target operating systems and memory acquisition strategies. The tool is then put into use while taking into account the design, architecture, and programming language. To evaluate the tool's usability, dependability, and performance in various scenarios, validation and testing are conducted. The testing phase's findings and analysis are presented, along with a comparison to other tools and discussions of the tool's advantages, disadvantages, and prospective improvements. Examples of actual use cases are given to show how the technology may be put to use in the real world. The study finishes with a discussion of the findings' implications, recommendations for further research, and a thorough list of references. This methodology makes sure that the creation of RAM dump collection tools is done in a methodical and organised way, encouraging innovation and developments in the field of memory forensics.

Steps involved	**Description**
Process ID	Selection of process id or memory range
Access Memory	The mechanisms provided by the operating system to access the memory. This can involve using libraries, or kernel interfaces that provide access to the physical memory using (Frida framework)
Capture RAM Contents	This process typically involves iterating through memory pages and copying their data into a file or buffer.
Write to Disk	This could involve creating a file in a specific format or encoding, compressing the data if necessary.

Table 1: *Summary of steps*

4. IMPLEMETATION

The creation of an effective RAM dump collecting tool necessitates a planned procedure that includes many essential components. The first choice is choosing a framework and programming language that function well together while taking into account aspects like platform compatibility, performance enhancement, and the accessibility of necessary libraries or modules. The selection of a memory acquisition technique is therefore of utmost significance. Options like physical memory acquisition, hibernation file extraction, or live memory acquisition need to be carefully considered depending on the goals and target operating systems. Different requirements and difficulties are brought to the fore with each strategy.A special module should be created to make the memory acquisition procedure easier.

This module serves as a link between the tool and the target operating system's memory management subsystem. It makes it possible for the tool to communicate with system memory, extract the necessary data, and then get the data ready for further analysis.It is crucial to choose the right data format for storing the collected memory dump. Depending on factors like storage effectiveness and simplicity of investigation, this can include using hibernation files or choosing raw memory dumps.The memory dump itself must be created and stored with extreme care To record and manage unforeseen circumstances and improve the tool's reliability, robust error handling.Validating the tool's compatibility and functionality across a range of operating systems and versions is essential. To guarantee consistent outcomes, performance, dependability, and accuracy must be evaluated in a variety of settings.These procedures must be carefully followed in order to create a powerful and efficient RAM dump gathering programme.

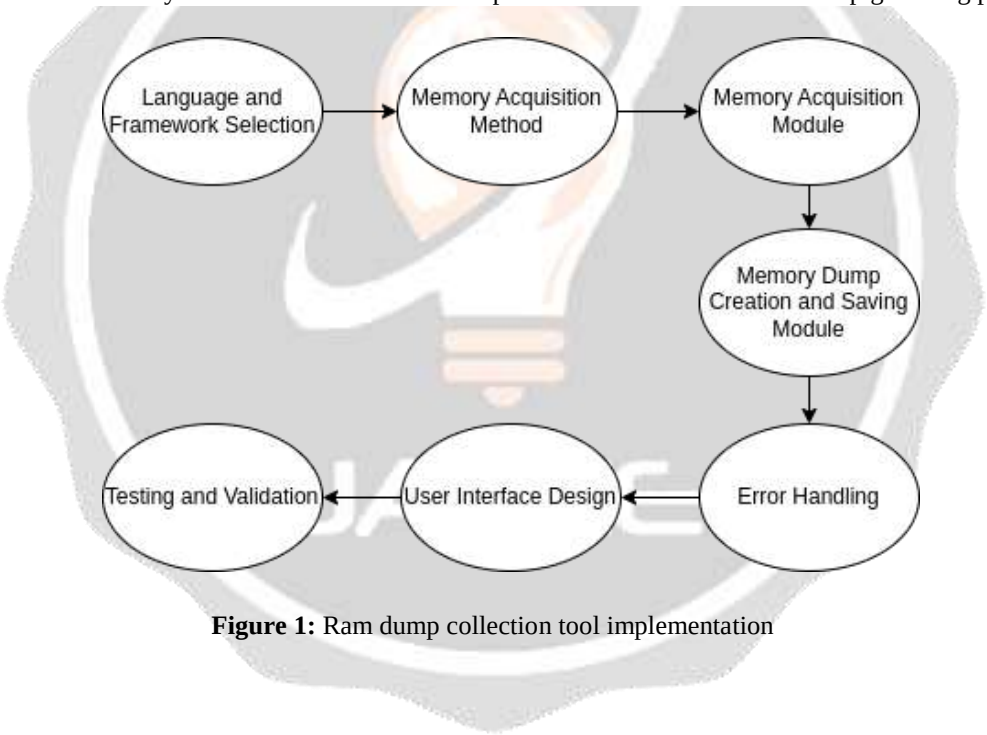

Figure 1: Ram dump collection tool implementation

5. RESULTS AND DISCUSSION

The RAM dump collection tool demonstrated reliable performance in capturing accurate and comprehensive memory snapshots. It provides valuable support for forensic investigations, incident response, and malware analysis.

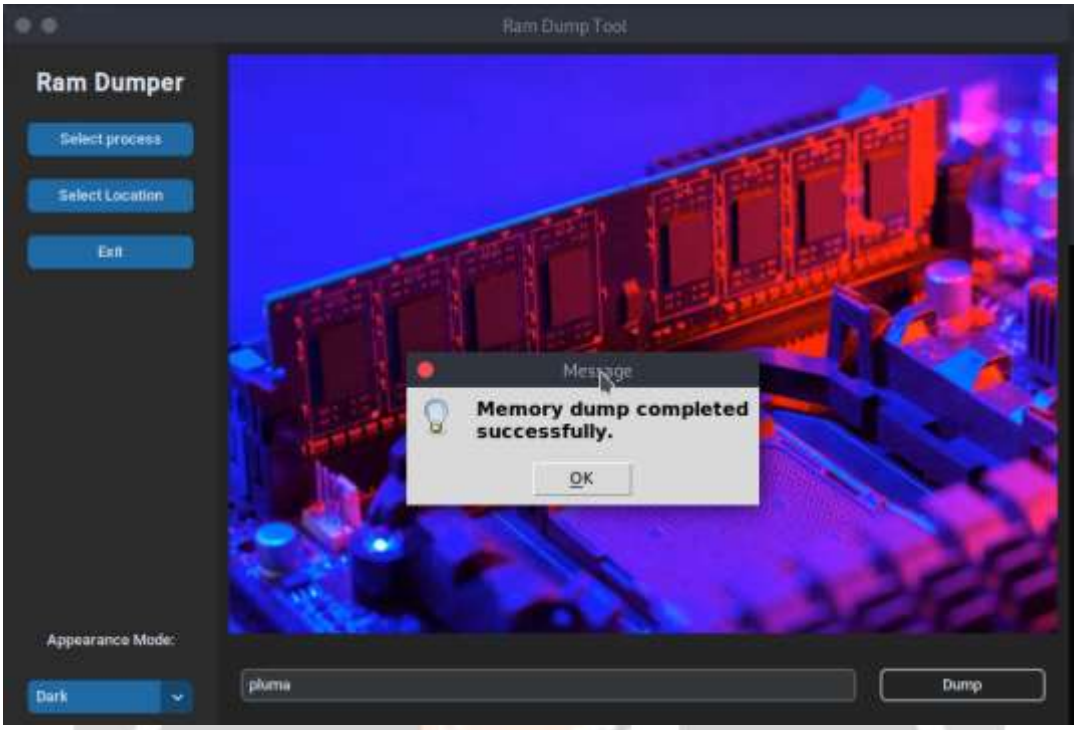

Figure 2(a): Ram dump collection tool GUI

The Tools consist of Select Process through an End user can select the process/Application that we to dump from memory,Select Location is used select storage location of dump files and there is an option for appearance mode through which user can change background mode and Finally Dump option through which we can dump the selected process.

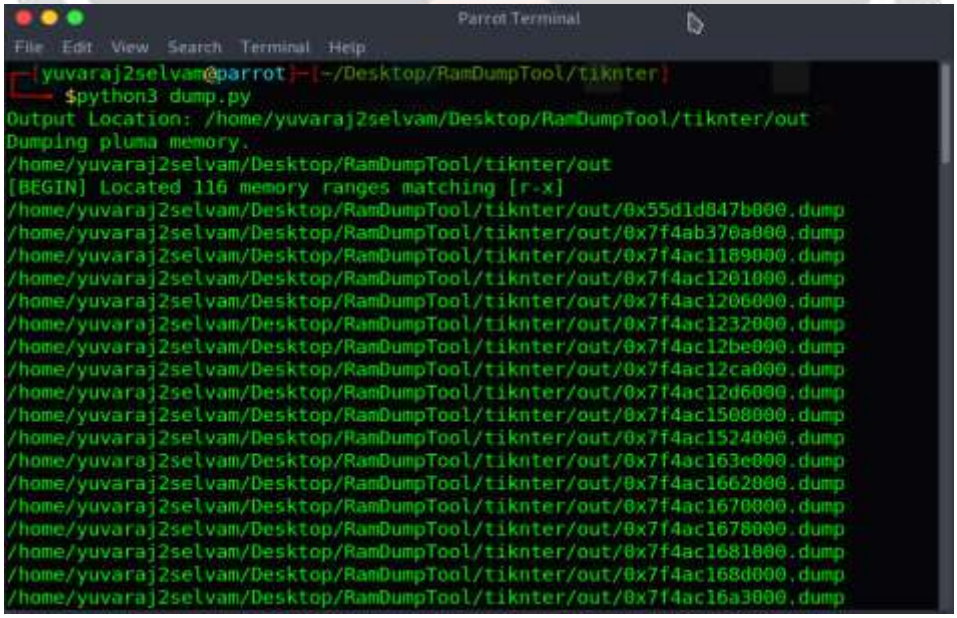

Figure 2(b): Ram dump tool GUI Background Process

When collecting memory dumps from a range of operating systems and configurations, the RAM dump collection tool has proven to have dependable functionality and efficient performance. The tool has effectively captured volatile memory contents after extensive testing and evaluation, giving important information for forensic analysis and investigation needs.

6. CONCLUSION

An expanding field, memory forensics offers a lot of potential. Although there are many technologies available to combat cybercrime, their efficiency and efficacy are insufficient to deal with the enormous rise in cybercrime. Despite the rapid expansion of digital forensics over the past decade, this area has a highly promising future. Focusing on memory forensics is a significant step in the direction of swiftly reducing cybercrime. The Ram dump tools for volatile memory have been covered in this study. The field of memory forensics has a very bright future.An important development in the realm of memory forensics and digital investigations is the RAM dump gathering tool.

7. REFERENCES

[1] K. Bharanitharan and V. Chandrasekaran. "A Comparative Study of Memory Acquisition Tools for Forensic Analysis"

[2]. Mahesh Kolhe et al (2018). Live Vs Dead Computer Forensic Image Acquisition. International Journal of Computer Science and Information Technologies

[3]. Vivek Ravindra, H.K. Khanuja ,(2018).The Analysis and Extraction of Malicious Processes from Memory Image Using GUI Based Memory Forensic Toolkit

[4]. Mifraz Murthaja ,Benjamine,Diluxana Uthayakumar ,(2019).An Automated Tool for Memory Forensics

[5].Rima Asmar Awad; Juan Lopez; Mike Rogers, (2019) .Volatile Memory Extraction- Based Approach for Level 0-1 CPS Forensics

[6]. Wiley Data ,(2020) Memory Analysis

[7]. Arash Habibi Lashkari; Beiqi Li; Tristan Lucas Carrier,(2021).Volatile Memory Analyzer for Malware Classification using Feature Engineering

[8]. Meenu Hariharan; Akash Thakar; Parvesh Sharma(2022),Forensic Analysis of Private Mode Browsing Artifacts in Portable Web Browsers Using Memory Forensics

[9]. Anh-Duy Tran; Quoc-Trung Nguyen; Anh-Minh Nguyen,(2022).OS-Independent Memory Forensics for IoT Devices in Cybercrime Investigations

[10]. Stuart Laing, Robert Ludwiniak, (2023) Forensic Investigation Using RAM Analysis on the Hadoop Distributed File System.

[11] Belkasoft tool. 2023 . Available from: https:// belkasoft.com/ec.

[12]Memoryze tool. 2023. Available from: https:// www.fireeye.com/services/freeware/memoryze.html.

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