A novel approach for threat detection in Windows using cache memory forensics

MSc Industry Internship
MSCCYB1

Pushkar Yewalekar
Student ID: X21194254

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Pushkar Yewalekar …………..……………………………………………………………………

Student ID: X21194254.…………………………………………………………………………………..……

Programme: MSCCYB1 ……………………………………………… **Year:** 2022-2023 ..

Module: MSc Industry Internship ……………………………………………………….………

Supervisor: Prof Vikas Sahni ………………………………………………………………….………

Submission Due Date: 04/09/2023 ……………………………………………………………………………………………….………

Project Title: A novel approach for threat detection in Windows using cache memory forensics ………………….…………………………………………………….………

Word Count: 5812 ………………………… **Page Count:** 20…………………………………………..…….

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Pushkar Yewalekar ……………………………………………………………………

Date: 04/09/2023 ………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A novel approach for threat detection in Windows using cache memory forensics

Pushkar Yewalekar
X21194254

Abstract

A forensic approach focusing on cache memory that comprises of volatile data containing highly sensitive information of data files. Considering its importance in digital forensics, this is a mine of information in forensics but being limited by its resources like time and storage. Modern day attacks target such volatile memory for malicious user, taking advantage of its limitations due to volatile and overwriting nature. To make use of this cached data, and to reconstruct events in case of any security incidence, a methodical approach is implemented in this paper, that focuses the digital forensic part of investigation on the cache data of Windows. To increase efficiency of detection of threats which executes during the run time, using combination of tools, techniques, and procedures, the novel approach uses key attributes of cache memory before its evasion.

An efficient methodology has been implemented designed to validate the proposed enhancements that highlights the advantages of identifying critical artefacts stored in cache memory. Significantly, this study aims to improvise threat detection, providing unique perspective in digital forensic to overcome existing challenges.

Keywords: Cyber threats, Cache memory, Cache forensics, Memory acquisition & analysis, Threat detection

1 Introduction

The increasing complexity and sophistication of cyber threats pose significant challenges to the security of modern computer systems and raises questions on the security aspect of the architecture. This demands advanced threat detection mechanisms that can effectively identify and mitigate potential risks. The area of exploration of possible solution that is discussed in this paper is the utilization of cache memory forensics to enhance threat detection capabilities.

Cache memory, a small but crucial component of contemporary computer architecture, plays a pivotal role in the execution of programs by storing frequently accessed data and instructions. The primary purpose of cache memory is to improve the overall performance of the computer by providing faster access to data than fetching it from slower main memory (RAM) or even slower storage devices like hard drives. As a result, cache memory can contain valuable information about the activities and interactions within a computer system. The inherent characteristics of cache memory, such as its high-speed access and temporary storage nature, make it an intriguing resource for forensic analysis in the context of threat detection.

Cache memory is typically implemented using high-speed volatile memory technologies like SRAM (Static Random-Access Memory). Unlike non-volatile memory technologies (e.g., flash memory or magnetic storage), SRAM and other cache memory types are designed for rapid data access and do not have the ability to retain data once power is removed. This means that the contents of cache memory are lost whenever the computer is shut down or experiences a power loss.

The purpose of this research is to develop an enhanced approach for threat detection by using the potential of cache memory forensics. By leveraging the information stored in cache memory, it becomes possible to identify patterns, traces, and indicators of malicious activities, thereby strengthening the ability to detect and respond to cyber threats proactively. It serves as crucial evidence in forensics as it simulates like a snapshot of recent user activities on a computer system, making it essential for reconstructing digital timelines during investigations. It contains artifacts, metadata, and evidence related to user actions, including timestamps, file paths, and web browsing history. This information servers in rebuilding the sequence of events and building a compelling case. However, the volatile nature of cache memory necessitates careful handling by forensic experts to ensure that evidence is preserved, and privacy rights are respected. Despite its temporary storage, cache memory plays a vital role in digital forensics, offering valuable insights into a suspect's digital footprint and activities, helping investigators uncover crucial evidence and establish timelines for their cases.

Furthermore, this research explores various techniques for processing and analysing the acquired cache memory data, with a focus on identifying potential threat indicators. Existing parameters of operating system that contain specific files are discussed to effectively detect and classify threats based on cache memory analysis, contributing to the development of advanced threat detection systems.

In summary, by extracting the power of cache memory forensics, this research aims to advance the state-of-the-art in threat detection capabilities using cache forensics. The developed approach has the potential to enhance the accuracy and efficiency of threat detection systems, ultimately increasing the security posture of computer systems and the evolving cyber threats.

1.1 Research Question

The research question addressed in the paper is:
"How can cache memory forensics be effectively utilized to identify and detect malicious activities in order to enhance threat detection capabilities?"

2 Related Work

In digital investigations, cache memory forensics is essential because it enables investigators to recover important evidence from volatile storage and reconstruct user behaviours. Security issues have recently been brought up by cache-based attacks and side channels, underscoring the importance of good and efficient cache memory analysis methods. This thorough overview of the literature intends to examine numerous publications on cache memory forensics, including techniques for gathering and analysing cache data, case studies contrasting the efficiency of inquiries with and without cache memory, and difficulties in this field of research.

In the research by Baryamureeba and Tushabe (2004), the Enhanced Integrated Digital Investigation Process (EIDIP) model was presented, revolutionizing digital investigation. This model holistically covers the investigation lifecycle, particularly emphasizing traceback phases, thus overcoming the drawbacks of earlier models. In an era where cybercrimes are becoming more sophisticated, the EIDIP framework is pivotal for effective digital investigations.

One such issue is the exploitation of cache memory, a temporary storage component in computers. Osvik et al. (2005) demonstrated how cache memory can be used for side-channel attacks, especially cache-timing attacks, which harness the time data retrieval takes to deduce sensitive information, including cryptographic keys.

The paper presented by Hannah et al. (2022) explain how volatile memory analysis has gained prominence due to the surge of fileless malware. While RAM examination reveals encrypted content and system processes, there's a research gap in memory acquisition and malware analysis. This study also reviews current tools, evaluating their effectiveness and highlights the role of forensics and machine learning.

Several studies, such as those by Nishtha & Meenu (2018) and Sandeep, Goutam & Manu (2018), have deep dived into cache memory attacks, defences, and forensics. They underlined the importance of cache memory forensics for detecting security vulnerabilities, understanding cache design, and optimizing evidence collection methods. Arafat et al. (2020) proposed an innovative technique for digital forensics cache memory analysis, stressing the benefits of advanced methods.

Synced data offers potential evidence sources, it complicates the attribution of wrongdoing, especially when distinguishing between local and synced data as researched by Boucher & le-Khac (2018). This paper introduces a framework aiding examiners in differentiating such data, demonstrating its application, and highlighting its reliability and associated considerations.

Cache memory, despite being transient, can house critical data fragments. This could include insights into user operations, ongoing processes, or even cryptographic activities (Matt, 2011). But, given cache's fleeting nature, conventional disk forensics tools prove ineffective. Instead, bespoke tools like Volatility[1] and Rekall[2] for memory imaging, and research-backed techniques for direct cache access are recommended.

2.1 Existing Cache memory forensics challenges and limitations

Cache Extraction:

In Garfinkel et al.'s (2010) study, the complexities of extracting digital evidence from computer systems, including cache memories, were explored. The research concluded that while cache memory can provide a wealth of evidence due to its volatile nature, many forensic tools fail to account for the nuanced ways data is stored and overwritten. This inherent volatility and inconsistency make cache memory a challenging source of forensic evidence.

Multilevel Cache Forensics: Implications and Limitations:

[1] https://www.volatilityfoundation.org/

[2] http://www.rekall-forensic.com/home

Apurva et al. (2011) emphasized that as technology has evolved, so has the complexity of cache structures. Modern CPUs come with multilevel caches (L1, L2, L3), each having its own purpose and behaviour. This layered architecture complicates forensic investigations as each level needs a different approach, and there's a lack of comprehensive tools that can effectively deal with this hierarchical structure.

Cache Attacks and Forensic Implications:

Cache-based side-channel attacks have been a topic of increasing interest in the cybersecurity community. In the paper by Erkay et al. (2015), the authors discuss potential attacks leveraging cache behaviour. This brings in a forensic challenge: while cache can be a source of evidence, it can also be an attack vector. As such, forensic tools not only need to extract evidence from caches but also identify signs of cache-based attacks—a duality that many current frameworks are ill-equipped to handle.

Cache Forensics in Virtualized Environments:

With the rise of cloud computing and virtualization, the challenges of cache memory forensics have multiplied. Zawoad and Hasan (2015) highlighted that virtualized environments introduce a level of abstraction in cache memory, making traditional forensic tools inefficient. Such environments might have multiple virtual systems sharing the same physical cache, complicating the forensic recovery process.

Tool Reliability and Validation:

One consistent challenge in digital forensics is the reliability and validation of tools. Pagani et al. (2018) pointed out that many tools are proprietary, with their inner workings obfuscated, leading to questions about their reliability. This concern is especially poignant for cache memory, where data is transient and rapidly changing.

Issues of Data Volatility:

The volatile nature of certain data types has always posed challenges for digital forensic investigators. Lee et al. (2009) examined RAM forensics, emphasizing the importance of timely data extraction before it's lost or overwritten – a concern that is magnified when dealing with cache memory due to its more limited size and faster data turnover.

Scale and Complexity of Modern Systems:

The multi-core and multi-threaded nature of modern processors introduces an additional layer of complexity to forensics. As Tanner et al. (2022) detailed, this can impact how evidence is located and extracted, particularly from temporary storage like cache.

Forensic Analysis in Virtualized Environments:

With the growing use of virtualization, Zhang et al. (2010) discussed the unique challenges presented by hypervisors and virtual machine environments. Cache memory in these settings can be especially elusive due to the abstraction layers introduced by virtualization.

Legal and Ethical Dimension:

The legal landscape is always evolving in response to technological advances. Manes and Downing (2019) examined the legal challenges in acquiring and analysing volatile memory, a topic with clear relevance to cache memory forensics which also explains clear limitations of forensic due to hardship faced in reconstruction of events.

Cloud Forensics and Remote Data:

As Meera et al. (2017) detailed, cloud storage and computation introduce issues of jurisdiction, data ownership, and remote access. While cache memory is inherently local to a device, its interaction with remotely fetched data is an area that warrants attention.

Real-time Forensic Analysis:

The push towards real-time analysis, as discussed by Periyadi et al. (2017), highlights the need for tools and methodologies that can rapidly process and analyze data. Cache memory, due to its inherent transience, is a natural fit for such real-time methodologies.

Standardization and Best Practices:

The field of digital forensics is diverse, and as Roy et al. (2019) argued, there's a pressing need for standardization and the establishment of best practices. Cache memory forensics, being a relatively new frontier, can benefit immensely from such standardization efforts.

Subject	Description (Key Insights)	Author(s)
Complex Extraction	Difficulties arise from the nuanced ways cache stores and overwrites data.	Garfinkel et al.'s (2010)
Multilevel Cache Structures	Each cache level (L1, L2, L3) demands distinct investigation strategies.	Apurva et al. (2011)
Cache Attacks	Cache can be both an evidence source and an attack vector.	Erkay et al. (2015)
Virtual Environments	Shared physical caches among virtual systems complicate recovery.	Zawoad & Hasan (2015)
Tool Reliability	Many forensic tools are proprietary, leading to reliability concerns.	Pagani et al. (2018)
Data Volatility	Quick data turnover in cache necessitates prompt extraction.	Lee et al. (2009)
Modern System Complexities	Multi-core processors affect evidence localization and extraction.	Tanner et al. (2022)
Legal Aspects	The evolving legal scene affects volatile memory acquisition and analysis.	Manes and Downing (2019)
Cloud Interactions	Jurisdiction, ownership, and remote access concerns arise with cloud solutions.	Zhang et al. (2010)
Real-time Analysis	There's a need for swift data processing and interpretation tools.	Meera et al. (2017)
Standardization	Cache memory forensics can benefit from standardized guidelines and practices.	Roy et al. (2019)

Table 1. Comprehensive study of Cache memory

2.2 Limitations in the NIST framework

The National Institute of Standards and Technology (NIST) has set foundational standards and guidelines for digital forensics particularly in the NIST SP 800-86 section. However, as cyber threats multiply, innovative methodologies are required, with cache memory forensics becoming increasingly crucial. Cache memory offers intricate insights into system activities, presenting potential evidence of cyber threats. Its role in program execution makes it a potential goldmine for traces of malicious activity.

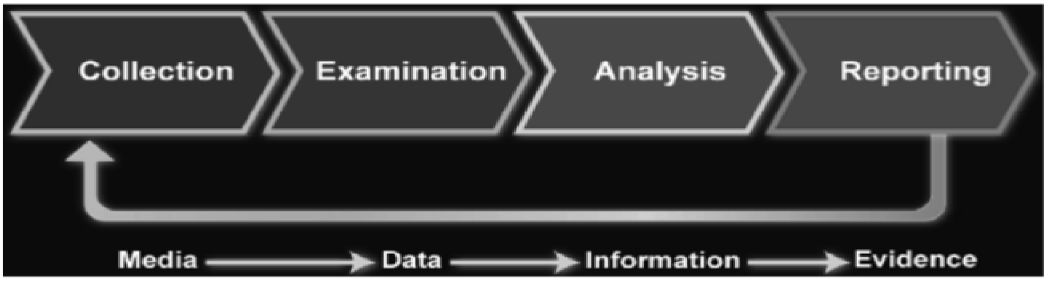


Fig 1. Digital Forensic Flow Standard by NIST SP 800-86 [3]

- There's an evident absence of guidelines tailored to cache memory forensics in NIST's frameworks.
- The tools listed by NIST, although exhaustive, doesn't cater specifically to cache memory forensic tools.
- Cache memory forensics training is conspicuously absent from NIST's recommended modules.

2.3 Conclusion

The absence of cache memory forensics guidance, specific tools, and training in NIST's frameworks concludes with the need for a dedicated cache memory forensics framework. Cache memory is crucial in digital investigations, and the lack of specialized resources remains ineffective. Therefore, developing cache memory-specific resources within a dedicated framework will substantially enhance investigative capabilities.

3 Research Methodology

3.1 Evidence acquisition procedure

Traditional forensic tools use data carving, disk level or physical data extraction techniques to collect data. However, most of the crucial data is stored in the system itself and the tools do not identify this. This can be understood from the forensic case studies mentioned in this paper as cases with volatile memory have shown faster and accurate findings as expected, while the case studies without it have shown slower results with results being inconclusive.

The approach that a forensic investigation should follow must include cache memory acquisition as the most primary and important step as it contains the most volatile data. The volatility of cache memory may tamper with evidence later during the acquisition or analysis stage. Hence, it is extremely important to acquire and analyse volatile data like cache memory during the initial stage.

In the systematic approach as shown in the below mentioned figure, it particularly focuses on cache memory to dig out crucial information before any other forensic activities. This is possible because other forensic methods like data carving or imaging takes longer time usually. However, for the data most recently used by the user can be found in deleted items or unindexed memory of the system and therefore, analysing this part of memory provides crucial information. This shows an ideal approach for digital forensics improving quality of findings and ability of an investigator to reach a conclusion.

[3] https://csrc.nist.gov/pubs/sp/800/86/final

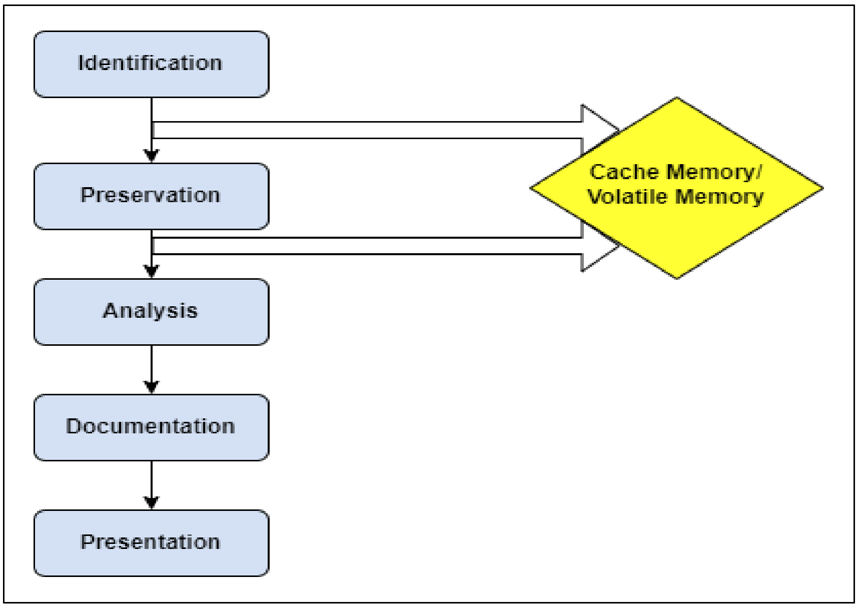


Fig 2. Proposed approach for cache memory analysis

- The initiation of the process is generally started by a detection of cyber incident. This can include many sources such as intrusion detection systems, logs generated by firewalls, or warnings provided by users, which serves as trigger for the cybersecurity team.
- Initial Analysis: Upon the detection of an alert, essential data pertaining to the event is collected. The collection of essential data for the investigation encompasses IP addresses, timestamps, and relevant system logs, hence establishing a need to initiate the inquiry.
- Acquisition of cache memory: In the event of a failed memory acquisition, which can arise from various reasons like encryption or a locked processes or a dead lock the process needs to be reinitiated . Alternative approaches, such as utilizing diverse tool sets or implementing privilege escalation techniques can be used.
- Advanced threat detection methods are referred to compare the processed data with threat databases to identify indicators of potential threats. Instances that possess identifiable patterns, hash values, or binaries that build suspicion are flagged & marked for additional assessment.
- The findings are documented, and the threat database is subsequently updated. A complete report is created, providing a detailed account of every aspect of the study.

3.2 Evidence analysis methodology

- Types of Cache: Modern CPUs have multiple levels of cache – L1, L2, and L3. L1 is the smallest but fastest, directly connected to the core. L2 is larger and slower, while L3 is even larger and slower, shared among all cores. Each level potentially stores different types of information.
- Cache Coherency Protocols: CPUs employ protocols like MESI (Modified, Exclusive, Shared, Invalid) to maintain cache coherency across cores. By examining cache states, it's possible to discern specific operations or interactions between cores.
- Cache Mapping Techniques:
    1. Direct-Mapped Cache: Uses mapping from memory to cache. Examining Direct-Mapped Cache will determine where certain memory data will end up in the cache.

2. Set-Associative Cache: A set contains several lines. A block of memory is mapped to any line in a specific set. By examining which lines have been replaced, one can infer certain usage patterns.
3. Fully Associative Cache: Any block of memory placed in any line of cache, making it more complex but potentially revealing more diverse data.

Furthermore, to determine the root cause of the incident and to deep dive into the memory to obtain insights of the malicious activity, an investigator should know crucial parameters of cache memory to pinpoint the scope of investigation as a part of preliminary analysis. This will also save a lot of time for an investigator to search and define for a scope. This is a constructive approach that proposes stepwise guide which can be used to achieve high quality results using cache memory.

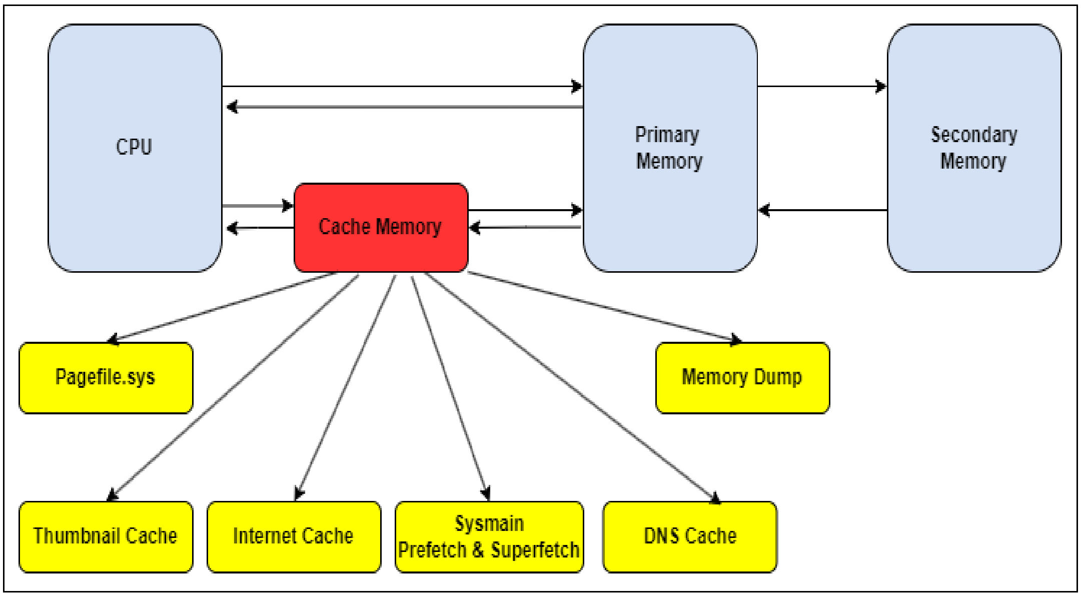


Fig 3. Cache Memory target areas

In the cache structure shown above, it particularly focuses on cache memory to dig out crucial information before any other forensic activities. This is possible because other forensic methods like data carving or imaging takes longer time usually. Additionally, any file, data or information deleted by the user but used last by the user end clearly on the cache rather than to search specifically for in other forensic methods. This shows an ideal approach for digital forensics improving quality of findings and ability of an investigator to reach a conclusion.

4 Design Specification

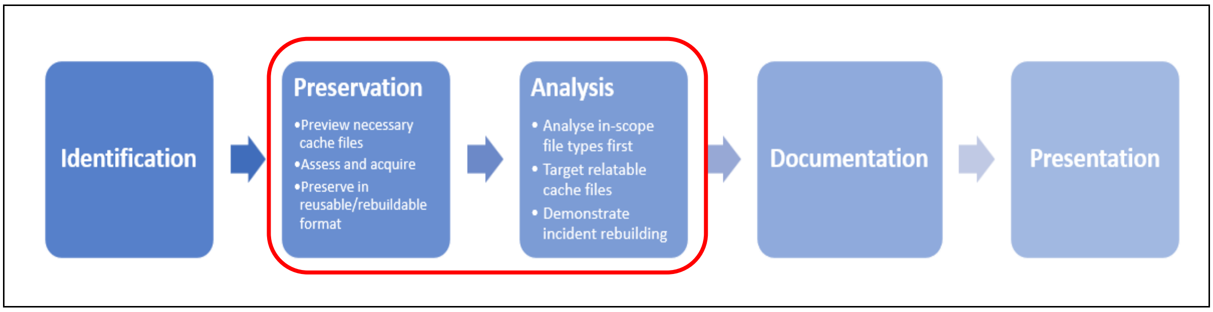

Identification
Preservation
•Preview necessary cache files
•Assess and acquire
•Preserve in reusable/rebuildable format
Analysis
• Analyse in-scope file types first
• Target relatable cache files
• Demonstrate incident rebuilding
Documentation
Presentation

Fig 4. Proposed approach

4.1 Preservation

This step helps in ensuring the originality and integrity of evidence as a primary concern. If data isn't properly preserved, it can be altered, making it inadmissible in legal procedures. To ensure integrity of artefacts, use write blockers proves to be beneficial to prevent accidental modification of data when accessing storage devices. This also ensures that original data is never directly accessed or modified; hence the analysis should always be worked on copies.

- The cache files are in temporary storage areas where frequently accessed data can be referred by the system for rapid access. They contain crucial evidence, such as user activity or downloaded files. Previewing cache files provide insights into recent user actions, visited websites, or downloaded data. To enhance the functionalities, there are specialized software tools that benefits in analysing cache contents without modifying them.
- Before acquiring digital evidence, assess the situation and the required devices, in this case, cache files and other volatile memory. Understand the nature of the incident, the type of data expected to find, and where it is located.
- Use forensically sound methods to acquire data. This involves disk imaging (creating a bit-by-bit copy of a device's storage) or logical acquisition (copying files and folders).
- Once data is acquired, validate its integrity, typically using cryptographic hashes like MD5 or SHA-256, to ensure that the copy is identical to the original.
- Evidence needs to be reviewed multiple times or shared with other investigators. Preserving in a reusable format ensures that evidence remains consistent and unaltered across reviews.
- Common formats include raw images (bit-by-bit copies) or formats like E01, which encapsulate the data and associated metadata. Such formats are standardized and can be read by multiple forensics tools. It's even advisable to have multiple copies of the preserved data, stored in different locations, to guard against loss or damage.

4.2 Analysis

This step begins by pinpointing and securing cache files that are relevant to the investigation. It's crucial to ensure these files remain unaltered during acquisition. Then it is very necessary to validate the integrity of the acquired cache files using cryptographic hash functions. This validation step confirms that the files have not been tampered with since acquisition.

- Apply filtering criteria, such as timestamps or file types, to narrow down the selection of cache files for examination. This helps focus the analysis on potentially pertinent data.
- It becomes necessary to integrate data from diverse sources, establishing connections between cache files and other digital artifacts to construct a comprehensive timeline or contextual understanding.
- Given the volume of cache files, prioritize examination based on importance or relevance, ensure that the most significant cache files are analysed first.
- Understand the structure of cache files, inspecting elements like headers and data blocks. This examining reveals how data is organized within these files.
- Examine the actual content stored in the cache files, which encompass cached web pages, images, scripts, or any cached data. This step extracts valuable information.
- Furthermore, also analyse timestamps embedded within cache files to establish precise timelines of digital activities. These timestamps are critical for reconstructing events.

- Conduct targeted searches within cache files using keywords or patterns, facilitating the retrieval of specific evidence or relevant information.
- Throughout these stages, maintain meticulous documentation and adhere to a strict chain of custody protocol to ensure the evidence remains legally admissible. Utilize specialized digital forensic tools and methodologies to guarantee that the analysis process remains forensically sound, preventing any inadvertent alterations to the original evidence.

5 Implementation

5.1 Acquisition Phase (Using FTK Imager):

- Assessment: Before acquiring digital evidence, assess the situation, identify the required devices (including cache files and volatile memory), and understand the nature of the incident.
- Forensically Sound Acquisition: Utilize FTK Imager to perform forensically sound acquisition of data. This involves creating a bit-by-bit copy of the device's storage (disk imaging) or copying relevant files and folders (logical acquisition).
- Integrity Validation: After acquisition, validate the integrity of the acquired data using cryptographic hashes like MD5 or SHA-256 to ensure the copies are identical to the originals.
- Preservation: Store the acquired data in reusable formats like raw images or E01 formats, which encapsulate data and metadata. Maintain multiple copies stored in different locations for redundancy and safeguarding against loss or damage.

5.2 Analysis Phase (Using Volatility Framework):

- Cache File Identification: Begin by pinpointing and securing relevant cache files that are crucial to the investigation. Ensure these files remain unaltered during acquisition.
- Integrity Validation: Validate the integrity of the acquired cache files using cryptographic hash functions to confirm they have not been tampered with since acquisition.
- Filtering and Prioritization: Apply filtering criteria such as timestamps or file types to narrow down the selection of cache files for examination. Prioritize the analysis of the most significant cache files first.
- Data Integration: Integrate data from various sources, establishing connections between cache files and other digital artifacts to create a comprehensive timeline or contextual understanding.
- Cache File Structure Examination: Understand the structure of cache files by inspecting elements like headers and data blocks. This examination reveals how data is organized within these files.
- Content Examination: Analyse the actual content stored in the cache files, including cached web pages, images, scripts, or any other relevant data. Extract valuable information.
- Timestamp Analysis: Examine timestamps embedded within cache files to establish precise timelines of digital activities, which are crucial for reconstructing events.
- Keyword Searches: Conduct targeted searches within cache files using keywords or patterns to facilitate the retrieval of specific evidence or relevant information.

- Documentation and Chain of Custody: Maintain meticulous documentation throughout the analysis process and adhere to a strict chain of custody protocol to ensure that the evidence remains legally admissible.
- Tool Utilization: Utilize specialized digital forensic tools and methodologies, such as the Volatility Framework, to guarantee that the analysis process remains forensically sound and prevents inadvertent alterations to the original evidence.

6 Evaluation

The evaluation of the above proposal is recorded from a comprehensive analysis of case studies performed during the research. The case studies involved indicate situations where analysis of evidence is performed without the volatile or cache memory as well as in cases where the volatile or cache memory is analysed.

6.1 Case Study – Using data carving

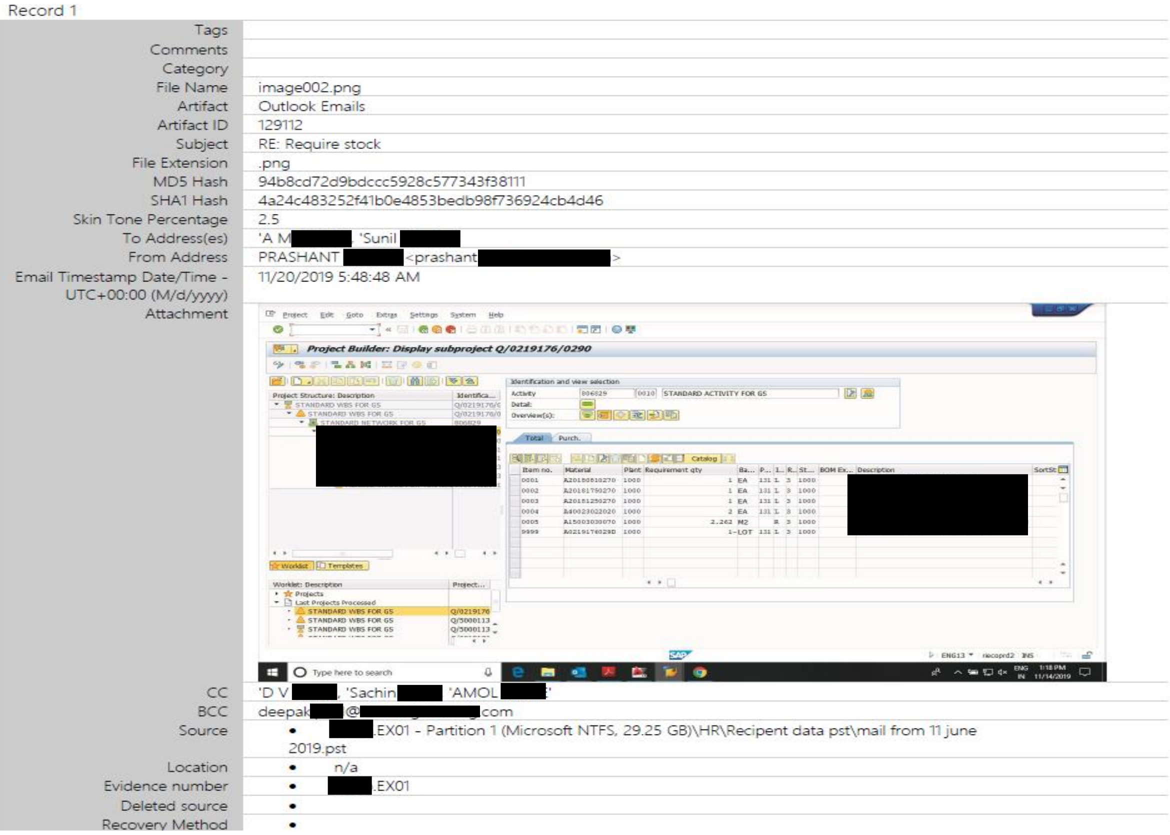
Background:
This is a case study about potential unauthorized access and use of sensitive files by a user. The primary objective is to determine if there is evidence of any misconduct and to gather adequate evidence to support any subsequent actions.

Methodology:
Acquisition of Evidence: Using the Tableau Forensic Imager in addition with a write blocker, bit-by-bit image of the suspect device is created, ensuring the integrity and authenticity of the evidence. This method prevents any alteration of the original data, maintaining its reliability.

Analysis: The imaged evidence is subjected to thorough examination using the Magnet Axiom forensic analyser. This software is used to parse through the digital artifacts present on the device, searching for any evidence of unauthorized access or usage of the sensitive files.

Key Findings:

- Several artefacts, including timestamps, user activity logs, and file access patterns, confirmed the suspicion of unauthorized access. These digital traces gave a timeline of the activities, which matched the periods when the suspicious user accesses the system.
- The analysis revealed instances of the files being opened, potentially copied, and then deleted.



Record 1

Tags	
Comments	
Category	
File Name	image002.png
Artifact	Outlook Emails
Artifact ID	129112
Subject	RE: Require stock
File Extension	.png
MD5 Hash	94b8cd72d9bdccc5928c577343f38111
SHA1 Hash	4a24c483252f41b0e4853bedb98f736924cb4d46
Skin Tone Percentage	2.5
To Address(es)	'A M[redacted], 'Sunil [redacted]
From Address	PRASHANT [redacted]<prashant[redacted]>
Email Timestamp Date/Time - UTC+00:00 (M/d/yyyy)	11/20/2019 5:48:48 AM
Attachment	Project Builder: Display subproject Q/0219176/0290
CC	'D V[redacted], 'Sachin[redacted] 'AMOL[redacted]'
BCC	deepak[redacted]@[redacted].com
Source	• [redacted].EX01 - Partition 1 (Microsoft NTFS, 29.25 GB)\HR\Recipent data pst\mail from 11 june 2019.pst
Location	• n/a
Evidence number	• [redacted].EX01
Deleted source	•
Recovery Method	•

[redacted]

Item no.	Material	Plant	Requirement qty	Ba...	P...	I...	R...	St...	BOM Ex...	Description
0001	A20180810270	1000	1	EA	131	1	3	1000		[redacted]
0002	A20181750270	1000	1	EA	131	1	3	1000		[redacted]
0003	A20181250270	1000	1	EA	131	1	3	1000		[redacted]
0004	A40023022020	1000	2	EA	131	1	3	1000		[redacted]
0005	A15003030070	1000	2.262	M2		R	3	1000		[redacted]
9999	A02191760290	1000	1-	LOT	131	1	3	1000		[redacted]

Fig 4. Artefact of Case study 1

- Despite the effectiveness of tools, a limitation with the Tableau imager is encountered, as it lacked the capability to acquire volatile memory (RAM). This means that any evidence that resided solely in the volatile memory is not captured. Given that volatile memory can often hold crucial pieces of evidence, like recently executed commands or active network connections, this posed a challenge.
- During the initial phases of analysis, several challenges were faced in reconstructing the sequence of the incident. Certain key pieces of evidence are found incomplete which turn poses as a challenge to reconstruct the incident. However, upon employing a data carving process using Magnet Axiom, it is possible to recover fragments of deleted or otherwise inaccessible files that filled in the gaps in evidence timeline.

Limitations and Challenges:

- The inability to acquire volatile memory limits the examination scope, potentially missing out on transient but vital pieces of evidence.
- The initial difficulty in incident reconstruction due to missing parts of evidence underscores the importance of comprehensive forensic tools. While carving helped recover some fragments, there remains a possibility that some data fragments were not retrieved.

6.2 Case Study – Using Forensic Imaging

Background:

This case study is regarding the unauthorized transfer of confidential files by user to another email. The objective is to ascertain and compile conclusive evidence, of such an unauthorized transfer.

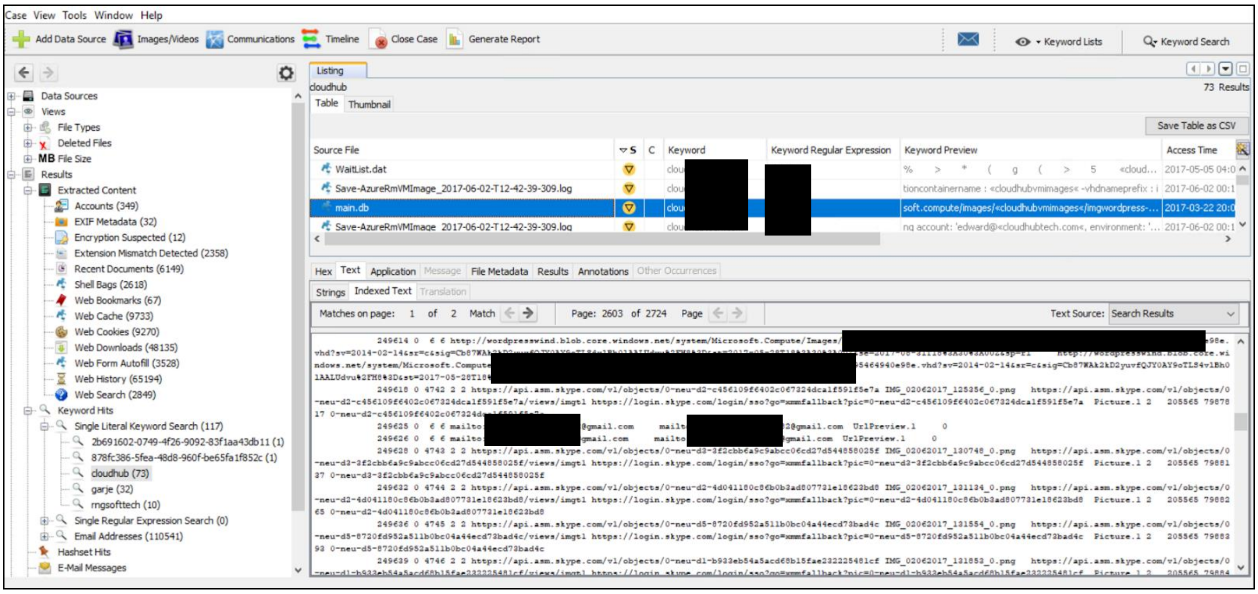
Methodology:

Acquisition of Evidence: To acquiring digital evidence forensically, FTK (Forensic Toolkit) Imager is used. This allowed to capture an exact image of the device while ensuring that the original evidence remained unaltered and preserved.

Analysis: Post the imaging process, the evidence is comprehensively analysed using the UFED4PC forensic analyser. This advanced tool aids in extracting, decoding, and analysing digital artifacts on a device to search for potential evidence or traces of misconduct.

Key Findings:

- Upon detailed examination, several digital artifacts that indicated a pattern of file transfer actions were traced. Specifically, these artifacts pointed to files being attached and sent via email.
- The investigation can validate the user's suspicious activity, confirming the users transfer of confidential files to unauthorized email address.
- However, UFED4PC's inability to acquire volatile memory posed as a significant limitation. Important evidence or traces of activity that resided only in the system's volatile memory were left unexamined, which could have offered a more comprehensive perspective on the employee's activities.



- Data Sources
- Views
  - File Types
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Accounts (349)
    - EXIF Metadata (32)
    - Encryption Suspected (12)
    - Extension Mismatch Detected (2358)
    - Recent Documents (6149)
    - Shell Bags (2618)
    - Web Bookmarks (67)
    - Web Cache (9733)
    - Web Cookies (9270)
    - Web Downloads (48135)
    - Web Form Autofill (3528)
    - Web History (65194)
    - Web Search (2849)
  - Keyword Hits
    - Single Literal Keyword Search (117)
      - 2b691602-0749-4f26-9092-83f1aa43db11 (1)
      - 878fc386-5fea-48d8-960f-be65fa1f852c (1)
      - cloudhub (73)
      - garje (32)
      - rngsofttech (10)
    - Single Regular Expression Search (0)
    - Email Addresses (110541)
  - Hashset Hits
  - E-Mail Messages

cloudhub

73 Results

Source File	S	C	Keyword	Keyword Regular Expression	Keyword Preview	Access Time
WaitList.dat	▽		clou[redacted]	[redacted]	% > * (g (> 5 «cloud...	2017-05-05 04:0
Save-AzureRmVMImage_2017-06-02-T12-42-39-309.log	▽		clou[redacted]	[redacted]	tioncontainername : «cloudhubvmimages« -vhdnameprefix : i	2017-06-02 00:1
main.db	▽		clou[redacted]	[redacted]	soft.compute/images/«cloudhubvmimages«/imgwordpress-...	2017-03-22 20:0
Save-AzureRmVMImage_2017-06-02-T12-42-39-309.log	▽		clou[redacted]	[redacted]	ng account: 'edward@«cloudhubtech.com«, environment: '...	2017-06-02 00:1

Matches on page: 1 of 2 Match   Page: 2603 of 2724 Page   Text Source: Search Results

```
          249614 0   6 6 http://wordpresswind.blob.core.windows.net/system/Microsoft.Compute/Images/[redacted]e98e.
vhd?sv=2014-02-14&sr=c&sig=Cb87WA[redacted]se=2017-06-31T18%3A30%3A00Z&sp=rl      http://wordpresswind.blob.core.wi
ndows.net/system/Microsoft.Compute[redacted]95464940e98e.vhd?sv=2014-02-14&sr=c&sig=Cb87WAk2kD2yuvfQJY0AY9oTL84v1Bh0
1AALUdvu%2FH8%3D&st=2017-05-28T18%[redacted]
          249618 0 4742 2 2 https://api.asm.skype.com/v1/objects/0-neu-d2-c456109f6402c067324dca1f591f5e7a IMG_02062017_125356_0.png   https://api.asm.skype.com/v1/objects/0
-neu-d2-c456109f6402c067324dca1f591f5e7a/views/imgt1 https://login.skype.com/login/sso?go=xmmfallback?pic=0-neu-d2-c456109f6402c067324dca1f591f5e7a  Picture.1 2   205565 79878
17 0-neu-d2-c456109f6402c067324d
          249625 0   6 6 mailto[redacted]@gmail.com     mailt[redacted]2@gmail.com  UrlPreview.1     0
          249626 0   6 6 mailto[redacted]gmail.com     mailto[redacted]@gmail.com  UrlPreview.1     0
          249628 0 4743 2 2 https://api.asm.skype.com/v1/objects/0-neu-d3-3f2cbb6a9c9abcc06cd27d544858025f IMG_02062017_130748_0.png   https://api.asm.skype.com/v1/objects/0
-neu-d3-3f2cbb6a9c9abcc06cd27d544858025f/views/imgt1 https://login.skype.com/login/sso?go=xmmfallback?pic=0-neu-d3-3f2cbb6a9c9abcc06cd27d544858025f  Picture.1 2   205565 79881
37 0-neu-d3-3f2cbb6a9c9abcc06cd27d544858025f
          249632 0 4744 2 2 https://api.asm.skype.com/v1/objects/0-neu-d2-4d041180c86b0b3ad807731e18623bd8 IMG_02062017_131134_0.png   https://api.asm.skype.com/v1/objects/0
-neu-d2-4d041180c86b0b3ad807731e18623bd8/views/imgt1 https://login.skype.com/login/sso?go=xmmfallback?pic=0-neu-d2-4d041180c86b0b3ad807731e18623bd8  Picture.1 2   205565 79882
65 0-neu-d2-4d041180c86b0b3ad807731e18623bd8
          249636 0 4745 2 2 https://api.asm.skype.com/v1/objects/0-neu-d5-8720fd952a511b0bc04a44ecd73bad4c IMG_02062017_131554_0.png   https://api.asm.skype.com/v1/objects/0
-neu-d5-8720fd952a511b0bc04a44ecd73bad4c/views/imgt1 https://login.skype.com/login/sso?go=xmmfallback?pic=0-neu-d5-8720fd952a511b0bc04a44ecd73bad4c  Picture.1 2   205565 79883
93 0-neu-d5-8720fd952a511b0bc04a44ecd73bad4c
          249639 0 4746 2 2 https://api.asm.skype.com/v1/objects/0-neu-d1-b933eb54a5acd68b15fae23222548lcf IMG_02062017_131853_0.png   https://api.asm.skype.com/v1/objects/0
-neu-d1-b933eb54a5acd68b15fae23222548lcf/views/imgt1 https://login.skype.com/login/sso?go=xmmfallback?pic=0-neu-d1-b933eb54a5acd68b15fae23222548lcf  Picture.1 2   205565 79884
```

Fig5. Artefact from case study 2

- A considerable challenge arose when trying to reconstruct the sequence of events. Many of the digital artifacts possessed timestamps that appeared distorted or inconsistent, making it challenging to trace a coherent timeline of actions. The combined limitations of not having access to volatile memory data and encountering unreliable timestamps hindered a clear and sequential incident reconstruction.

Limitations and Challenges:

- UFED's incapacity to capture volatile memory introduced a potential blind spot in the investigation, omitting any transient evidence that could be essential to the case.

- Distorted timestamps posed serious challenges in painting an accurate picture of the employee's actions, emphasizing the importance of reliable timestamp data in digital forensic investigations.

6.3 Case Study – Using Cache Memory Forensics

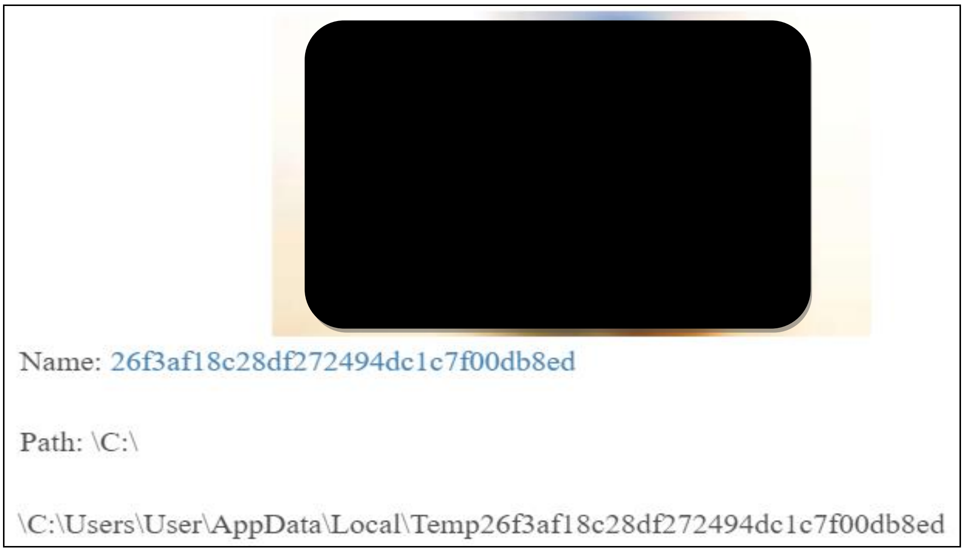
Background:
This case study about a situation where a user accessed restricted files on the system and the files are to be recovered as it is in deleted state. Due to the extreme sensitivity of the information in the evidence, traditional imaging of the entire system is not permitted, which introduces unique challenge and a need for alternative forensic methods.

Methodology:
Acquisition of Evidence: Considering the restrictions on full-system imaging, it is decided to pivot the approach. Hence targeting the volatile memory (RAM) of the device, given its potential to retain recent system activities. Volatility is used here for forensic analysis.

Analysis: With the volatile memory safely acquired, this embarks on a deep dive analysis using two forensic analysers; Magnet Axiom and UFED4PC. Both these tools are equipped to parse and scrutinize digital artifacts present in the volatile memory, drawing out crucial pieces of evidence.

Key Findings:

- The decision to focus on volatile memory proved to be advantageous. Within the acquired memory dump, artifacts were identified that confirmed the employee's actions of opening the restricted files.
- Evidence within the system's cache memory were discovered, which showed footprints of the recently accessed restricted files. Cache memory, being a subset of volatile memory, retains snippets of recent actions and files, offering a goldmine of potential evidence.



[redacted]

Name: 26f3af18c28df272494dc1c7f00db8ed

Path: \C:\

\C:\Users\User\AppData\Local\Temp26f3af18c28df272494dc1c7f00db8ed

Fig. 6 Evidence acquired from cache memory

- Interestingly, this method of volatile memory acquisition expedites investigation timeline. Compared to previous case studies which relied on traditional imaging and analysis methods, focusing on volatile memory allows to achieve findings in lesser time. This is largely due to the nature of volatile memory containing recent system activities, enabling a more direct route to the evidence related to the incident in question.

Advantages and Insights:

- Volatile memory, despite its transient nature, can be rich in vital pieces of evidence, especially concerning recent system activities.
- Focusing on volatile memory in scenarios where traditional imaging is not feasible can not only lead to conclusive evidence but also expedite the investigation process.
- This case emphasized the importance of adapting to the constraints of an investigation and leveraging alternative forensic methods to achieve objectives.

6.4 Discussion

Across the three case studies undertaken, a spectrum of forensic methodologies and their associated challenges is observed. This comprehensive evaluation of proposed approach underscores the evolving dynamics of digital forensics, especially in the realm of data acquisition and analysis.

1. Evaluation and Criticism of the Experiments:

- **Traditional Imaging Limitations:** In the first two case studies, the forensic examinations primarily relied on traditional imaging techniques using the Tableau Forensic Imager and FTK Imager respectively. While these tools ensured the preservation of digital evidence, their inability to capture volatile memory presented significant blind spots in the investigation. Especially in the second case, the UFED4PC's inability to acquire volatile memory compounded the limitations were experienced.
- **Incident Reconstruction Challenges:** Across all three cases, a recurring challenge is the reconstruction of the entire sequence of the alleged incidents. Whether due to distorted timestamps, as seen in the second case, or due to the inherent limitations of tools like the Tableau, piecing together a coherent timeline proved to be a daunting task.
- **Volatile Memory's Potential:** The third case study is unique in its emphasis on volatile memory. The results show; not only conclusive evidence in half the time compared to the earlier methods, but it also highlights the depth of information volatile memory can offer.

2. Suggested Modifications and Improvements:

- **Comprehensive Acquisition**: A clear takeaway is the need for a more holistic data acquisition approach. Tools that can integrate both traditional imaging and volatile memory extraction would plug the evident gaps seen in the first two studies. By ensuring that no potential evidence source is overlooked, this elevates the reliability of findings.
- **Time-Stamp Verification**: Given the challenges experienced with distorted timestamps in the second case, it's paramount to employ secondary methods or tools that can corroborate or validate timestamp data. This would help in constructing a more precise incident timeline.

3. Proposing a Novel Approach:

Volatile Memory-Centric Forensic Acquisition (VMCFA):

- **Preliminary Assessment:** Before initiating forensic acquisition, a preliminary assessment is to be made to determine if volatile memory extraction is feasible and beneficial based on the nature of the alleged incident.
- **Tiered Acquisition Strategy:** Begin with the extraction of volatile memory to secure recent system activities. Tools like Volatility can be incorporated as standard practice. Subsequently, depending on case requirements, traditional imaging can be executed.
- **Enhanced Analysis Tools:** Forensic analysers like Magnet Axiom and UFED4PC is to be further optimized to delve deeper into volatile memory dumps. This means enhancing the ability to interpret, reconstruct, and present evidence from transient data sources like cache memories.
- **Cache Memory Emphasis:** Given the potential of cache memory in retaining snippets of recent actions and files, as observed in the third case, future forensic tools need to place an enhanced focus on cache memory analysis.

7 Conclusion and Future Work

From the above case studies performed, various tools and techniques are used to perform forensic activities and recreational activities. The case studies successfully performed however, some tools and techniques lacked in providing crucial information and which resulted in additional time consumption. One of the methods that used volatile memory analysis in the third case study, consumed less time in acquisition and analysis and even presented exact findings from the limited sources. This proves that use of volatile memory for forensics purposes improves the current approach.

This research paper also concludes with a dire need for a framework that guides to acquire and analyse the volatile memory as a part of preliminary investigation as most of the data that is being used in runtime is present in the volatile memory, hence proves how important cache memory is and how important cache memory forensics is in forensic investigations. Additionally, this also shows how cache memory forensics helps in detecting any threat actors or risks that are malicious to regular system.

As a part of future work, a specialized tool can be built targeting cache files of the operating system which will forensically analyse and examine the memory for any persistent threats. Additionally, a reporting mechanism can also be implemented to document the key findings. Specifically looking for cache files into the memory will help in detecting artefacts useful for the analysis. Moreover, accessing cache memory directly through program would be next step to improvise in the framework.

References

Adams, R., Hobbs, V. and Mann, G. (2013) 'The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice', *Journal of Digital Forensics, Security and Law* [Preprint]. Available at: https://doi.org/10.15394/jdfsl.2013.1154.

Al-Dhaqm, A. *et al.* (2020) 'Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field', *IEEE Access*, 8, pp. 145018–145032. Available at: https://doi.org/10.1109/ACCESS.2020.3008696.

Boucher, J. and Le-Khac, N.-A. (2018) 'Forensic framework to identify local vs synced artefacts', *Digital Investigation*, 24, pp. S68–S75. Available at: https://doi.org/10.1016/j.diin.2018.01.009.

Henricksen, M. (2010) 'Comments on Cache-Timing Attacks on Stream Ciphers', in *2010 First ACIS International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery, E-Commerce and Its Applications, and Embedded Systems*. *Its Applications and Embedded Sys (CDEE)*, Qinhuandao, Hebei, China: IEEE, pp. 196–200. Available at: https://doi.org/10.1109/CDEE.2010.46.

V. Baryamureeba, F. Tushabe (2019) '*The Enhanced Digital Investigation Process Model - DFRWS*', *The Digital Forensic Research Conference*. Available at: https://www.researchgate.net/publication/228870524_The_enhanced_digital_investigation_process_model.

Ito, A. *et al.* (2021) 'Imbalanced Data Problems in Deep Learning-Based Side-Channel Attacks: Analysis and Solution', *IEEE Transactions on Information Forensics and Security*, 16, pp. 3790–3802. Available at: https://doi.org/10.1109/TIFS.2021.3092050.

Lee, J.-T., Choi, H.K. and Kim, K.-J. (2009) 'Gathering and Storage Technique Implementation of Volatility Memory Data for Real-Forensic', in *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*. *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, Seoul, Korea: IEEE, pp. 1076–1079. Available at: https://doi.org/10.1109/ICCIT.2009.234.

Lei Zhang, Dong Zhang, and Lianhai Wang (2010) 'Live digital forensics in a virtual machine', in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, Taiyuan, China: IEEE, pp. V4-328-V4-332. Available at: https://doi.org/10.1109/ICCASM.2010.5620364.

Manes, G.W. and Downing, E. (2009) 'Overview of Licensing and Legal Issues for Digital Forensic Investigators', *IEEE Security & Privacy Magazine*, 7(2), pp. 45–48. Available at: https://doi.org/10.1109/MSP.2009.46.

Meera, V., Isaac, M.M. and Balan, C. (2013) 'Forensic acquisition and analysis of VMware virtual machine artifacts', in *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*. *2013 International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, Kottayam: IEEE, pp. 255–259. Available at: https://doi.org/10.1109/iMac4s.2013.6526418.

Nalawade, A., Bharne, S. and Mane, V. (2016) 'Forensic analysis and evidence collection for web browser activity', in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*. *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, Pune, India: IEEE, pp. 518–522. Available at: https://doi.org/10.1109/ICACDOT.2016.7877639.

Nishtha and Meenu (2018) 'Security in Cache Memory: Review', in *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*. *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, Erode: IEEE, pp. 659–662. Available at: https://doi.org/10.1109/ICCMC.2018.8487674.

Nyholm, H. *et al.* (2022) 'The Evolution of Volatile Memory Forensics', *Journal of Cybersecurity and Privacy*, 2(3), pp. 556–572. Available at: https://doi.org/10.3390/jcp2030028.

Osvik, D.A., Shamir, A. and Tromer, E. (2006) 'Cache Attacks and Countermeasures: The Case of AES', in D. Pointcheval (ed.) *Topics in Cryptology – CT-RSA 2006*. Berlin, Heidelberg:

Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 1–20. Available at: https://doi.org/10.1007/11605805_1.

Pagani, F. and Balzarotti, D. (2022) ‘AutoProfile: Towards Automated Profile Generation for Memory Analysis’, *ACM Transactions on Privacy and Security*, 25(1), pp. 1–26. Available at: https://doi.org/10.1145/3485471.

Periyadi, Mutiara, G.A. and Wijaya, R. (2017) ‘Digital forensics random access memory using live technique based on network attacked’, in *2017 5th International Conference on Information and Communication Technology (ICoIC7). 2017 5th International Conference on Information and Communication Technology (ICoIC7)*, Melaka, Malaysia: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ICoICT.2017.8074695.

Raghavan, S. (2012) ‘Digital forensic research: Current state of the art’, *CSI Transactions on ICT*, 1. Available at: https://doi.org/10.1007/s40012-012-0008-7.

Rowe, N.C. and Garfinkel, S.L. (2010) ‘Global Analysis of Drive File Times’, in *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, Oakland, CA, USA: IEEE, pp. 97–108. Available at: https://doi.org/10.1109/SADFE.2010.21.

Roy, S., Wu, Y. and LaVenia, K.N. (2019) ‘Experience of Incorporating NIST Standards in a Digital Forensics Curricula’, in *2019 7th International Symposium on Digital Forensics and Security (ISDFS). 2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ISDFS.2019.8757533.

Savaş, E. and Yılmaz, C. (2015) ‘A Generic Method for the Analysis of a Class of Cache Attacks: A Case Study for AES’, *The Computer Journal*, 58(10), pp. 2716–2737. Available at: https://doi.org/10.1093/comjnl/bxv027.

Shrivastava, G. and Gupta, B.B. (2014) ‘An Encapsulated Approach of Forensic Model for digital investigation’, in *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE). 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, Tokyo, Japan: IEEE, pp. 280–284. Available at: https://doi.org/10.1109/GCCE.2014.7031241.

Tang, C. *et al.* (2023) ‘Cache eviction for SSD-HDD hybrid storage based on sequential packing’, *Journal of Systems Architecture*, 141, p. 102930. Available at: https://doi.org/10.1016/j.sysarc.2023.102930.

Tanner, A. *et al.* (2022) ‘The Need for Proactive Digital Forensics in Addressing Critical Infrastructure Cyber Attacks’, in *2022 International Conference on Computational Science and Computational Intelligence (CSCI). 2022 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA: IEEE, pp. 976–982. Available at: https://doi.org/10.1109/CSCI58124.2022.00174.

Ulupinar, S. *et al.* (2017) ‘The importance of standardization in biometric data for digital forensics’, in *2017 International Conference on Computer Science and Engineering (UBMK). 2017 International Conference on Computer Science and Engineering (UBMK)*, Antalya: IEEE, pp. 781–785. Available at: https://doi.org/10.1109/UBMK.2017.8093529.

Wang, L. *et al.* (2020) ‘Analyzing The Security of The Cache Side Channel Defences With Attack Graphs’, in *2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC). 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*, Beijing, China: IEEE, pp. 50–55. Available at: https://doi.org/10.1109/ASP-DAC47756.2020.9045664.

Zawoad, S. and Hasan, R. (2013) ‘Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems’. Available at: https://doi.org/10.48550/ARXIV.1302.6312.