International Journal for Electronic Crime Investigation

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

DOI: https://doi.org/10.54692/ijeci.2024.0803208

Research Article

Vol. 8 issue 3 Jul-Sep 2024

Live Memory Forensic: Capture and Analyzing Volatile Data

Rabia Mehmood and Zohaib Ahmad
Department of Computer Sciences, COMSATS University, Lahore
Corresponding author: rabiamehmoodciit@gmail.com

Received: Aug 08, 2024; **Accepted:** Aug 28, 2024; **Published:** Sep 12, 2024

ABSTRACT

As almost 90% of malware is resident in memory, live memory forensics is an essential part of cybersecurity. Live memory forensics refers to the process of analyzing computer RAM or volatile memory (which is lost after rebooting) while the computer is running. This article provides depth on live memory forensics, which is key in the detection and analysis of cyber threats and forensics investigations. Case studies and actual events demonstrate how this method can detect unauthorized access and discover hidden malware, which will help law enforcement investigators. The practical uses of Live Memory Forensics are illustrated using real world examples. Currently, live memory forensics are faced with the temporal nature of volatile data, other technical challenges, the instantiation of indirect data related to data privacy, and evidence handling problems. The paper emphasizes the importance of moral attitude and careful handling of data to keep the forensic process incorrupt. Investigators and cybersecurity professionals should now have a good understanding of live memory forensics and how to utilize live memory forensics to enhance security across borders, not just as a detective technique.

Key words: malware, Volatility, FTK Imager, Live Memory Forensics, incorrupt, data privacy, evidence handling.

1. INTRODUCTION

However, live memory forensics is the approach used to capture and inspect the temporary data stored in a computer's RAM (Random Access Memory) when the system is up and running [1]. This type of forensics allows the researcher to capture a snapshot of the current state of the system, with all processes active, modules loaded, user interactions and network connections. Memory Captured RAM is used for storing pieces of information the computer needs while running, like open files and running software [2]. Unlike data stored on nonvolatile storage such as hard drives, the data in RAM is lost when the system is powered off, which is why it is memory capture is crucial for preservation of temporary data. Volatile data refers to data that is stored temporarily in a computer system's Random Access Memory (RAM). Memory/memory utilization/CPU/memory/CPUS tats/active applications, threads and system processes, Sessions and connection of a network, Operating System Functionality and Transient Storage. Volatile data is transitory, meaning it is available only while the system is in operation [3]. Typically, this data is lost when the system is shut down or rebooted, which is why we need to capture the live data during search/investigation. Importance of Volatile Data in Digital Investigations: In numerical surveys, volatile data is important for a few reasons: Transactional Awareness: Transitional data provides an instantaneous snapshot of the operations running on a system, allowing researchers to identify what was running on the machine at the exact moment of capture. This includes monitoring user activity, network communication and the process runtime. Which would tip them off to unauthorized access. Advanced threat detection: Advanced threats such as rootkits and malware often reside in memory and evade discovery by traditional file-based antivirus scans [4]. Researchers can investigate these in memory threats which do not appear on hard drives by analyzing volatile data [11]. Malevolent actors also hide their activities, either throughin memory execution or code injection. Such unseen actions can be captured using Live memory forensics, which examines the contents of RAM, including hidden processes and injected code. Sensitive Data Retrieval: Sensitive data, including encryption keys, decrypted content, and passwords, often resides in memory [5]. Retrieval of this data can be critical for determining the magnitude of security incidents, recovering ransomware data, and identifying compromised credentials. This means that while using the exec option allows copying the memory through every exec call because it saves the processor state and system setup (acpile polled, for instance), volatile data covers other data related to the exact state of the system: system configurations, memory mappings, kernel internal structures. This data helps forensic experts to comprehend the network implementations where an assault took place and to evaluate the overall damage to the system(ii) Capture app install | the full hardware property data. It is required to track the current information only through the given tools, we can get the data. Signs because live memory forensics is

important: Live memory forensics is important for locating indicators that are not even stored on a hard disk. Hoo Tem Forest Encapsules about Traditional Forensic is defined by a scope that goes back to the age of when. Low levels, in particular, include the existence of data in the file system and various file systems and the detection of random data. However, many crucial pieces of evidence exist only in RAM, which dissipates when the computer is powered off. Researchers are, therefore, able to analyze or take snapshots of live memory to: Detection of active rootkits & malware: Identify data exfiltration attempts and immediate network connectivity, Check system interactions & user interaction, this form of live memory forensics is a live investigational procedure in the modern digital obehilton. It brings insights that contrast traditional forensic analysis, enriching a theoretical approach to cyber incidents.

2. METHOD AND MATERIAL

2.1. Live Memory Forensics Basics

Live memory forensics is a sub analysis for digital forensics in which the volatile data resident in a computing system is analyzed and extracted while the system is still running. This provides researchers with a snapshot of the system's current state in real time and captures important information that may not persist on the disk.

2.2. Volatile Data

The data that is stored temporarily in the RAM (Random Access Memory) of a computer is referred to as volatile data. It holds information on loaded modules, network connections, system processes, user activities, active processes and the temporary files used by the Operating System. The volatile one is data available in memory only, and it is lost when the system loses power or restarts. It is a solution that means the data is stored on nonvolatile storage devices like hard drives or SSDs.

2.3. Importance of Digital Investigations

Live memory forensics is necessary in digital investigations because it can acquire live artefacts that are critical for the detection of malicious activities and for understanding system interactions. Through the examination of volatile data, forensic experts can identify open network connections, memory resident malware, and live processes that old antivirus programs could miss. This forensically sound scanning triggers the preservation and extraction of vital evidence, which constructs a timeline and restores digital events and prevailing lawful records.

2.4. Tools and Techniques

Researchers make use of specific tools and techniques to carry out live memory forensics in the most optimum way. Volatility Framework isolates forensic traces in volatile memory [6], memory imaging and memory dump analysis for controlling tools. It also supports many operating systems (architectures) That give forensic experts great power to analyze memory fillings and find hidden processes. Remembering, the different noticeable instruments offer progressed memory examination functions that are more suited for free examination than custom personalized memory procurement for complex forensic circumstances. Redline, founded by FireEye [7], provides automated memory forensic analysis and detection of malicious software and activity, allowing

cybersecurity incident response and operations teams to perform rapid response.

2.5. Live Memory Forensics Methodologies

The technique of performing live memory forensics [8] is made up of multiple important steps. Forensics analysts first record a memory dump or image with tools like Volatility Framework or FTK Imager. The method is responsible only for capturing the live memory data, which is stored in the Eccentric RAM, including the system artefacts, network connections, processes, etc. The researcher then performs detailed memory dump forensics by identifying the IoCs mentioned above and producing a timeline using signature based scanning and string searching [10]. This method allows analysts to recreate online interactions, identify security violations, or collect proofs needed for cybercrime investigations.

2.6. Applications in Cybersecurity

Live memory forensics is a very powerful tool for incident response and Threat detection in Cybersecurity. By analyzing and collecting volatile data live, cyber security professionals can rapidly identify and remediate incidents such as APTs (Advanced Persistent Threats), security incidents, data breaches, and insider threats. This pragmatic measure strengthens the ability of the organization to recover from cyber threats quickly and reduce the impact of security breaches on critical systems and data. Moreover, live memory forensics enables practical threat hunting activities by assisting analysts in uncovering and mitigating early-stage threats before they escalate into silver platter attacks.

2.7. Challenges and Considerations

As with any great reward, live memory forensics is not without its own set of challenges and considerations. If data is located in RAM, volatile data can be quickly lost if it is not detected in time. Furthermore, ethical and legal considerations also make it necessary for forensic professionals to convey sensitive standards of privacy and indication heading. Moreover, the sophistication of these memory structures and the sheer amount of data the investigations produced created unique challenges and required scientific abilities and understanding.

3. SIGNIFICANCE

Live memory forensics is an important focus of Cybersecurity and digital forensics. It provides a snapshot of data in a computer's RAM without needing to cease the system. The technique is important for cyber security people and digital forensic researchers to improve digital investigation, malware analysis, and incident response.

3.1. Incident Response

Live memory forensics is valuable in incident response scenarios with the need for quick action. Real time analysis and capture of volatile information are needed to help cybersecurity teams identify network connections, memory resident threats, and active processes during a security breach or suspected malware attack. Such a practical methodology enables organizations to surround the event on the go without letting it escalate and without risking any sensitive data.

By analyzing the volatile data in the RAM, detectives can piece together a sequence of events before and during the incident. This skill is invaluable when considering event likelihood, understanding attackers' entry methods,

or communicating effective response measures. Developing an analytical model that can quickly identify the event allows a company to isolate it before it disrupts the normal business process, resulting in the smallest possible economic and reputational loss.

Live memory forensics is a very integral part when it comes to the analysis of malware as it works especially well in the case of hunting memory resident complex threats. Traditional malware detection methods, like signature-based antivirus solutions or static file analysis, can easily miss memory resident malware that silently remains hidden while it performs its actions.

Forensic analysts learn live memory forensics tools to capture and analyze volatile memory. This lets them spot bad processes in action, help them abstract out IoCs, and track the malicious process as it performs its actions. By reverse engineering malware memory interaction, experts uncover the malware's persistence mechanism, command and control communication channels, and impact on the compromised environment.

3.2. Unauthorized Access Detection

They use live memory forensics to detect unofficial access attempts and internal threats. Monitoring memory actions in real time allows administrators to detect out of the ordinary user behaviour, unauthorized network connections, or unusual processes a signal of a security compromise. This security monitoring helps improve the cybersecurity posture by quickly identifying and responding to potential threats, which reduces the chance of data loss and insider attacks.

If an attacker demands temporary access which they do most of the time they need to run a process or two to execute a network connection, followed and usually partially littered with strange process executions or state sponsored memory feasting processes that linger in volatile memory and leave traces. Live memory forensics allows forensic experts to detect those traces and identify them to assess the potential and impact of unauthorized access events. Prompt ID and response to those events are needed to stop the bleeding, comply with regulatory requirements, and correlate to sensitive info and data exfiltration.

3.3. Applications of Live Memory Forensics

Live memory forensics serves as an important tool for collecting illegal evidence and reconstructing digital crime scenes in digital investigations. The volatility data surveillance with memory dumps allows forensic experts to establish timelines, reenact user action and search for malevolent elements. Crucial to legal records, this forensic evidence provides the physical evidence that will prove unauthorized entry, data exfiltration, or other cybercrimes leading to a long day in court as law enforcement carries out its exhausting role and ensures that accountability is procured.

Digital investigations frequently involve forensic analysts examining the system at a particular moment in time to piece together the sequence of events by which a threat actor carried out their actions. Live memory forensics allows us to capture a memory image of the system in a live state. It can be used in cases where a system is going to be shut down or rebooted, where evidence can

degrade in system memory. It integrates multiple related artefacts to support comprehensive investigations and comprehensive documentation of digital incidents to help make informed decisions and prosecution efforts.

3.4. Boosting Cybersecurity Level

Live memory forensics helps boost the cybersecurity level, providing visibility into real time data breaches and detecting threats proactively. By capturing and analyzing volatile data, organizations can take immediate action in incident response, including identifying the threat, preventing its spread, and preventing future attacks. By incorporating live memory forensics into cybersecurity procedures, incident response efforts become more robust, threat detection more precise, and key systems and data more resistant to the diverse swath of security threats that are now commonplace.

Leveraging live memory forensics proactively allows organizations to uncover and mitigate new threats instantly, shortening attacker dwell time on their networks and lessening the implications of security incidents. Some actionable insights that can be derived with the help of volatile data in real time include the ability to detect indicators of compromise (IOCs), catch stealthy malware infections that might go undetected otherwise, and help prevent exposure to attacks by unauthorized means before they eventually snowball into full blown breaches.

3.5. Understanding Tools and Techniques of Memory Capture

Memory images themselves are foundational to live memory forensics, the practice of reading volatile data from a computer's RAM during active operation. This section will present major tools for memory image capture and explore the roles they have in a digital investigation.

The FTK Imager is a tool that assists in capturing and analyzing disk and memory images created by the Access Data Team. It has an intuitive interface and works with a wide range of file types (DD (raw), E01 (forensic image), and AFF (Advanced Forensic Format)). With FTK Imager, forensic analysts can perform live memory forensics to /capture volatile memory snapshots with acquired active processes, network connections, and loaded modules.

To capture memory with FTK Imager, the examiner usually boots the application on the target system or remotely, chooses "Capture Memory," and then specifies the location and the desired output format. The solution pronounces a memory dump file containing important information, which can be analyzed to affirm evidence of manipulative activities or a system compromise.

Belkasoft Live RAM Capturer is a tiny, free, standalone executable that enables you to focus on obtaining live memory images in a condition as close to the original as possible, without even USB drives because the memory conservation feature is provided in the most similar way to a hibernation file on both 32 and 64 bit systems. Belkasoft Live RAM Capturer is widely known for its ability to guarantee flawless functionality and minimal system load, ensuring rapid and reliable acquisition of volatile data. Belkasoft Live RAM Capturer allows forensic specialists to create memory dumps of the working processes of the computer, as well as to obtain data on operating network connections and operating system registry records. Its

advanced memory acquisition techniques for data integrity allow full forensic analysis and evidence recovery by those trained in its use.

An open source Memory Dumper by Moon Sols is very popular among digital forensics investigators for capturing the memory of Windows operating systems. Its simplicity and reliability make it great for capturing memory snapshots in a live forensics scenario without disrupting the volatile memory state.

In general, a forensic analyst or IT security researcher will run the tool against a system of interest, providing a path for the output memory dump file, and letting it grab the contents of physical memory. The resulting file dump has some vital artefacts that can be analyzed using forensic tools to check for malware infection, unauthorized access attempts, or any other suspicious activities.

3.6. Choosing the Right Tools for the Right Jobs

While choosing a memory capture tool for live memory forensics, analysts look at many factors, such as target OS compatibility, Capture method, i.e., physical vs. virtual memory, preferences for output format, and, most importantly, integration capabilities with forensic analysis platforms. Every tool has its strengths and points to consider depending on the investigation requirements or type/characteristics of the target system.

Tools such as FTK Imager [9], Belkasoft Live RAM Capturer [12], and DumpIt are famous in the world of live memory forensics. They produce excellent results in acquiring and preserving volatile data for analysis. Their use allows forensic practitioners to collect the valuable evidence they need to build a case for legal action, respond to an incident, or take cybersecurity precautions.

4. STEP BY STEP CAPTURING OF VOLATILE DATA

Live memory forensics allows investigators to gather real time data stored in a computer's RAM while the computer is running. This step-by-step walkthrough illustrates how to use Volexity Capture to capture volatile data for forensic analysis safely and effectively.

4.1. Preparation and Planning

Target System Identification: Choose the target system from which you wish to acquire volatile data. If your remote access is needed, deploying Idea Scale V2 must be configured as a system and ready to go on the network.

Choose The Capture Tool: Select a memory capture tool like FTK Imager, Belkasoft Live RAM Capturer, or DumpIt [13] that is compatible with the target system and the investigation requirements.

Prepare Storage and Environment: Reserve adequate storage for the memory dump file to avoid interference during the capture process and ensure a safe and distraction free capturing environment.

4.2. Run Memory Capture

Start the Capture Tool: The capture method you selected will determine how you start the memory capture tool, either on the target or remotely (if the tool supports that and you have the necessary permissions).

Capture Settings Configuration: Use the below settings in the tool to configure the capture settings, such as where to select the memory (either

physical or virtual) to capture and what should be the output format and path for the memory dump file.

4.3. Start memory capture in the tool

Run the tool and take a snapshot of the volatile data stored in the system's RAM. The time the capture will take depends on the tool's memory size and efficacy.

4.4. Verify and Validate

Validate Data Integrity: Ensure that the collected memory dump file contains complete and correct volatile data of the target system.

4.5. Validate Against Source

The captured data should be compared to the live system to verify that the snapshot of memory correctly represents the system's state at that time.

Capture Details: Write down important information like the time of capture, the duration of capture, the tool used in the capture and any other information about the capture observations, system condition, etc.

4.6. Analyze and Interpret:

Forensic Analysis Tools: Move the memory dump file to a forensic analysis workstation with tools like the Volatility Framework, Magnet AXIOM, Encase Forensic, etc. These tools help in depth analysis and extraction of artefacts from the captured memory.

Retrieve Significant Artifacts: Extract and investigate artefacts from the memory dump file, such as active processes, network connections, loaded modules, set registry keys, and user actions. Spot any oddities or Indicators of Compromise (IOCs) that may suggest security attacks or evil activities.

Document Findings: Enter your findings in a structured way, including artefacts, time stamps and how they relate to the investigation. Keep clear and comprehensive logs to support forensic analysis and potential criminal proceedings.

4.7. Secure and Preserve

Protective Storage: Save the memory dump file and generated analysis in safe and controlled storage to avoid unauthorized tampering with the generated data.

Chain of Custody: Follow the chain of custody principles to ensure that evidence is preserved in a way suitable for use in court. Capture all handling and transfer activities of the memory capture and associated data.

5. Examine Captured Image and Memory

This is the most important phase in live memory forensics, and it allows forensic investigators to extract and interpret volatile data from dumped memory images taken from a live running system. This part details the process of memory dump analysis through Volatility and Rekall, providing the reader with the ability to perform some basic memory dump examinations, such as listing running processes, network connections, and other types of malicious indicators.

5.1. Using Volatility

Volatility is a popular open source memory forensics framework that uses memory dumps to analyze memory in memory related forensic investigations. It comes with a ton of plugins specifically designed to pull out different forms of information from memory images, such as running processes, network connections, loaded modules, and registry keys.

Step by Step Process:

Environment: Move the image file to a forensic analysis workstation with Volatility installed. Safe and seclusion of the environment to avoid contaminating or tampering with evidence.

Choose the Best Plugins: Identify and choose the right Volatility plugins for some of the artefacts you need to analyze. Common plugins are pslist (list processes), netscan (list network connections), malfind (find injected code), and ldrmodules (list loaded modules).

Run Volatility Commands: Execute Volatility commands with chosen plugins on the memory dump file.

Analyzing Output: Reviewing the output of the Volatility commands to extract relevant artefacts and data. It determines running processes, checks for unknown or suspicious programs, monitors network connections and evaluates loaded modules for potential signs of malware.

Correlate Data & Interpret Data: Correlate findings across different volatility plugins to build a unified picture of the system's state at the time of memory capture. Examine identified artefacts with the investigation goals in mind to determine potential security incidents or indicators of compromise (IOCs).

5.2. Using Rekall

Rekall (Now Plaso) is a second dominant framework (rekall) that supports the analysis of memory images across different platforms. It provides a scalable/extensible platform for analyzing memory dumps and taking out useful information from it.

5.2.1. Step by Step Process

6. RESULTS AND DISCUSSIONS

Real Life Case Studies

First, you need to set the Rekall Environments, which means Installing and configuring Rekall on the memory dump file analysis workstation. Then, you need to match the format of memory dumps with its architecture.

Profile: Create a Rekall profile for the particular operating system and version from which the memory dump was taken. E.g., profiles) is that which tells Rekall about how it should interpret memory structures and data formats.

Investigate the memory dump: Load the memory dump file using the correct profile in Rekall. Rekall Commands and scripts used: Rekall Lin Profile memory filename D drivers profile mainline pgx32 hives can list |> /root/VikingTools.py

Perform Analysis Tasks: Issue Rekall commands to examine which processes are running (pslist), network connections (netscan), loaded modules (ldrmodules) and registry keys (hivelist).

Rekall Command Output Analysis and Interpretation: Analyze Rekall Command output to ascertain relevant artefacts along with potential security issues. Compare the ground cinnamon to other forensic discoveries to construct a timeline and reenact the events leading up to the incident.

Using these tools, memory images can be analyzed comprehensively, extracting important forensic artefacts and revealing the activities of an attacker or breached organizations. This is the ideal class of tools for aiding investigative efforts and bolstering Cybersecurity and the legitimacy of digital forensic examinations.

Finally, practical examples in real cases will show us how useful live memory forensics are and their effectiveness in

dealing with ongoing cybersecurity incidents. The following section illustrates some of the important scenarios where live memory forensics was essential in identifying, investigating and responding to different types of cyber threats.

Case Study 1: Cyber Attack on Financial Institution

One of the largest financial institutions was facing a sudden surge of suspected network activities, signalling a potential data breach. Forensic analysts used a live memory forensics tool like Volatility to extract memory dumps of the compromised systems. Examination of the evidence discovered further that the attackers had used stolen credentials for initial access. Also, that code designed to evade traditional, signature based security controls was being employed. The institution used memory analysis to identify the attack and address it with confidence for spotting and to respond to the threat, thwarting further exfiltration and hardening itself against similar future attacks.

Case Study 2: Healthcare Malware Incident:

The client was a healthcare facility that recently had an issue in which its malware antivirus protection system failed. Another healthcare organization was rattled by a significant malware outbreak, which disrupted critical systems. We used live memory forensics tools, such as Rekall, to take memory dumps from affected endpoints. Investigations showed that legitimate applications were being injected by malicious processes that were trying to get access to patient records and healthcare information. Examination of volatile data determined the malware's persistence and C2 communications, allowing the organization to contain the infection, prevent or limit the loss of PII/PHI, and implement improved security to protect patient privacy and operational capacity.

Case Study 3: Insider Threat Detection at a Technology Firm

Suspected unauthorized data access and leakage by an insider in a technology firm background to a corporate espionage investigation. Live memory forensics was pivotal to retrieving volatile content from the suspect's workstation while it was being used. Memory dump analysis, on the other hand, disclosed access to requested confidential project files and suspicious network activity characteristic of data exfiltration cascades. A thorough analysis of the volatile data ended up giving valuable evidence that positioned the actions of the insider as the cause of the security breach, which enabled prompt decisions on disciplinary consequences and improved internal security guidelines to prevent new threats from within.

Example in the Real World of Government Agency Cyber Attack

Hackers launched a well-crafted cyber-attack against a government agency to compromise classified national security information. Live memory forensics allowed us to dump the memory of the compromised system and find IOCs associated with APTs. Advanced forensic analysis revealed the presence of stealthy malware implants, zero-day exploits, covert malicious communications, and other advanced malware loads used for illegal activities. Identifying and responding to

the volatile data allowed the agency to close vulnerability gaps used by the adversary, minimizing the extent of the breach, limiting the impact and hardening its cyber security posture from penetrations posed by persistent and emerging cyber threat actors holding government and critical infrastructure adversaries in their target list.

Retail Sector Data Breach (Real World Example)

Data Breach for A Leading Retail Corporation, Exposing Sensitive Payment and Corporate Data Live memory forensics tools were used to capture memory dumps from infected point of sale (POS) systems and device servers. The forensic examination of volatile data identified malware specifically designed to collect and then transmit payment card data from transactions where its rupture point was intercepted from the POS software. Investigators used forensic analysis of memory artefacts to identify the malware's activities, found the systems affected, and took immediate action to halt unauthorized data access, alert the affected customers, and meet regulatory reporting requirements.

The value that memory forensics brings to modern cybersecurity operations becomes very clear when we review these case studies and real world examples. Forensic analysts detect, investigate, and mitigate cyber threats by capturing and analyzing volatile data from systems that are live, all done to protect organizations from threats that can cost them money, hurt their reputations, and bring about operational disturbances. Experience With live memory, forensics often demonstrates real importance in incident response, threat detection, and digital investigations across many industries financial, healthcare, technology, government, and retail.

Key features of live memory forensics enable organizations to proactively surveil and secure their cyber environments against the constantly evolving cyber threat landscape, resulting in resilience, robust defence capabilities, and guaranteeing the forensic soundness of investigations. Incorporating live memory forensics into broader cybersecurity operations increases the likelihood of identifying and responding to any nefarious behaviour early, preserving digital evidence and reducing the risks associated with advanced cyber adversaries.

7. CHALLENGES AND LIMITATIONS

One of the many challenges and limitations of live memory forensics, used in modern cybersecurity investigations, is making sure the forensic analyst can #1 get the information they need and #2 that this information is accurate and reliable without violating the integrity of the data present when performing a forensic investigation should it be necessary.

Data Volatility

This presents a formidable challenge for forensic investigators, and many varieties of hardware trojans persist in a computer's volatile RAM. Unlike data saved in persistent storage such as a hard drive, volatile data stored on RAM is gone when your system shuts down. Just like RAM, this means that all data in RAM is lost once the system loses power or is turned off. From the

forensic perspective, real time volatile data acquisition is very important as this provides a frozen image of the system at the time of investigation. But this also means that if the capture process is delayed or interrupted, so is the evidence, which could be crucial.

An obstacle is the fact that data remains volatile, and forensic tools and techniques are deployed in an attempt to minimize disruption during capture. Techniques, Volatility tools of Rapidly memory dump and Rekall.execSQL. It is a very fast way to create memory dumps with both tools. These dumps take an image of the currently running processes, all network connections and other volatile data on the RAM. Swift and accurate capture of the data allows forensic analysts to maintain the integrity of the evidence and recreate the events on the victim system.

Potential Contamination

Another important problem is the corruption of volatile data during forensic analysis. Forensic analysts should be careful not to modify or taint memory contents. Analysis of live memory may be subject to inaccuracies due to some factors, i.e. malware in memory. These on disk memory analysis tools change data in memory or artefacts incorrect detection because some processes can be active and modify data. To minimize this risk, we outline some of the strict protocols we adhere to, such as the use of credible forensic tools, verification and validation of forensic tools, verification of memory image integrity via checksums, and finally, chain of custody documentation.

Furthermore, forensic analysts implement methods to ensure the system is not significantly affected during data acquisition. Therefore, anything operating within volatile memory, such as memory only live forensics, can never contaminate disk storage, and the integrity of volatile data can be obtained directly without time consuming and unreliable methods of extraction. These are intended to protect the collected evidence from being invalidated in case of legal issues, which thus further enables the evidence to still come out as actionable intelligence usable for cybersecurity incident response.

Legal Considerations

Privacy Rights Data Protection Regulations Admissibility of Evidence in court and more. The process of collecting and analyzing volatile data is a sensitive topic as it has to do with volatile memory, which may contain personal data, user communications, and sensitive business data. Those performing live memory forensics need to abide by constraints imposed by law concerning data privacy and electronic evidence.

Legal issues

Making sure data is legal to be collected, have a chain of custody and privacy agendas are defined. For example, jurisdictions could implement regulations around how long data could be retained, how data needed to be secured, and how consent was to be achieved before accessing and analyzing volatile data. Noncompliance with these legal mandates may then potentially preclude forensic evidence from entering, effectively nullifying the utility of live memory forensics as an investigative tool.

7.1. Technological Limitations

Cybersecurity investigations are also impacted by technological limitations that make live memory forensics much less effective. Different computational environments use different hardware architectures, operating systems, and memory management, and these differences make it difficult for forensic tools and methods to produce constant output. The forensic analyst should have a sufficient understanding of the underlying behaviours of these complexities and should evolve their methodology to be sustained to maintain forensic soundness and reliability.

In addition, cyber adversaries are highly developed, which adds complexity to live memory forensics. Prolific malware techniques such as file less malware and antiforensic methodologies can also avoid detection and control from forensic tools. Polymorphic ransomware is particularly problematic because of the ease with which it can be customized to elude existing security measures, and spotting them is virtually impossible without forensic capabilities, ongoing research and information sharing among organizations in the security community to create the necessary countermeasures and detection techniques.

Mitigation Approaches for the Real World:

To effectively address these challenges and limitations, organizations and forensic analysts can follow some pragmatic strategies:

Training and Certification: Regular training and certification in live memory forensics keep forensic analysts current with the tools, techniques, and legal prerequisites.

Validation and Utilization of Tools: Use verified and trusted forensic tools, ensure the tool is competent with every other operating system, and test the tool to validate its efficiency.

Evidence Records: keeping detailed records of how evidence was accessed, ensuring the integrity of the evidence so that it can be presented in court

Legal Proficiency: Working with legal experts of the company to cope with the regulatory environments, solve problems by keeping privacy intact and also complying with the data protection laws.

Stakeholder Standpoint: Continue monitoring technological development, researching new threats, and adapting forensic techniques so that detection and analysis capabilities remain up to date.

The practices mentioned here (among many others) will help organizations carry out better live memory forensics, thereby reducing accompanying risks and elevating the cybersecurity posture against emerging Cyber threats.

ETHICAL AND LEGAL ISSUES

The technique of live memory forensics in the investigation of Cybersecurity is important but also full of legal and moral pitfalls that must be complied with to preserve a correct forensic process and respect the rights of the individual. This section examines the ethics and legal issues of capturing and analyzing live memory data and the need for compliance in this area.

7.2. Ethical Implications

In the world of live memory forensics, ethicality is the primary concern with privacy, data confidentiality, and the

sensitive information being processed being handled responsibly. While pulling up live memory captures, forensic analysts can see a broad swath of volatile data, including personal communications, websites visited and patterns of application usage. To keep forensic investigations ethically sound and professionally set, respecting the privacy of individuals and maintaining confidentiality are the most important factors.

Forensic analysts must have proper analysis consent to access volatile data, especially in corporate and legal settings. Transparent data collection practices also help build trust and accountability by making people more fully aware of when and for how long all forensic investigations are taking place. Forensic examiners should also adhere to the concept of data depreciation, which is to say that they should only gather and preserve the necessary volatile data to avoid privacy implications and to conform to ethical guidelines.

One strong point is associated with the ethical consideration of negative externalities that come to the subject of forensic investigations in the form of people or organizations. The application of live memory forensics, in this case, can unearth confidential information, and you never know it. Still, evidence of nuisance is also possible, which can have a stronghold upon stakeholders. Forensic analysts have to deal with the facts of cases sensitively and professionally, ensuring that they remain objective and unbiased concerning their findings throughout the process of investigation.

7.3. Legal Considerations

In live memory forensics, legal aspects refer to data protection legislation, the admissibility of evidence in court, and procedural standards and guidelines for forensic investigation. One of the numerous legal frameworks around data privacy, electronic communications, and the admissibility of digital evidence is collecting (only the most legally defensible portions) and analyzing volatile data from live systems, which is a minefield.

Forensic investigations often fall under regulations like the General Data Protection Regulation (GDPR) in the European Union or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. To comply with these laws, data protection obligations, such as obtaining consent for data processing, notifying individuals when there is a personal data breach, and taking appropriate measures to ensure the security and confidentiality of personal data, are very strict.

Forensic experts may have to justify the use of a particular forensic technique in a court of law before evidence obtained using live memory forensics is admissible for the intended application. The judiciary construes these rules as entitling volatile data to stand under the

Application of Ethical and Legal Principles into Practice

There are several best practices forensic analysts and organizations can consider when grappling with ethical and legal considerations.

Ethical Standards and Codes of Conduct: Follow professional ethical guidelines and codes of conduct, such as the IACIS or ADFSL code of ethics.

Building Trust Informed Consent and Forensic Live Memory Captures: At the heart of any live forensic investigation is trust, Employees Individuals Stakeholders Informed Consent Asking for the consent of individuals or stakeholders aware of the potential memory capture before a forensic investigation is about to begin is critically important.

Data Protection Mechanics, which include Securing volatile data using strong encryption, anonymization, and secure storage, restricting unauthorized access, and preventing data disclosure.

We Take Legal Compliance: Seriously, We Must Stay abreast of all laws and any updates affecting forensic investigations and consult with legal experts as needed to ensure compliance.

Documentation and Chain of Custody: keeping detailed records of forensic procedures, including ensuring the chain of custody or that it has not been tampered with before legal proceedings so that the volatile data can be admitted as evidence.

If properly formalized, adopting these practices can help organizations abide by necessary ethical standards, reduce legal liabilities, and even strengthen the reputability of live memory forensics as an indispensable method in cyber security forensics.

8. FUTURE TREND

Due to the sophistication of cyber threats and the complexity of modern digital stagings, memory forensics needs to be achieved at a faster pace than traditional techniques. This paper discussed recent trends and innovative perspectives, although this portion emphasizes the improvements in memory forensics.

Recent Technological Improvements in Forensic Tools

The memory forensics tool landscape is constantly evolving, primarily based on the need to support a varied range of operating systems, architectures, and memory management methodologies. Old ones like Volatility or Rekall are still being enhanced by new functionalities that make them faster when capturing and analyzing volatile data. Advancements in these areas have included greater support for virtualized environments, upward compatibility with newer operating systems and improvements to multi core processing optimizations that make memory dump analysis faster.

Additionally, a key trend which is expected to gain ground in the memory forensics market is the growing usage of memory forensics tools by embedding machine learning and artificial intelligence (AI). Anomalous memory patterns are automatically detected and prioritized as critical findings for forensic analysts by using AI algorithms. It takes the burden off analysts, makes the entire investigative process more efficient and augments the capability to uncover advanced, stealthily in memory malware.

EDR Integration

Memory forensics is merging with Endpoint Detection and Response (EDR) solutions. Transforming how Organizations are defending themselves against cyber threats. Now, EDR platforms support memory file forensics so that during a security breach or incident, memory snapshots can be collected and stored for later analysis. The integration helps to perform real time threat hunting, fast

incident response, and link memory based artefacts to endpoint behavioural data.

Utilizing EDR integrated Memory Forensics can increase organizations' insight into memory resident threats (e.g., Fileless malware, and APTs). This keeps dwell time to a minimum and damage low while improving security resilience against new threats.

Virtualization and Cloud Forensics

The emergence of cloud computing and virtualization creates new difficulties and opportunities for memory forensics. Cloud based memory forensics collects and analyzes volatile data on virtual machines (VMs) and cloud instances due to the memory state of VMs running in shared environments with dynamically distributed memory resources. Forensic analysts are developing special tools and techniques to address the unique challenges of cloud memory forensic areas such as data isolation, chain of custody preservation across virtualized environments, and legal issues relevant to cross border data transfers.

Cloud native memory forensics tools are likewise advancing, allowing organizations to naturally extend their investigatory prowess into the cloud and cloud based workloads and applications. These tools cover functionalities like capturing memory dumps from cloud instances and remote memory analysis, and they integrate with cloud security platforms for coordinating response actions across expanded environments.

Privacy Preserving Techniques

Introduction Privacy concerns and regulatory requirements are forcing memory forensic practitioners to learn privacy preserving techniques. Increasingly, forensic tools are embedding encryption and anonymization technology to safeguard sensitive data that can be protected at the time of data capture, storage, and analysis. By doing so, you can prevent unauthorized access or leaks of personal and sensitive data and avoid fines under data protection laws like GDPR and HIPAA.

In addition, innovations in differential privacy and secure Multiparty computation seek diverse ways to reconcile forensic access with privacy rights. This provides forensic analysts with the channels to fully investigate without risking the identity and security of persons connected to legal and corporate inquiries.

Future Dangers and Safeguards

As we move forward, memory forensics needs to keep up the pace of new methods and tools adversaries can and will use to evade and hide their malicious activity. At the same time, threat actors are using increasingly sophisticated obfuscation tools, anti-forensic techniques and memory resident malware aimed at escaping the detection and manipulation of traditional forensics approaches. Overcoming these limitations will be the main areas of research for future memory forensics development as we move towards both proactively detecting threats, refining memory introspection procedures, and incorporating real time anomaly detection algorithms.

Through this solution, forensic analysts can proactively detect and respond to threats in real time using behavioural analysis and machine learning driven

techniques, eliminating security gaps and reducing organizational risk. Collaborative research and information sharing among the cybersecurity community best position memory forensics capabilities to address the propagations associated with today's fast changing threat landscape.

9. CONCLUSIONS

Live memory forensics is really important in Cybersecurity because it allows you to recover volatile data from the RAM of a computer, which could be evidence that is not stored on hard drives and other storage that typically only is used to store data but not to process it. This process is important in the field of digital forensics as it gives an instantaneous picture of the state of a system, which includes active processes, network connections, and users. Appreciating the basics of live memory forensics is essential as it provides forensic analysts with the essential knowledge and resources to carry out comprehensive investigations efficiently. FTK Imager, Belkasoft Live RAM Capturer and DumpIt are some of the essential tools available for efficiently capturing memory images that secure the evidence for legal and corporate investigations. Live memory forensics is an essential tool used in Cybersecurity in areas such as incident response, malware analysis, unauthorized access detection, and search for insider threats. Emphasizing the incidents in which live memory forensics is crucial, organizations can improve the depth and efficiency of their cybersecurity defences and their capacity for rapid and effective response to security incidents. This practical knowledge of tools and their methodologies enables forensic analysts to manoeuvre complex digital environments with accuracy in compliance with forensic best practices and legal standards. A step-by-step way of taking volatile data from any forensic related activity, which provides a definite systematic process for why and how to execute memory dump on any running systems. This procedural guidance is key in making certain that forensic practitioners follow the proper data handling practices to keep the evidence maintained to its integrity and admissibility in a legal setting.

REFERENCES

[1] I. Taha, M. Mirhassani, and A. E. Analog, "A Monotonically Linear DCO for 77 GHz Automotive Radars," *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, Windsor, ON, Canada, pp. 77–80, 2018.

[2] M. M. Rahman, M. M. Hossain, and K. K. Karmakar, "Π shape microstrip antenna design for WiMAX, Wi Fi and biomedical application at 2.45 GHz," *2013 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, India, pp. 546–549, 2013.

[3] S. I. Md Salim, H. A. Sulaiman, R. Jamaluddin, L. Salahuddin, M. N. S. Zainudin, and A. J. Salim, "Two pass assembler design for a reconfigurable RISC processor," *2013 IEEE Conference on Open Systems (ICOS)*, Kuching, Malaysia, pp. 77–82, 2013.

[4] W. Alkohlani and J. Cook, "Towards Performance Predictive Application Dependent Workload Characterization," *2012 SC Companion: High Performance*

Computing, Networking Storage and Analysis, Salt Lake City, UT, USA, pp. 426–436, 2012.

[5] J. N. Mahajan and A. M. Jain, "Conversion of existing inverter into solar inverter," *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, pp. 859–862, 2017.

[6] N. Kumar and S. Agarwal, "A dynamic Workload Management model for saving Electricity Costs in cloud data centers," *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Delhi, India, pp. 1246–1251, 2014.

[7] Y. Qiao, N. Wu, C. Pan, and M. Zhou, "Petri net based response policies to process module failure in time constrained single arm cluster tools," *Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control*, Miami, FL, USA, pp. 144–149, 2014.

[8] M. F. M. Fudzee, J. Mohamed, J. Abawajy, S. Kasim, and M. N. Ismail, "An SLA Evaluator for Multimedia Content Adaptation Services," *2014 International Conference on Information Science & Applications (ICISA)*, Seoul, Korea, pp. 1–4, 2014.

[9] P. Ameri, U. Grabowski, J. Meyer, and A. Streit, "On the Application and Performance of MongoDB for Climate Satellite Data," *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, pp. 652–659, 2014.

[10] V. C. Valgenti, H. Sun, and M. S. Kim, "Protecting Runtime Filters for Network Intrusion Detection Systems," *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, Victoria, BC, Canada, pp. 116–122, 2014.

[11] Y. Tian, F. Deng, Z. Chen, P. C. Loh, and Y. Hu, "Impedance analysis of control modes in cascaded converter," *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society*, Yokohama, Japan, pp. 003545–003550, 2015.

[12] S. Jamalian and H. Rajaei, "Data Intensive HPC Tasks Scheduling with SDN to Enable HPC as a Service," *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, USA, pp. 596–603, 2015.

[13] K. E. Adetunji and M. K. Joseph, "Development of a Cloud Based Monitoring System Using 4Duino: Applications in Agriculture," *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, pp. 4849–4854, 2018.

[14] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, pp. 124–134, 1994.