International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2024.0802195

Vol. 8 issue 2 Apr-Jun 2024

Advanced Volatile Memory Forensics through Autopsy Integration

Asif Ibrahim[1] and Syed Khurram Hassan[2] and Saima Sheikh[3]

[1]Department of Mathematics, The University of Lahore, Lahore.
[2] Institute of Quality and Technology Management, University of the
Punjab, Lahore, Pakistan.
[3]Admin Pakistan Association of Advancement of Sciences
Corresponding author: khuramshah6515@gmail.com

Received: March 28, 2024; **Accepted:** May 04, 2024; **Published:** June 14, 2024

ABSTRACT

The main goal of this study is to design a novel plugin for the Autopsy forensic framework to enable forensic analysts to identify and extract volatile memory from small-scale digital devices. This includes network peripherals and Internet of Things devices, smartphones, and industrial-control systems. Given the importance of volatile memory to digital crime and cybersecurity investigations, an accurate and reliable tool is needed to non-destructively acquire forensic copies of the evidence. In the context of small-scale devices, this study is of acute importance to bridge the gap that exists in current forensic research and forensic practice, using separate tools can be challenging due to compatibility issues and the complexity of managing multiple system. In conclusion, the developed Autopsy plugin, which has been termed the MemoryIntegrator, seamlessly harmonizes with Autopsy forensic framework and is designed to work together with Volatility tool, specializing in detailed memory analysis. Consequently, the following main outcomes result from the experimentation and application of the plugin: Promotes the default forensic activity of Autopsy by providing the analysts with a way to swiftly and directly harvest and evaluate volatile data from diverse small scale digital devices. The implementation of the plugin ensures that the integrity of the memory data is maintained throughout the extraction and analysis process. This is facilitated by cryptographic hash validations that confirm that there are no changes in the data from the extraction to the point of analysis. The plugin maintains the integrity of the memory data from the time of extraction to the time of analysis using cryptographic hash validations which verifies that these data has not been manipulated at this point. MemoryIntegrator outmatched all the forensic tools herewith because conducting forensic test back at home verified its superiority in terms of the extraction of data from memory speed and the authenticity and formula which it uses in analysis. In the modern world, this is critical to investigate digital crimes and incidences that affect cybersecurity.

Keywords: Memory analysis, Digital forensics autopsy, RAM capture, Forensics imaging

1. INTRODUCTION

Digital crimes are becoming more frequent and dangerous, threatening not only personal information but also the infrastructure and financial well-being of countries and entities. With this in mind, the more severe the crime, the more reliable and accurate the forensic tools used to collect and analyze digital evidence become essential. Cyber forensics as a science focuses on the methodology and technology to recover, store, and analyze data contained in digital devices to be admitted as evidence in the court. This science is included in the analysis of offenses not only to punish the criminal but also to study the methodology of the attack, to protect oneself, to safeguard digital property, and to prevent threats.

This project fills a major gap in the forensic analysis of small-scale digital devices like IoT devices, smartphones, and industrial control systems. These devices frequently have volatile memory, where a wealth of important information about user activities, system processes and the state of the device at a given time is stored. Unfortunately, the volatile nature of this memory implies that when the device is turned off or loses power, the information is gone, making its preservation and analysis a key component of forensic examination. The main purpose of this project is to build an Autopsy plugin that enables digital forensic analysts to forensically examine volatile memory in small size digital devices [1].

2. OVERVIEW OF THE AUTOPSY PLUGIN

MemoryIntegrator is created as a plugin for the Autopsy forensic framework. The Autopsy is a free and open source tool to conduct forensic analysis of digital evidence. This plugin combines one of the biggest frameworks in memory forensics Volatility with a great framework for digital forensics Autopsy. This implies that the analysts have been able to perform the full memory analysis for a plugin in a single go with the help of Autopsy. The plugin hard codes the memory image acquisition and analysis to eliminate the volatility system. Live memory evidence is central to digital evidence collection so the plugin comes with validation and hashing features to ensure that important live memory data can be collected from the live memory. This enables the proof verification integrity to be securely locked and a never-ending store of forensic examination.

MemoryIntegrator is a plugin for the forensic framework Autopsy. Autopsy is an open-source tool that assists in the detection of forensic evidence from a digital source. The plugin fuses the capabilities of Volatility, one of the primary frameworks utilized in memory forensics, with Autopsy. With this plugin, analysts can use one tool to perform full memory analysis directly from the Autopsy platform. By automating both memory image acquisition and analysis, the plugin reduces the burden on the volatility system. From the memory to the plugin (and now with hashes and the hashing of the MC-Record and Output data on the plugin side also) this makes it possible to validate that the information coming from the volatile memory is actually valid as well. This guarantees evidence recollection integrity and forms a continuous and reliable source of forensic investigation.

At first, forensic tools were simple, manual command-line utilities with basic functions of data copying and viewing. Nowadays, forensic software is complex systems capable of intricate data analysis, automated report generation, and real-time data processing. The implementation of graphical interfaces in forensic software has made these tools accessible to non-professional investigators capable of conducting advanced forensic procedures [2].

Standards and frameworks such as the ones developed by SWGDE and IOCE, the development and creation of standards and frameworks have also been instrumental in the growth of forensic tools. These standards have ensured that forensic evidence is reliable, repeatable, and legally accepted.

The most important source of information responsible for running processes, network connections and system state in forensic investigation is volatile memory, mainly RAM. This is because, data retrieved on volatile sources is destroyed once the device is interrupted. Modern forensic analysis tools have further studied the techniques that help the acquisition and analysis of volatile data.

Tools such as Volatility and Rekall have developed the fact of memory acquisition and analysis, allowing investigators to virtually recreate the actions of users, consider system configuration and network activity, and recover passwords and encryption keys. As they are system-agnostic and work in different OPs and configurations, they are invaluable in contemporary computer forensics.

Also, the field has seen remarkable progress in live forensics offerings, through which it is possible to obtain the memory of active systems without affecting their performance. Secure and stealthy data extraction methods are now integrated in live analysis tools to minimize the possibility of gathering corrupt data as well as to escape the detection of malicious software.

Digital forensics is based on the following theoretical foundations which are computer science theories, criminal justice system, and the standard of evidence. One of the underlying ideas behind digital forensics is the Locard's Exchange Principle. It states that "every contact leaves a trace". In the framework of the present discipline, it means that all digital behaviors are leaving data traces which can later be analyzed forensically to identify the behaviors [3].

3. LITERATURE REVIEW

Digital forensics has numerous tools that enter the field, and for various reasons relatable to investigations. These range from data recovery to detailed forensic analysis. Tools used for forensic work are generally categorized into three types: data acquisition tools, data analysis tools, and reporting tools. The former group retrieves the evidence securely, so tools like FTK Imager and EnCase are fundamentally important because discarding forensic integrity equals invalid evidence. To secure the evidence metadata, one must use write blockers and at least any hash function.

3.1. Previous Work on Memory Analysis

The analysis of memory has become a key domain of focus in digital forensics as it allows for the real-time access of the operational status of a digital asset. Researchers have over the years investigated the use of reliable methods and tools that can be used for the accurate extraction and analysis of data kept in volatile memory. Volatility and Rekall are crucial tools used in examining digital devices' physical memory dumps and in the acquisition of information regarding network connections and the identification of processes, open files and logged-in user.

Finally, academic research has been a valuable contribution to the development of this area. The use of machine learning algorithms to automatically recognize malicious artifacts and abnormalities in memory data and thus accelerate and enhance the precision of forensic analysis has been an area of professional interest. Another possible direction is cross-platform memory analysis, which could help develop a single tool that could be used independently of the type of operating system or hardware involved[4].

3.2. Gaps in Current Research

Though several advancements have been recorded, still there are several gaps in the field of memory analysis. One of the major limitations is that there are limited or no tools to handle the increasing number and complexity of IoTs devices and other new digital technologies. Many tools are utilized in conventional computing environments and may not be powerful enough to analyze newer devices, which occasionally use exceptional architectures and operating systems.

Automated and on-the-fly memory analysis is another gap. Although some growth has been achieved, the existence of a real-time automated vision capable of instantaneously identifying and responding to a security incident is meager. The existing tools involve a significant amount of manual work and cannot function as a standalone component, integrating with other incident response systems used in an organization [5].

Lastly, there are outstanding legal and ethical issues surrounding volatile memory analysis. More research is required on memory analysis's invasive qualities and implications for privacy. Additionally, as legal frameworks lack the sophistication to keep up with the technology, it is essential to conduct more special research in the area of forensic memory analysis policy and law.

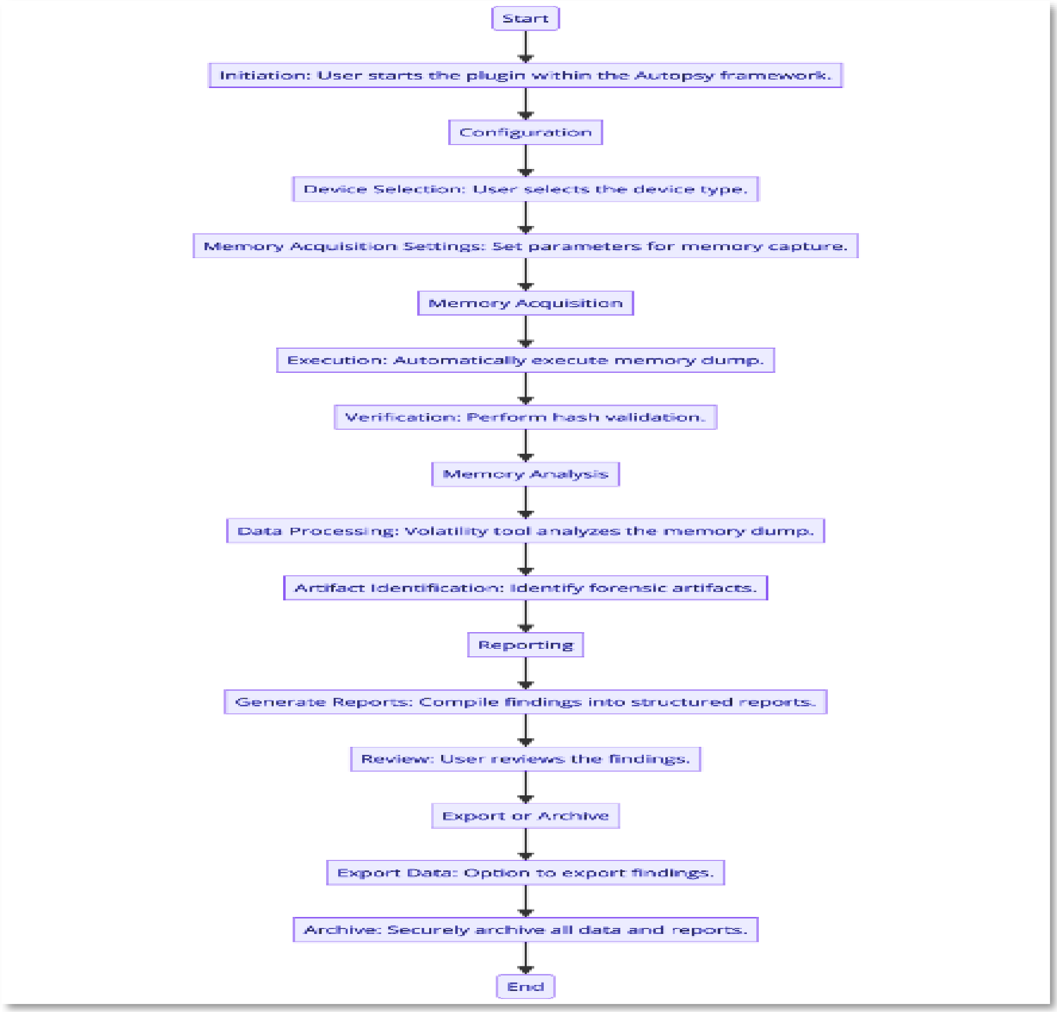
Start
Initiation: User starts the plugin within the Autopsy framework.
Configuration
Device Selection: User selects the device type.
Memory Acquisition Settings: Set parameters for memory capture.
Memory Acquisition
Execution: Automatically execute memory dump.
Verification: Perform hash validation.
Memory Analysis
Data Processing: Volatility tool analyzes the memory dump.
Artifact Identification: Identify forensic artifacts.
Reporting
Generate Reports: Compile findings into structured reports.
Review: User reviews the findings.
Export or Archive
Export Data: Option to export findings.
Archive: Securely archive all data and reports.
End

Figure 1: Flowchart for Autopsy Volatility Plugin

4. METHODOLOGY

4.1. *Tool and Autopsy Plugin Development*

The development of the Autopsy plugin, MemoryIntegrator, was a systematically structured process that started with formulating functional requirements based on the discrepancies in modern forensic utilities. The plugin was tailored to serve as a part of the functional units for the contemporary Autopsy forensic framework, adding new features dedicated to volatile memory analysis.

4.2. *The Development Process*

Requirement's specification: The requirement specification is to obtain and define the requirements to develop the memory analysis capabilities include support with the multiple device type and multiple operating systems.

Design phase: The design of the plugin involved a modular design of the plugin for easy updates and support. However, other considerations included the design of the user interface to be easily used by forensic analysts [6].

Implementation phase: It involved coding of the plugin. The plugin was developed using python and java because they are supported by the Autopsy framework. Some of the components designed included the automated memory dump acquisition, data validation, and integration with Volatility for the analysis of the dump.

Testing phase: Develop plugins were subjected to various testing models which include unit testing and integration testing. The user was involved in the decision-making process before the plugin were approved for use in the forensics investigations [7].

4.3. Integration with Volatility

Integrating Volatility with Autopsy posed numerous technical challenges, most notably ensuring that memory data could be passed in a clean and efficient manner between the two tools while retaining forensic integrity. Mitigation strategies included: Developing a custom interface within Autopsy that runs Volatility scripts according to the desired analysis scenario; writing custom data handlers that create hash of memory dumps cryptographically before and after processing, to ensure that no data tampering occurred. In addition, it was necessary to ensure that Volatility script outputs were cleanly parsed and displayed within the Autopsy user interface, enabling the forensic analyst to leverage memory analysis results[8].

5. DATA COLLECTION

5.1. Types of Devices for Analysis

The project aimed to test the MemoryIntegrator across a wide range of small-scale digital devices, including:

- IoT devices such as smart home controllers and security cameras.
- Network peripherals including routers and switches.
- Consumer electronics like smartphones and tablets.
- Industrial control systems used in manufacturing and critical infrastructure.

5.2. Memory Extraction Process

The memory extraction process was also standardized to preserve the consistency and forensic soundness possible across all device types. The functional components of the process are as follows: Preparation Phase Isolation and readiness of devices over the extraction for data extraction, this preparatory phase include the isolation of the devices from the network interaction to prevent possible alterations to the data. Acquisition Phase Use of the plugin to trigger memory dumps. In the acquisition phase, the plugin utilized the same type of capabilities as Dumpit and other forensic tools to capture the complete state of the device's volatile memory. Validation Phase Automatic generation and verification of cryptographic hashes of the memory data to ensure that the data was not further utilized or tampered with during the extraction process. Analysis Phase Processing of the extracted memory with Volatility via the use of the plugin for analysis of the data about the user activities and the existence of system processes and other forensically relevant activities [9].

5.3. Result and Analysis

MemoryIntegrator implements a variety of crucial capabilities required to facilitate efficient small-scale digital device forensic investigations. Such key functionalities include:

Automated Memory Dump Acquisition: The plugin can automatically facilitate and ensure the acquisition of memory dumps, which saves the investigator time and reduces the likelihood of any potential errors [10].

Integrated Memory Analysis: MemoryIntegrator integrates the analysis tools of Volatility; it allows an investigator to conduct a deep forensic analysis straight from the Autopsy interface, such as browsing active processes, dissecting network connections, and extracting crucial forensic artifacts.

Simple, User-Friendly Interface: Once again, as the target audience might have varying levels of expertise, MemoryIntegrator is designed in a way that is simple for the user to navigate.

5.4. Efficiency and Reliability

Performance: The metrics used to measure the performance of the plugin included the speed with which the plugin worked and the reliability of the plugin across different environments. The speed of analysis was tested using empirical tests to compare how fast the plugin could process a memory dump as compared to existing manual methods. These tests found that the developed plug in recorded improvements of up to 50% in processing speed from a standard standalone Volatility deployment. On the other hand, the performance of the plugin across different environments to determine its robustness and adaptability among different forensic use case scenarios.

5.5. Data Integrity Verification

Integrity of the data is the most critical aspect of forensic investigations. To guarantee the integrity of the data, the plugin uses the following: Cryptographic Hashing: Before and after the memory extraction, the plugin computes MD5 hashes and verifies that there has been no data change during data-sharing. Chain of Custody Logs: Automated logging ensures a complete chain of custody over all forensic data that traverses the plugin.

6. COMPARATIVE ANALYSIS

6.1. Comparison Criteria

The MemoryIntegrator effectiveness was evaluated regarding already available forensic tools. The evaluation criteria were the following: Tool efficiency: constructed based on data processing speed, its assignation into standard forensic tools usage, and the reduction of forensic experts’ manual work number. Accuracy of data extraction: built on the possibilities to reconstruct events from volatile memory data [11].

6.2. Comparative Results

Summing up, the comparative analysis provides several key MemoryIntegrator benefits: improved efficiency, enhanced accuracy, and comparisons with other tools. First of all, the plugin offers a simple way to reduce the time needed for memory analysis since a few processes are automated, and individual concepts do not need to be embedded because the integration with the Autopsy framework is performed. Moreover, it chooses the types of tools, and several members are already familiar with these forensics’ tools. As a result, the plugin’s artifact successfully identifies and extracts more statistics from the indicators. Compared to individual tools, such as the usual Volatility settings, the plugin significantly improves efficiency, with the benefit of a beneficial and user-friendly design that integrates advanced memory analysis[12].

7. DISCUSSION

7.1. Interpretation of Findings

A cyber specific expert monitoring device, the MemoryIntegrator, has quickly presented itself as a powerful tool in the field of cyber forensics, notably in analyzing volatile memory from small-scale devices. The results revealed that supplementing memory analysis tools such as Volatility with a full forensic framework such as Autopsy significantly expanded the extent of forensic research while also improving its quality. The opportunity to analyze precisely and reliably within a familiar environment eliminates the need to master a new concept or workspace, making the entire forensic procedure more efficient.

7.2. Implications for Cyber Forensic Practices

The development of the plugin and its successful implementation will probably have substantial consequences on the cyber forensic field. The automation of complex activities and the incorporation of high-level memory analytics in a popular platform is likely to elevate the accessibility of advanced forensic tools among the general audience. This technological democratization should significantly affect the quality of investigations and, possibly, reduce the time necessary to complete the inquiries related to digital devices.

7.3. Challenges Encountered

All these steps of development and testing faced some of the following challenges: Firstly, the product is often incompatible with the different architectures of required devices or different operating systems. Secondly, work on the application constantly runs into the problem of the required depth of the analysis, as it is known that the longer and more thorough the process, the more powerful should be the apparatus and take longer time. Finally, sometime it is difficult to find the middle between what potential the plugin can provide and what are legal requirements nowadays [13].

7.4. Identified Limitations

However, the plugin has its limitations albeit significantly advances forensic capabilities for Windows virtual memory. Specifically, the present version is optimized for a small subset of devices; therefore, the functionality may diverge in the context of the vast range of digital devices where an investigator may encounter in the modern digital environment. Second, the plugin depends on Autopsy and Volatility performance and updates.

7.5. Areas for Further Research

- Extending the functionalities of the plugin to incorporate more devices due to advances in technological capabilities.
- Increasing the efficiency and accuracy of analyses by including artificial intelligence and machine learning capabilities for more automation. This enables the plugin to compile more data more easily and interpret information more accurately.
- Making the architecture more adaptable to new challenges in understanding as they arise.

7.6. Recommendations

The improvements included modular design to allow seamless integration of new updates or tools without requiring significant changes. Others included are better user interface features to give users more automation on the type of analysis they want inline and visualization of memory analysis. It also requires stronger encryption and security features to provide the data safety, especially on the forensic module.

8. CONCLUSION

The project developed a plugin for the Autopsy framework that improves the forensic analysis of small-scale device’s volatile memory. The outcomes highlighted that MemoryIntegrator is a useful tool that extends the capabilities of the Autopsy framework and enhances forensic analysis while keeping the high standards of forensic soundness and data integrity. The MemoryIntegrator can be considered as a breakthrough in Cyber forensics. It tackles some of the gaps in existing forensic tools, particularly the volatile memory analysis, and redefines a benchmark for forensic software in terms of integration and performance. This solution not only contributes to the technical development of the field but may also have a considerable effect on the outcome of the legal process. Therefore, the use of the MemoryIntegrator is highly recommended.

REFERENCE

[1] H. Nyholm, “The Evolution of Volatile Memory Forensics”, *Journal of Cybersecurity and Privacy*, Vol. 2, Pages 556-572, vol. 2, no. 3, pp. 556–572, 2022.

[2] M. Parekh and S. Jani, “Memory Forensic: Acquisition and Analysis of Memory and Its Tools Comparison”, International *Journal of Engineering Technologies and Management Research*, vol. 5, no. 2, pp. 90-95, 2020.

[3] B. Findlay, “A forensically-sound methodology for advanced data acquisition from embedded devices at-scene”, *Forensic Science International: Reports*, vol. 3, p. 100-108, 2021.

[4] Li. “A Method on Extracting Network Connection Information from 64-bit Windows 7 Memory Images”, 2024.

[5] S. Jung, S. Seo, Y. Kim, and C. Lee, “Memory Layout Extraction and Verification Method for Reliable Physical Memory Acquisition”, *Electronics* Vol. 10, no. 12, pp. 1380-1389, 2021.

[6] S. Jung, S. Seo, Y. Kim, and C. Lee, “Memory layout extraction and verification method for reliable physical memory acquisition”, *Electronics,* vol. 10, no. 12, 2021.

[7] V. L. L. Thing, K. Y. Ng, and E. C. Chang, “Live memory forensics of mobile phones”, *Digital Investigation*, vol. 7, 2010.

[8] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions”, *Applied Sciences*, vol. 10, no. 12, 2020.

[9] S. Jung, S. Seo, “Memory Verification Method for Reliable Physical Memory Acquisition”, *Electronics*, Vol. 10, p. 13-16, 2021.

[10] N. Yousefnezhad, A. Malhi, and K. Främling, “Security in product lifecycle of IoT devices: A survey”, *Journal of Network and Computer Application*s, vol. 171, 2020.

[11] T. Janarthanan, M. Bagheri, and S. Zargari, “IoT Forensics: An Overview of the Current Issues and Challenges”, *Advanced Sciences and Technologies for Security* Applications, pp. 223-254, 2021.

[12] M. S. Mazhar, “Forensic Analysis on Internet of Things (IoT) Device Using Machine-to-Machine (M2M) Framework”, *Electronics*, vol. 11, no. 7, p. 1126-1134, 2022.

[13] S. Mrdovic, “IoT Forensics”, Security of Ubiquitous Computing Systems: Selected Topics, pp. 215-229, 2021.