STM JOURNALS

Journal of
Polymer & Composites

ISSN: 2321-2810 (Online)
ISSN: 2321-8525 (Print)
Volume 12, Special Issue 3, 2024
DOI (Journal): 10.37591/JoPC

http://engineeringjournals.stmjournals.in/index.php/JoPC/index

Review JoPC

3D Printing for Polymer Science Visualization

Princy Tyagi

Abstract

The burgeoning field of 3D printing offers exciting possibilities for various scientific disciplines. This paper explores the potential integration of 3D printing technology within the realm of polymer analysis. While the core focus of memory forensics investigations lies in digital forensics, the concept of 3D printing complex data structures presents intriguing possibilities for the visualization and communication of findings in polymer science. Here, we propose a future research avenue where 3D printing could be employed to create physical representations of intricate polymeric structures derived from analytical techniques. This could revolutionize the communication of complex polymer morphologies, enhancing collaborative research efforts and potentially leading to advancements in polymer design and characterization. The information technology landscape is undergoing a period of explosive growth. Data processing capabilities have surged in both speed and accuracy, while storage capacities have ballooned, allowing for the easy accumulation of vast troves of digital information. This accessibility, however, presents a double-edged sword. While it facilitates information sharing and analysis, it also creates tempting opportunities for criminal activity. Sensitive data, like passwords and credit card PINs, becomes a target for malicious actors. As a result, the onus falls on security professionals to safeguard this critical information. This review will explore the various tools and techniques available for conducting memory forensics investigations on Windows systems. We will examine both open-source and commercial solutions, evaluating their strengths and limitations. Furthermore, the paper will discuss the potential of integrating 3D printing technology into the digital forensics' workflow. By creating physical representations of complex data structures extracted from memory, 3D printing could potentially enhance the visualization and communication of forensic findings. Finally, the paper will conclude by proposing avenues for future research in the field of memory forensics. This includes exploring the integration of artificial intelligence and machine learning for automating memory analysis tasks, as well as investigating the feasibility of using advanced memory acquisition techniques for real-time incident response. By fostering innovation in these areas, we can empower digital forensic investigators to more effectively combat cybercrime and safeguard sensitive data.

Keywords: Polymer, Memory forensics, Computer Forensics, Chemical imaging. 3D Printing.

INTRODUCTION

Computers have become an essential component of our everyday routines, facilitating activities such as paying bills, conducting bank transactions, managing emails, and storing personal information. With this increase in data volume on computers, there has been a corresponding rise in crimes related to digital activities. In today's landscape, the storage capacity of hard disks has dramatically increased, with 500 GB being the norm in modern computers. Consequently, there is a need to enhance the forensic capabilities of existing tools and procedures to effectively analyze such vast amounts of data. Similarly, the RAM in modern computer systems is also

***Author for Correspondence**
Princy Tyagi

Assistant professor, Computer Science & Engineering, Swami Rama Himalayan University Dehradun, Uttarakhand, India

Received Date: March 01, 2024
Accepted Date: July 16 2024
Published Date: July 18, 2024

Citation: Princy Tyagi. 3D Printing for Polymer Science Visualization. Journal of Polymer & Composites. 2024; 12(Special Issue 3): S96–S101.

experiencing exponential growth, with 2 to 4 GB being the standard in end-user computers. In certain situations, crucial evidence can only be found in RAM. For instance, malware programs that execute directly in memory may leave traces that are vital for digital crime investigations. Therefore, it is imperative not to overlook the significance of RAM, despite its increasingly large capacities, in the realm of digital crime investigation.[1].

Memory forensics, like other forensic disciplines, concentrates on recovering relevant information that can be used as evidence in criminal inquiries [2]. The primary data item to collect in a system is the content of RAM. Unlike other branches of digital forensics, memory forensics is still developing. Its objective is to retrieve data from the RAM of a computer [3].

STATE OF ART RAM FORENSICS

Numerous research efforts have been conducted in the field of RAM forensics. Lee and colleagues have authored multiple papers discussing the collection and examination of memory and page files. They successfully extracted usernames and passwords from RAM through keyword searches. Their findings suggest that with the increased size of RAM, there is a greater chance of discovering confidential data in the page file.[1]. In 2006, Deutsche Telekom AG [4]and its team members introduced the idea involves scans to identify processes and threads within Windows memory dumps. They highlighted that Microsoft Windows NT and its legacy systems are built on object-oriented principles. Consequently, any resource vital to the operating system is represented as an object containing data and methods for its management. Processes and threads belong to a category of object classes. The most crucial and frequently accessed objects, such as process and thread objects, are stored in the non-paged pool, indicating they permanently occupy RAM. [1]. Qian Zhao and Tianjie in [3] extracted some critical information from RAM like username and passwords system running under Windows XP. They considered RAM, page file, hibernation file and crash dump in their experiment. In research [5, 6] they extracted confidental data from RAM and the page file of a live system operating under the Windows XP OS. They scrutinized various states of the computer system. i.e ready state, steep state, hibarnation mode, hard reboot and soft reboot are investigated running different applications [2]. Hejazi, S. M., C. Talhi, and M. Debbabi[7] discovered the sensitive data in RAM like process ftp.exe on the list of process that were running at the time of imaging. They listed all DLL files imported by these processes and all imported functions. Furthermore, they identified the stack for the thread of execution and inspected addresses on the stack to identify return addresses [8]. Mariusz Burdach [9] detected and recovered file executed by intruder and all user mode process for the RAM.

MEMORY ACQUISITION METHODS

Acquisition of memory is one of the main factors when determining the reliability of evidence in memory. Two approaches is used to acquisition of memory contents. Software-based and hardware-based methods are utilized. Hardware-based memory acquisition is favored because depending solely on the OS and software applications to provide reliable data may not be adequate. Unlike software-based methods, hardware-based acquisition does not utilize system memory during the acquisition process. This approach reduces the risk of an attacker altering the procedure to generate unreliable data. Carrier and Grand in 2004 introduced the idea of dedicated PCI expansion card. The advantage of this idea is memory is not modified during acquisition process and disadvantage is devices have to install prior to incident [1].

Hardware Based Memory Acquisition

Fire wire

It is introduced by Apple Computer's (version IEEE 1394). It utilizes the High-Performance Serial Bus to join devices. The FireWire port enables access to RAM without disrupting the host OS. This form of RAM access is known as direct memory access (DMA). [1].

Virtualization

It involves running a guest operating system (OS) within a virtual environment managed by a host operating system (HOS). This product has the capability to capture RAM called snapshot saved as ". vmem" file in host operating system. When a snapshot is taken all activates of guest is captured and saved as a snapshot.

Crush Dumps

Crash dumps are a feature of Windows systems, commonly referred to as the "blue screen of death" (BSoD). When a hardware problem or driver conflict occurs, the system may display a blue screen and require a restart after fixing the error. Throughout this process, the contents of RAM are stored in the system's page file. Additionally, A crash dump can be generated by pressing a specific sequence of keys. It's crucial to mention that this feature is disabled by default. [1]

Hibernation File

During hibernation mode, the contents of RAM are saved on the hard drive in a compressed Microsoft proprietary format prior to the system being shut down. Upon system restart, the boot loader searches for the hibernation file. If found, the system reverts to its previous state as it was before shutdown. This hibernation file can be utilized for analysis after conversion into a readable format.

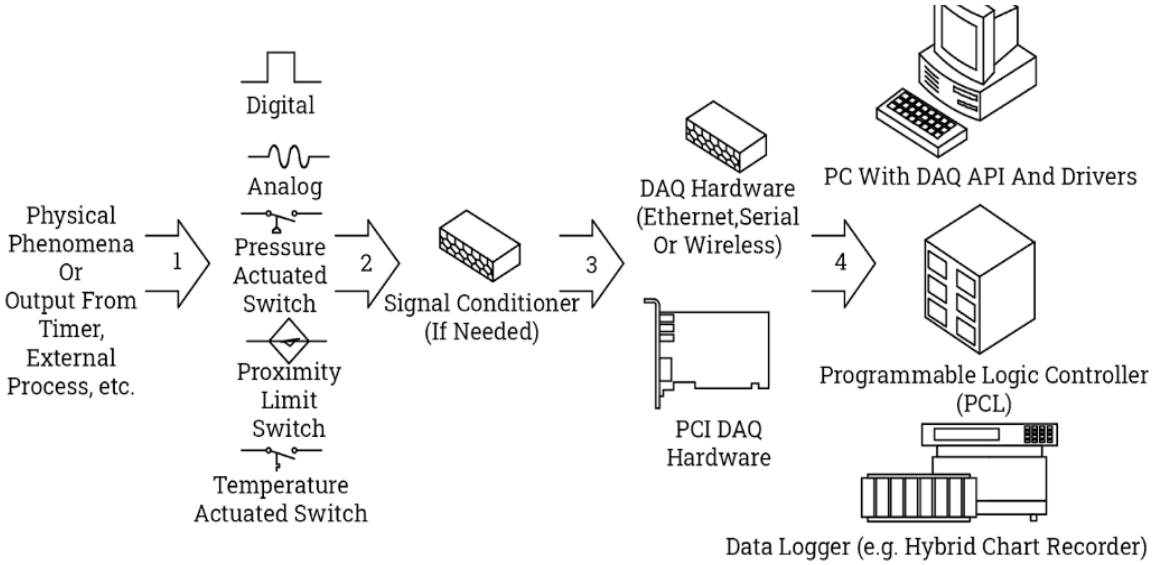

Figure 1. Hardware Based Data Capture.

Software Based Memory Capture

Software-based solutions have the potential to alter data during the collection process. Adding new software may change data that is currently stored in memory due to the volatile nature of RAM. Certainly, it is not ideal for forensically sound acquisition. It needs more consideration, particularly when evidentiary rule and standard applied [1]. Tools for software-based acquisition.

KnTDD

It is primarily utilized for extracting RAM and is developed by GMG Systems. KnTDD is included in the Knt Tools kit and is compatible with both Windows 32-bit and 64-bit systems. It saves the acquired memory image locally, on USB drives, or through network connections. One disadvantage of using this tool is that it requires loading into memory when acquiring images of RAM.

Data Dumper (DD)

It is a Linux utility program crafted to capture RAM. images as well as hard disks. A modified version of DD for the Windows platform has been developed by GMG Systems. This forensic utility is freely

available. However, it's important to note that Microsoft no longer provides direct access to memory from the user end since Windows Service Pack 3. Access to memory is restricted to kernel drivers only. [2].

Memory DD

It is also a freely accessible tool for capturing RAM (Random Access Memory) on Windows systems. Memory DD retrieves a forensic image of RAM and stores it as a raw binary file from the targeted system. The acquired image can subsequently be analyzed using an external tool. To maintain data integrity, it uses MD5. It is nice tool but cannot say surely about its impact on memory during acquiring process.

Nigilant 32

Developed by Agile Risk Management, this tool enables investigators to image memory, preview hard disks, and capture snapshots of active Processes and accessible ports on the target system. Agile asserts that its tool has minimal impact during the memory acquisition process [10].

ProDiscover IR

Technology Pathway's forensic acquisition tool, ProDiscover, serves as an incident response tool, allowing investigations of live systems across the network. It permits imaging of RAM or hard disks. However, using this tool necessitates installing a server the software installs an applet on the target system before commencing the acquisition process via removable storage media such as USB or CD/DVD. This prerequisite might make the tool less appealing for acquisition, hence making it more suitable for corporate environments. [10].

Win32 DD

This is a free kernel-level tool created to capture images of RAM (RAM). The tool asserts its ability to acquire RAM (RAM) images on all Win32 systems. However, it does not explicitly state support for 64-bit OS. [11].

EnCase

This is a commercial tool that offers comprehensive solutions for acquiring and analyzing RAM.

MEMORY ANALYSIS

All applications and processes simultaneously running utilize memory as a gaming table. Data must be presented at this table in order to participate in the game. This information encompasses a wide range of data, including but not limited to user credentials, passwords, executable code of processes, data files accessible by processes, and URLs obtained through web browsers. These categories could be applied to data that is stored in memory.

- Meta data
- Files
- Sensitive information
- Case-Irrelevant data

When analyzing RAM (RAM), establishing correlations between collected evidence can strengthen the reliability of outcomes or even question suppositions. [11]. To locate and extract sensitive information from RAM, there are two types of tools available: commercial tools and free tools.

Commercial Tools

WinHex

At its essence, WinHex is a universal hexadecimal editor created by X-Ways Software Technology. It acts as a valuable tool for seasoned forensic examiners to authenticate data obtained using other applications. Furthermore, it is beneficial for students studying data structures and file systems. WinHex

enables in-depth examination of digital evidence through its data interpreter and template features. While WinHex is a commercial tool, the evaluation version provides sufficient capability to analyze memory and disk images from most Windows platforms. [2].

Forensic Toolkit

Developed by Access Data Corporation, it comprises several components such as FTK Imager, Known File Filter (KFF), and Registry Viewer. Each of these components can be installed independently. FTK is capable of both imaging and acquisition tasks. It also allows searching and previewing of evidence. FTK can enumerate all active processes, including those hidden by rootkits, along with their corresponding DLLs. It includes a robust index and live search feature. The live search feature permits a detailed comparison of items with search terms specified by the investigator, while the indexed search employs a powerful search engine. [2].

KnTList

The KnTList tool, developed by GMG Systems, is restricted to some bodies only. It is included in the Knt Tools package and offers both acquisition and analysis capabilities for RAM. It can construct virtual address space, Meta data and other processes. It produces output in both text and XML format [2].

Free Tools

Volatility

It is a set of free software tools created in Python for the study of RAM. Volatile systems invented volatility. Any platform with Python currently installed can use it. The utility works with Windows 32-bit, Cygwin, and Linux machines. Volatility, according to its specifications, has the capability to extract various types of data from memory images. This encompasses details “such as running processes, process addressable memory. It supports various sample formats, including DD, Hibernation, and Crash dump.

Memoryze

From MANDIANT, it is a free memory analysis tool. On Windows 32-bit, memorize can analyse RAM in both active and offline states, much as it does for hard disc images. It is capable of listing the virtual address spaces of all processes while enumerating all currently active processes, even those concealed by rootkits. Show every string in RAM, broken down by process.

PTFinder (Process and threat finder)

It is a freely available tool developed by Andreas Schuster for analyzing RAM on the Windows platform. PTFinder, is designed to list processes from within Windows memory dumps. It supports various dump formats and offers output in both text and XML formats.

Sleuth Kit (Digital forensic toolkit) and Autopsy

It is a compilation of open-source tools, with Autopsy serving as its browser-based graphical user interface (GUI) developed by Brian Carrier for conducting disk-based examinations. The tool provides cross-platform compatibility. Its key functionalities include findings for deleted files, analyzing the file system and metadata, as well as detecting malicious programs. [12-13]

CONCLUSION

Advancement in technology increases new and exciting challenges. It also leads to more appropriate solutions. The increasing capacity of components of computer system such as hard disk and RAM, made difficult for an investigator to find digital evidence from these important sources. So the tools and techniques used in present scenario needs more consideration for development of efficient tools and techniques for digital investigation.

REFERENCES

1. Ankam AK. Implementation of a Windows Tool to Conduct Live Forensics Acquisition in Windows Systems. Diss. Texas A&M University. 2012.
2. Wagner J, Rasin A, Grier J. Database forensic analysis through internal structure carving. Digital Investigation. 2015 Aug 1;14:S106-15.
3. Zhao Q, Cao T. Collecting Sensitive Information from Windows Physical Memory. J. Comput.. 2009 Jan 1;4(1):3-10.
4. Schuster A. Searching for processes and threads in Microsoft Windows memory dumps. digital investigation. 2006 Sep 1;3:10-6.
5. Mann HK, Chhabra GS. Volatile memory forensics: a legal perspective. International Journal of Computer Applications. 2016;155(3):11-5.
6. Prakash V, Williams A, Garg L, Savaglio C, Bawa S. Cloud and edge computing-based computer forensics: Challenges and open problems. Electronics. 2021 May 21;10(11):1229.
7. Hejazi SM, Talhi C, Debbabi M. Extraction of forensically sensitive information from windows physical memory. digital investigation. 2009 Sep 1;6:S121-31.
8. Skadron K, Ahuja PS, Martonosi M, Clark DW. Improving prediction for procedure returns with return-address-stack repair mechanisms. InProceedings. 31st Annual ACM/IEEE International Symposium on Microarchitecture 1998 Dec 2 (pp. 259-271). IEEE.
9. Hausknecht K, Foit D, Burić J. RAM data significance in digital forensics. In2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2015 May 25 (pp. 1372-1375). IEEE.
10. Eoghan C. Tool review–Winhex Digital Investigation. Issue. 2004;2:114-28.
11. Hausknecht K, Foit D, Burić J. RAM data significance in digital forensics. In2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2015 May 25 (pp. 1372-1375). IEEE.
12. Vázquez JA, Casteleiro-Roca JL, Jove E, Zayas-Gato F, Quintián H, Calvo-Rolle JL. Data collection description for evaluation and analysis of engineering students' academic performance. InInternational Conference on EUropean Transnational Education 2020 Aug 15 (pp. 317-328). Cham: Springer International Publishing.
13. Kechagias JD, Ninikas K, Vakouftsi F, Fountas NA, Palanisamy S, Vaxevanidis NM. Optimization of laser beam parameters during processing of ASA 3D-printed plates. The International Journal of Advanced Manufacturing Technology. 2024 Jan;130(1):527-39.

